הצעת חוק

הגנת הפרטיות
התשע"ט- 2019

רחל ארידור הרשקוביץ
תהילה שוורץ אלטשולר

יוני 2019

המכון הישראלי
לדמוקרטיה

הצעת חוק הגנת הפרטיות, התשע"ט–2019

רחל ארידור הרשקוביץ | תהילה שוורץ אלטשולר

יוני 2019

המכון הישראלי
לדמוקרטיה

Privacy Protection Bill, 2019-5779 – A Proposed Draft
Rachel Aridor-Hershkovitz | Tehilla Shwartz Altshuler

עריכת הטקסט: ענת ברנשטיין
עימוד: נדב שטכמן פולישוק
הדפסה: גרפוס פרינט, ירושלים
עיצוב העטיפה: סטודיו תמר בר-דיין

מסת"ב ISBN 978-965-519-265-0

© כל הזכויות שמורות למכון הישראלי לדמוקרטיה (ע"ר), 2019
נדפס בישראל, תשע"ט/2019

אין לשכפל, להעתיק, לצלם, להקליט, לתרגם, לאחסן במאגר ידע, לשדר או לקלוט בכל דרך או אמצעי אלקטרוני, אופטי או מכני או אחר — כל חלק שהוא מהחומר בספר זה. שימוש מסחרי מכל סוג שהוא בחומר הכלול בספר זה אסור בהחלט אלא ברשות מפורשת בכתב מהמו"ל.

המכון הישראלי לדמוקרטיה
רח' פינסקר 4, ת"ד 4702, ירושלים 9104602
טל': 02-5300888
אתר האינטרנט: www.idi.org.il

להזמנת ספרים
החנות המקוונת: www.idi.org.il/books
דוא"ל: orders@idi.org.il
טל': 02-5300800 ; פקס: 02-5300867

כל פרסומי המכון ניתנים להורדה חינם, במלואם או בחלקם, מאתר האינטרנט.

המכון הישראלי לדמוקרטיה

המכון הישראלי לדמוקרטיה הוא מוסד עצמאי א־מפלגתי, מחקרי ויישומי, הפועל בזירה הציבורית הישראלית בתחומי הממשל, הכלכלה והחברה. יעדיו הם חיזוק התשתית הערכית והמוסדית של ישראל כמדינה יהודית ודמוקרטית, שיפור התפקוד של מבני הממשל והמשק, גיבוש דרכים להתמודדות עם אתגרי הביטחון מתוך שמירה על הערכים הדמוקרטיים וטיפוח שותפות ומכנה משותף אזרחי בחברה הישראלית רבת הפנים.

לצורך מימוש יעדים אלו חוקרי המכון שוקדים על מחקרים המניחים תשתית רעיונית ומעשית לדמוקרטיה הישראלית. בעקבותיהם מגובשות המלצות מעשיות לשיפור התפקוד של המשטר במדינת ישראל ולטיפוח חזון ארוך טווח של תרבות דמוקרטית נכונה לחברה הישראלית ולמגוון הזהויות שבה. המכון שם לו למטרה לקדם בישראל שיח ציבורי מבוסס ידע בנושאים שעל סדר היום הלאומי, ליזום רפורמות מבניות, פוליטיות וכלכליות ולשמש גוף מייעץ למקבלי ההחלטות ולציבור הרחב.

המכון הישראלי לדמוקרטיה הוא זוכה פרס ישראל לשנת תשס״ט על מפעל חיים — תרומה מיוחדת לחברה ולמדינה.

הדברים המובאים במסמך זה אינם משקפים בהכרח את עמדת המכון הישראלי לדמוקרטיה.

תוכן העניינים

מבוא 7

הצעת חוק הגנת הפרטיות, התשע"ט–2019, ודברי הסבר מפורטים 21

תוכן העניינים 23

הצעת חוק הגנת הפרטיות, התשע"ט–2019, ודברי הסבר מקוצרים 163

תוכן העניינים 165

השוואת נוסחים בין חוק הגנת הפרטיות, התשמ"א–1981,
לבין נוסח הצעת חוק הגנת הפרטיות, התשע"ט–2019,
ודברי הסבר מקוצרים 223

מבוא

חוק הגנת הפרטיות נחקק בשנת 1981, ומאז חקיקתו תוקן פעמים אחדות. בשנת 1985 נוסף לו פרק ד, אשר עסק במסירת מידע מאת גופים ציבוריים; בשנת 1996 עודכן פרק ב לחוק העוסק במאגרי מידע; ובשנת 2007 תוקנה הגדרת ה"הסכמה" והוספו פיצויים ללא הוכחת נזק במצבים מסוימים.

כבר עם חקיקתו כלל החוק הן הגנה על פרטיות במובנה הקלסי (privacy) הן הגנה על מידע שנמצא במאגרי מידע (data protection). בשנת 2004 התגבשה במשרד המשפטים ההבנה שיש לבחון מחדש את ההסדר הקבוע בחוק בעניין מאגרי מידע ולגבש הצעה למכלול התיקונים הנדרשים. הסיבות העיקריות להבנה זו היו עיגונה של הזכות לפרטיות כזכות חוקתית בסעיף 7 לחוק-יסוד: כבוד האדם וחירותו והחידושים הטכנולוגיים שהביאו להתגברות השימוש במאגרי מידע ממוחשבים באופנים חדשים שלא היו ידועים ומוכרים בעת חקיקת החוק. כדי לבחון מחדש את החוק מונתה ועדת מומחים, מתוך המערכת הממשלתית ומחוצה לה, בראשות המשנה ליועץ המשפטי לממשלה יהושע שופמן. הדוח המקיף הוגש בינואר 2007.[i] ואולם מתוך מכלול התיקונים שהציעה הוועדה נדון בכנסת רק התיקון להגדרת "הסכמה".

בעשור וחצי האחרון יצרה ההתפתחות הטכנולוגית המהירה מתח ואי–הלימה בין הזכות לפרטיות לבין פרקטיקות של איסוף, איגום ועיבוד של מידע אישי, שהכלכלה הדיגיטלית מבוססת עליהן. כולן התרחבו דרמטית:

- נוצרו טכניקות חדשות וזולות של אחסון כמויות עצומות של מידע אישי.
- התחוללה מהפכת הקישוריות (אינטרנט), לא רק במה שקשור למסרי תוכן אלא הכול (החל במכשירים וכלה בננו-בוטים בתוך גוף האדם עצמו). מהפכת הקישוריות מאפשרת העברת נתוני עתק (Big Data) בלתי פוסקת מחיישנים וממכשירים אוגמי מידע אישי ל"מוחות" מרכזיים.
- קרתה מהפכת הבינה המלאכותית – המאפשרת את ניתוח הנתונים, לרבות המידע האישי שנאגם.

i הצוות לבחינת החקיקה בתחום מאגרי המידע, דין וחשבון (ינואר 2007), עמ' 19-23 (להלן: "**ועדת שופמן**").

מדינות, וגם גופי ענק מסחריים, הפכו להיות "כּוֹרֵי מידע אישי". למעשה אפשר לומר — במונח השאול מן הדירקטיבה להגנת נתונים של האיחוד האירופי[ii] — שכולנו "נושאי מידע" (data subjects). ליבת הכלכלה הדיגיטלית והמודל העסקי של חברות ענק כגון גוגל, אמזון ופייסבוק היא צבירת עוד ועוד מידע אישי וניתוח שלו לצורך הפקת תובנות חדשות. יתר על כן, מיליוני עסקים קטנים ובינוניים אוגמים מידע אישי כל העת. ערכם של מאגרי המידע הפרטי אדיר – למן מידע על הרגלי גלישה ועד למידע על היסטוריה רפואית. המדינות לא נותרו מאחור, וגם הן מפתחות מערכות לאיסוף מידע אישי מסוגים שונים – החל במידע אישי הנאסף בפעילות ממשלתית שגרתית (כדוגמת חינוך, מיסוי, בריאות ושירותי רווחה), עבור במצלמות במרחב הציבורי וחיישני חום וקול לזיהוי אזרחים ולניטור פעולותיהם, וכלה במאגרים למידע ביומטרי או איסוף יזום של מידע מרשתות חברתיות.

איסוף המידע האישי האינטנסיבי והיתרונות הגלומים בטכנולוגיה מחייבים חשיבה מחודשת על דמותה של הזכות לפרטיות ועל ההסדרים הקיימים בחוק הגנת הפרטיות. כניסתה לתוקף של החקיקה להגנת נתונים של האיחוד האירופי במאי 2018 (General Data Protection Regulations (להלן: "**GDPR**"), שהחליפה את הדירקטיבה להגנת נתונים של האיחוד האירופי שקדמה לה, וחשיפת השימושים הבעייתיים שנעשים במידע אישי על מיליוני משתמשים ברחבי העולם, ובכללם אזרחי ישראל (כגון פרשת **קיימברידג' אנליטיקה**), מחזקות גם הן את העמדה שחוק הגנת פרטיות חדש למדינת ישראל הוא צורך השעה.

זאת ועוד, ב-2011 קיבלה מדינת ישראל את ההכרה בדבר תאימות הדין הישראלי למשטר הגנת הפרטיות באיחוד האירופי (adequacy). מכיוון שאירופה היא שוק ייצוא חשוב ביותר של ישראל, הכרה זו מאפשרת העברת מידע פשוטה וקלה בין האיחוד לבין חברות, ארגונים ומוסדות מחקר בישראל. אלא שהכרה זו נמצאת בעצם הימים האלה בבחינה מחדש, ויש יסוד לחשש שהיא תישלל בשל הפער הגדל בין ה-GDPR לבין חוק הגנת הפרטיות הישראלי המיושן וההסדרים שנוספו לו מאז 2011. מסיבות אלה, הצעת החוק שתפורט להלן שואבת השראה גם מהוראות ה-GDPR.

במאי 2016, בחלוף 35 שנה מאז חקיקת חוק הגנת הפרטיות, נולדה יוזמה משותפת של המכון הישראלי לדמוקרטיה ועו"ד חיים רביה, ראש קבוצת הסייבר במשרד עורכי דין פרל כהן צדק לצר ברץ. היעד שהצבנו לעצמנו היה ליצור יחד הצעת נוסח חדש לחוק הגנת

ii Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (Official J. L 281, 23/11/1995 P. 0031-0050) (להלן: "**הדירקטיבה להגנת נתונים של האיחוד האירופי**"). הדירקטיבה הוחלפה על ידי ה- General Data Protection Regulation 2016/67 (להלן: "**GDPR**").

הפרטיות. לשם כך גיבשנו קבוצת מומחים של משפטנים, אנשי אקדמיה ומומחי טכנולוגיה מן השירות הציבורי, החברה האזרחית, המגזר הפרטי והתעשייה. רצינו לגבש הצעה לחוק הגנת פרטיות חדש שיהלום את צורכי הזמן – החל בהגדרת הזכות לפרטיות, עבור בהגנות המצויות בו, וכלה בהתאמתו לעולם דיגיטלי. הקבוצה נפגשה במשך שנתיים אחת לכמה שבועות ודנה בכל פגישה בנושא אחר על רקע ההסדרים הקיימים בחוק הקיים, בפרשנות השיפוטית שניתנה להם ובהסדרים השוואתיים. חברי הקבוצה פעלו בהתנדבות מלאה וייחדו שעות רבות של עבודה מאומצת בדיונים.

הדרך שפסענו בה לא הייתה מסומנת מראש. השאלות הונחו כולן על השולחן. למשל: האם נכון לנסח חוק להגנת הפרטיות הקלסית במשולב עם חוק פרטיות במידע? מה ראוי ומה לא ראוי לקחת מה-GDPR, ומה נכון יותר לשאוב מהסדרים קיימים במדינות אחרות, כגון אוסטרליה, קנדה או ניו זילנד? כיצד נכון להתאים את ההסדרים שב-GDPR כך שיהלמו את תנאי הארץ ותושביה, מצד אחד, ובה בעת יאפשרו פעילות שוטפת בעולם של העברת מידע אישי חוצת-גבולות, מצד שני? מהם החסרים ב-GDPR כפי שהם מתגלים כבר כעת, תוך כדי תנועה, ועל כן מוטב שלא לאמצם? מהן התפיסות המשפטיות שהתגבשו בישראל במרוצת השנים באשר להיקפה של הזכות לפרטיות, ומה מהן נכון לשמר? כיצד צריך להתייחס להצעות חקיקה תלויות ועומדות כגון תיקון מס' 13 לחוק הגנת הפרטיות?[iii] האם נכון לנסח הצעת חוק חדשה ומקיפה או שמא עדיף להציע תיקונים לחוק הגנת הפרטיות הקיים על מנת להביא לתיקון נושאים בוערים במהירות? מהם האתגרים הטכנולוגיים הרובצים לפתחנו, למשל – האם "הזכות להישכח" יכולה להתקיים בעולם שבו מכונות לומדות אינן שוכחות דבר מן הנתונים שעליהם התאמנו? מהו המשקל שראוי לתת להסכמה כאמצעי להחרגה מאחריות על פגיעה בפרטיות, והאם מדובר במשקל מופרז ובעצם במכבסה הגדולה של דורנו?

המבנה ההטרוגני של הקבוצה חִייב גם התייחסות לעמדות שונות ועריכת איזון עדין ביניהן. למשל, האיזון בין תפיסת הזכות לפרטיות כזכות מרכזית בעולם הדיגיטלי בגלל האפשרות להשתמש בעיבוד של מידע אישי כדי להשפיע על קבלת החלטות ועל האוטונומיה האישית לבין הצורך להתחשב באינטרס החשוב של מימוש חדשנות והתפתחות טכנולוגית וכלכלית.

חרף הקושי העדפנו לייצר תוצר בדמות הצעת חוק ולא רק מסמך מדיניות שיגדיר באופן כללי את הכיוונים ואת האיזונים העקרוניים. סברנו כי הזמן דוחק וכי החשיבות של יצירת הסדרים קונקרטיים כבר בתקופה הקרובה היא קריטית, הן להגנה על זכויות האדם ועל

iii הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח–2018 (להלן: **"הצ"ח תיקון מס' 13"**).

מימושו של הליך דמוקרטי תקין והן להתפתחות הכלכלית והטכנולוגית וליצירת כללי משחק בהירים ועדכניים. המחלוקת בין חברי הקבוצה באשר להסדר הקונקרטי הייתה נוכחת, אבל לאחר שהכרענו בה, נתנו לה מקום בדברי ההסבר – כדי שתוכל לשרת דיון עתידי סביב הליכי החקיקה.

תוצר העבודה של הקבוצה, כפי שגובש על ידינו, מוצג לפניכם כעת. בטרם נפרט את רשימת השינויים והחידושים שיש בו באשר לחוק הקיים, נציין כי לאחר התלבטויות לא מעטות החלטנו להותיר בהצעה שגיבשנו את השילוב שבין הגנת הפרטיות הקלסית להגנת הפרטיות במידע. עשינו זאת אף שבמרבית מדינות העולם, ובכלל זה באיחוד האירופי, חוקי הגנת הפרטיות מתמקדים בהגנה על הפרטיות במידע. השיקולים שהנחו אותנו היו הרצון לשמור על מבנה החקיקה הקיים בישראל – כדי למנוע קשיים בהטמעה במערכת המשפט, במגזר הציבורי ובתעשייה; מפאת החשש מפני האטת הליך החקיקה אם יוצעו שני חוקים נפרדים; ובשל השאיפה ליצור דבר חקיקה מקיף וחדשני להגנה על מכלול מופעי הפרטיות האפשריים.

העדפנו לנסח הצעת חוק חדשה ומקיפה ולא להתמקד בתיקון החוק הקיים בנושאים ספציפיים בלבד. לדעתנו, חשיבותה הגוברת של הזכות לפרטיות לנוכח הפיכת המידע האישי לנכס סחיר בעל ערך רב, המכונה אפילו "הנפט החדש",[iv] מחייבת לשנות מן היסוד את חוק הגנת הפרטיות בישראל. אי-אפשר לספק הגנה ברמה נאותה לזכות היסוד לפרטיות באמצעות תיקוני חקיקה בשיטת טלאי על טלאי ואשר נשענים על חוק מיושן המותאם למציאות בדרך של פרשנות יצירתית. דעתנו היא אפוא שיש לבטל את חוק הגנת הפרטיות הקיים ולחוקק במקומו את הצעת החוק. משום כך בחרנו לקרוא למסמך "הצעת חוק הגנת הפרטיות".

אנו סבורים ומאמינים שמדובר בתרומה חשובה לחברה בישראל ולמדינה. דיון נוקב בזכות לפרטיות וקביעה בהירה של כללי המשחק וההסדרים שצריכים לעטוף אותה בהקשרים השונים שבהם היא משפיעה על חיינו הם צורך השעה. אנו מקווים שמקבלי ההחלטות יעשו בהצעה שימוש לתועלת הכלל.

החידושים העיקריים בהצעת החוק שלנו

1. סעיף המטרה

ההחלטה לקבוע בהצעת החוק סעיף מטרה נועדה לסייע בפרשנותו המשפטית ולהבהיר כי המטרה בהגנה על הזכות לפרטיות היא משולשת:

iv *The World's Most Valuable Resource is no longer Oil, but Data*, THE ECONOMIST (May 6, 2017)

(א) הגנה על הזכות להיעזב במנוחה, הגנה על סוד השיח והגנה על צנעת החיים האישיים הן הזכויות הקלסיות שסביבן התפתחה הגנת הפרטיות.

(ב) הגנה על יכולתו של אדם לשלוט במידע אישי עליו, שנאסף או מעובד בידי אחרים כחלק מליבת הפעילות בעולם הדיגיטלי ובכלכלה מבוססת המידע.

(ג) הגנה על יכולתם של אנשים לקבל החלטות באופן חופשי ואוטונומי, בייחוד בהקשר של בחירות דמוקרטיות וסביבן, בעולם שבו עיבוד מידע אישי יכול לשמש ליצירת "מלכודות על האוטונומיה" ותהליכי שכנוע ברמת פרטנות וחודרנות שלא נודעו בהיסטוריה האנושית.

שלוש יתדות אלה אמורות לייצר מסגרת ערכית, ניטרלית-טכנולוגית, להגנה על הפרטיות בישראל.

2. הגדרת הפגיעה בפרטיות

עדכנו את הרשימה הסגורה של העילות המהוות פגיעה בפרטיות לפי חוק הגנת הפרטיות הקיים, ולכן הוספנו לרשימת עילות הפגיעה הקלסיות (כגון הטרדה, צילום ברשות היחיד, פרסום מידע פרטי שעלול להשפיל או לבזות, האזנה אסורה, שימוש בשמו של אדם, הפרת הוראת סודיות הקיימת בדין) עוד שתי עילות: עילת הצפייה או העיון במידע אישי ועילת עיבוד המידע האישי על אדם בניגוד להוראות החוק. עילות אלו יהיו עמוד השדרה של הגנת הפרטיות במידע אישי דיגיטלי.

3. ביטול החובה לרישום מאגרי מידע

החובה לרישום מאגרי מידע היא אחד העוגנים של החוק הקיים להגנת פרטיות. חובה זו הפכה לאות מתה.

שלוש סיבות לכך:

- אין על החובה לרישום מאגרי מידע אכיפה מספקת;
- החובה אינה ערובה להגנה על פרטיות;
- אגרות הרישום בוטלו על ידי הרשות להגנת הפרטיות החל באוגוסט 2017.

נציין שוועדת שופמן המליצה כבר ב-2007 לצמצם את חובת הרישום,[v] וכך המליץ גם משרד המשפטים בתזכיר תיקון חוק הגנת הפרטיות (צמצום חובת הרישום

v ועדת שופמן, **לעיל** ה"ש i, בעמ' 24.

וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולתיעודם במסמכים), התשע"ב-2012. בתזכיר אף נאמר שחובת הרישום אינה מבטיחה ציות להוראות החוק ועל כן יש להעדיף מנגנון חלופי שיגרום להפנמת החובות להגנת הפרטיות.[vi]

אנו סבורים כי בעולם דיגיטלי, שבו מידע אישי נאגם ונשמר כעניין שבשגרה, הדרישה לרישום מאגרי מידע מטילה נטל רגולטורי בלתי סביר כמעט על כל אדם המחזיק רשימת שמות של לקוחות, צרכנים או משתמשים בשירות שהוא נותן. אנו חושבים כי מערך הכלים החלופי להגנת פרטיות במידע אישי שאנו מציעים (ושיפורט להלן) ייתן מענה מקיף ומדויק יותר לצורך בהגנה על הפרטיות משנותנת החובה לרישום מאגרי מידע.

4. ניטרליות טכנולוגית

לתפיסתנו, אין צורך בהתייחסות לטכנולוגיות או לסוגי ממסר ספציפיים. אנו מציעים לעגן הסדרים כלליים וניטרליים לטכנולוגיה ככל האפשר. לפיכך, למשל, לא כללנו בהצעת החוק הוראות בעניין דיוור ישיר.

5. הגדרות

חידדנו את ההגדרות הקיימות בחוק הגנת הפרטיות הקיים, ובכלל זה:

(א) החלפנו את ההגדרות של "מנהל מאגר מידע" ו"מחזיק במידע" ב"בעל שליטה במידע" וב"מעבד מידע". ההחלפה נעשתה בד בבד עם הסרת החובה לרישום מאגרי מידע וכן בעקבות ההגדרות ב-GDPR.

(ב) החלפנו את הגדרת "מידע" שבחוק הגנת הפרטיות הקיים בהגדרה מהודקת יותר של "מידע אישי" בדומה להמלצות ועדת שופמן. ההגדרה שהצענו מקיפה יותר ומתייחסת ל"נתונים על אדם מזוהה או שניתן לזהותו במאמץ סביר", ולא לסוגים שונים של מידע כגון מידע על מעמדו האישי של אדם או על מצבו הבריאותי.

(ג) הרחבנו את הגדרת "מידע רגיש" בחוק הקיים כך שתכלול מידע אישי שיש בו כדי לזהות סוגי מידע שונים, כגון עבר פלילי, נתונים ביומטריים ונתונים גנטיים.

(ד) החלפנו את הגדרת ה"שימוש" במידע אישי שבחוק הקיים בהגדרת "עיבוד" מידע אישי. ההגדרה החדשה שאנו מציעים קובעת רשימה סגורה של שלושה

vi תזכיר חוק לתיקון חוק הגנת הפרטיות (לצמצום חובת הרישום וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולתיעודם במסמכים), התשע"ב–2012 (להלן: "**תזכיר צמצום חובת הרישום**").

סוגי פעולות: איסוף, ניתוח והפצה. לפיכך היא מותאמת למכלול הפעולות שאפשר לעשות במידע אישי בעולם דיגיטלי.

(ה) הגדרנו את ההסכמה ככזו שניתנת במפורש או מכללא, מדעת, כאמור בחוק הקיים, והוספנו שיש צורך שההסכמה תינתן גם "מרצון חופשי". השינוי שאנו מציעים נותן ביטוי לדרישה לשליטה טובה יותר של נושאי המידע במידע האישי עליהם, והיא מנוסחת בעקבות הנוסח ב-GDPR.

6. שינוי תפיסה כלפי דרישת ההסכמה

תגובת הנגד החקיקתית הטבעית לאיגום המסיבי של מידע אישי כך שהוא מקיף היבטים רבים בחיינו היא שכלול הזכות לפרטיות כדי לקדם שליטה טובה יותר של אנשים במידע עליהם. הנגזרת הראשונה של השליטה היא האיסור על ביצוע פעולות במידע אישי ללא הסכמת נושא המידע. זו הגישה המקובלת במדינות רבות, וגם בישראל, בניתוח של סכסוכי פרטיות, ויש לה מקום חשוב ביותר ב-GDPR. הקושי הוא שתלות חזקה מדי בדרישת ההסכמה בעולם שבו מידע אישי מעובד בדרכים שונות ולמטרות שאת חלקן לא ניתן לצפות מראש בעת ההסכמה היא בעייתית. יתרה מזו, מומחי כלכלה התנהגותית טוענים שהסכמה הפכה להיות עניין שאנשים עושים כמצוות אנשים מלומדה. יש פער בין תפיסת הפרטיות של האנשים כפי שהיא באה לידי ביטוי בהצהרות של משתמשים לבין התנהגותם הלכה למעשה. עוד הם טוענים כי להסכמה לפגיעה בפרטיות יכולות להיות השלכות שליליות על אחרים. למשל, הצטרפות לרשת חברתית מאפשרת לרשת לקבל את רשימת אנשי הקשר של המצטרף, ותיוג פָּנים מאפשר ללמוד על אחרים שמצולמים באותה תמונה – בבחינת אמור לי מי חבריך ואומר לך מי אתה; והסכמה למסירת מידע גנטי מאפשרת ללמוד על בני המשפחה.

אנו סבורים כי הפתרון הוא לקבוע בחקיקה, בבהירות רבה, מתי לגיטימי וסביר לפגוע בזכותו של אדם לפרטיות. כמו כן אנו מציעים לראות בהסכמה כלי חשוב, אך לא יחיד ואף לא ראשון, להכשרת פגיעה בפרטיות. קבענו כי פגיעה בפרטיות היא פגיעה שנעשית שלא לפי הוראות החוק – שלא כמו הנוסח הנוכחי שבחוק הגנת הפרטיות: "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". הצעת החוק שאנו מציעים מפרטת בסיסים לגיטימיים לפגיעה בפרטיות, בכלל זה בדרך של עיבוד מידע אישי ומידע רגיש, שהאחרון שבהם, מבחינת סדר הופעתו ומבחינת חשיבותו, הוא הסכמת נושא המידע. עוד קבענו כי לנושא המידע זכות לחזור בו בכל עת מהסכמתו, ועל בעל שליטה במידע להביא זאת בחשבון.

7. פגיעה בפרטיות של קטינים

בהתבסס על הצעת איגוד האינטרנט הישראלי בעניין שימוש במידע פרטי על קטינים מתחת לגיל 13 הוספנו את החובה לקבל הסכמה מהורה או מאפוטרופוס לשם פגיעה בפרטיות של קטינים, ובכלל זה בדרך של עיבוד מידע אישי עליהם.[vii] כמו כן הצענו כי הרשות להגנת הפרטיות תקבע הנחיות לאימות גיל של קטינים ולדרכי ההסכמה וכי כאשר מדובר בפגיעה בפרטיות בדרך של עיבוד מידע רגיש, תידרש הסכמה הורית לעיבוד מידע אישי על קטינים מתחת לגיל 16.

8. דרישת קיום המטרה

הרחבנו את העיקרון הקבוע בסעיף 2(9) לחוק הקיים ("עקרון צמידות המטרה"), הקובע כי אין להשתמש במידע אלא למטרה שלשמה נאסף, וקבענו בסעיף נפרד, על דרך החיוב, כי מותר לעבד מידע אישי גם לְמטרה דומה לַמטרה שלשמה נאסף המידע האישי מלכתחילה, מתוך אימוץ הסדר דומה לזה שב-GDPR. הטעם לקביעה שלנו הוא שלא תמיד אפשר לצפות מראש ובמדויק את טווח המטרות של עיבוד המידע האישי שנאסף. אנו מבינים גם את הצורך של תעשיית עיבוד המידע האישי לאפשר לעצמה מרחב פעולה להתפתחות ולחדשנות.

9. חיזוק אגד זכויות השליטה במידע אישי

הצעת החוק כוללת רשימה של זכויות שאינן קיימות במתכונת זהה בחוק הקיים ושתכליתן חיזוק שליטתם של נושאי מידע במידע האישי עליהם.

זכויות אלו הן:

(א) הרחבת זכות העיון במידע אישי כך שתכלול, נוסף על העיון במידע האישי עצמו, את האפשרות לדעת מה מקור המידע האישי אם לא נאסף מנושא המידע עצמו, מה מטרת עיבוד המידע האישי ולמי הוא נמסר. בד בבד התרנו בהצעה לסרב לבקשת עיון לא רק במקרים של חשש מגרימת נזק בריאותי או נפשי, אלא גם במקרים של פגיעה בחיי אדם או פגיעה קשה בזכויות צד שלישי.

(ב) הוספת הזכות לקבל הסבר כאשר עיבוד המידע האישי נעשה ברובו באמצעים אוטומטיים וכאשר יש להחלטה המתקבלת בעקבות עיבוד המידע האישי כאמור השלכה משמעותית על זכות או חובה של נושא המידע לפי

vii הצעת חוק הגנת הפרטיות (תיקון – הגנת על פרטיות של קטינים), התשע"ז–2017 (להלן: "**הצ"ח פרטיות קטינים**").

דין – כדי לאפשר ביקורת על הליכי קבלת החלטות המתבצעים על ידי מכונות ובדיקה נוספת של ההטיות שהם עשויים לגלם.

(ג) הוספת הזכות לניוד מידע אישי, שכזכות כלכלית במהותה משמעה היכולת להעביר צבירי נתונים שיש בהם מידע אישי לפלטפורמות עיבוד מידע נוספות בלי שיהיה צריך להשקיע בכך משאבים או מאמץ מחודש.

(ד) הוספת הזכות להישכח, שהיא למעשה הזכות למחיקת מידע ועניינה יכולתו של נושא מידע לדרוש את מחיקת המידע עליו אם חזר בו מהסכמתו או אם התברר שהעיבוד נעשה בניגוד למטרה שלשמה נאסף או בניגוד לחוק.

(ה) הרחבת החובה למתן ההודעה לנושאי מידע בעניין זכויותיהם, פירוט הנושאים שיש לכלול בהודעה ומידת הנחיצות של העיבוד להגשמת המטרה, וכן הפרטים ליצירת קשר עם המבקש לעבד את המידע.

10. הרחבת החובות של בעל השליטה במידע או של המעבד, לפי העניין

הרחבת החובות של בעל שליטה במידע או של המעבד, לפי העניין, בכל הנוגע להגנת הפרטיות במידע אישי שאותו הם מעבדים ולאבטחת המידע האישי הנמצא ברשותם.

חובות אלה כוללות, בין השאר:

(א) אימוץ התקנות לאבטחת מידע שנכנסו לתוקף במאי 2018 אל תוך דבר החקיקה הראשי כאמירה ערכית המכירה בחשיבותן להגנה על מידע אישי בעולם דיגיטלי. עם זאת, לא אימצנו את המודל שנמצא בתקנות, המבחין בין רמות אבטחת מידע בינונית וגבוהה לפי מספר נושאי המידע במאגר המידע. בעתיד נפעל להצעת תיקון לתקנות אבטחת מידע לפי המוצע בהצעת חוק זו. ואולם לעת עתה, כדי שנוכל להציג את התמונה המלאה של מכלול התיקונים המוצעים, בחרנו להציג את התיקונים כחלק מהצעת החוק.

(ב) שילוב הוראות לעניין אבטחת מידע ברוח תקנות אבטחת המידע החדשות, התיקון לחוק הגנת הפרטיות באוסטרליה וה-GDPR, הכוללות: חובת תיעוד אירועי אבטחה ודיווח עליהם; חובת הכנת תסקיר השפעה על פרטיות במקרים שקבענו; מינוי ממונה על הגנת הפרטיות בחברה העוסקת בעיבוד מידע אישי.

(ג) עיצוב לפרטיות ("privacy by design"): הוספה לחובותיו של בעל שליטה במידע את החובה להבטיח הטמעת אמצעי הגנה על פרטיות במידע אישי כבר משלבי התכנון והפיתוח של המערכות לעיבוד מידע אישי, ואחר כך בשלבי הטמעתן והפעלתן – כל אלו על ידי אימוץ דרישות "פרטיות כברירת מחדל" ("privacy by default") ו"עיצוב לפרטיות" ("privacy by design"), בדומה לקָבוע ב-GDPR.

11. תחולה חוץ-טריטוריאלית

בעולם דיגיטלי שבו חברות רב-לאומיות מעבדות מידע אישי על נושאי מידע הנמצאים בישראל וחברות שנמצאות בישראל מעבדות מידע אישי על מי שנמצאים מחוץ לישראל, הכרחי לקבוע הסדרים חוץ-טריטוריאליים להגנה על הפרטיות. הוספנו הסדר הקובע כי הוראות החוק יחולו על כל מי שמאוגד או פועל בישראל ומעבד מידע אישי. ההוראות יחולו גם על עיבוד מידע אישי על נושא מידע שנמצא במדינת ישראל על ידי חברות שנמצאות גם מחוץ לישראל, בדומה להוראות ב-GDPR.

12. חיזוק הרשות להגנת הפרטיות

ברמה המוסדית הצענו לחזק את הרשות להגנת הפרטיות ולהפוך אותה לגוף חקירה ואכיפה עצמאי שיהיה אחראי על תקציבו ועל גיוס עובדיו, בדומה לרשות להגבלים עסקיים ולרשות להגנת הצרכן ולסחר הוגן.

(א) קבענו רשימה ברורה של תפקידי הרשות, בדומה לקבוע בחוק הגנת הצרכן.

(ב) הצענו להטמיע את ההסדרים המוצעים בהצ"ח תיקון מס' 13 לחוק הגנת הפרטיות שהוגש לכנסת ה-20 ולכלול בחוק המוצע את סמכויות האכיפה המינהלית הקיימות בהצ"ח תיקון מס' 13. עם זאת, לא הטמענו את הוראות הצ"ח תיקון מס' 13 כלשונן אלא התאמנו את ההסדרים המוצעים בתיקון להצעת החוק שלנו ולהוראות בדבר סמכות האכיפה המינהלית הקבועות בחוק הגנת הצרכן, התשמ"א–1981. הוראות אלו מייצגות את המסגרת המשפטית החקיקתית העדכנית בנושא זה, וחשוב לדעתנו לשמור על אחידות בדברי החקיקה המעניקים סמכות אכיפה מינהלית לרשות ציבורית.

(ג) הצענו להרחיב את סמכויות החקירה של הרשות להגנת הפרטיות כך שיכללו גם חקירת עבירות נלוות, בדומה לסמכות הנתונה כיום בידי רשות ההגבלים העסקיים.

(ד) קבענו הוראות לשיתוף פעולה עם רשויות חוץ למטרות חקירה ואכיפה, בדומה לקבוע בחוק ניירות ערך – מתוך הכרה בכך שלנוכח האופי הבינלאומי והגלובלי של עיבוד מידע אישי, שיתוף פעולה מסוג זה יהיה הכרחי לאכיפת ההגנה על הזכות לפרטיות.

(ה) הצענו לבטל את המועצה הציבורית הקיימת לפי החוק הקיים, שהיא חסרה כל סמכויות אופרטיביות, ולהקים במקומה ועדה מייעצת לרשות להגנת הפרטיות, בדומה לזו הקבועה בחוק הגנת הצרכן.

(ו) הצענו להוסיף אפשרות ערעור לבית משפט לעניינים מינהליים על כל החלטה של הרשות להגנת הפרטיות.

13. חידוד המשמעויות הנזיקיות והפליליות של החוק

קבענו כי אחריות נזיקית ופלילית תחול רק על הפרת הוראות ספציפיות בחוק.

(א) בחוק הקיים אחריות נזיקית קיימת רק במקרה של פגיעה בפרטיות, ואילו כאן הצענו להרחיבה להוראות הנוגעות לפגיעה בפרטיות, לחובת הודעה ולכלל זכויות נושאי המידע ואופן מימושן.

(ב) אחריות פלילית תחול על כל הפרה של סעיף 4 (פגיעה בפרטיות). מכיוון שהגדרנו את הפגיעה בפרטיות בניסוח מהודק והגיוני יותר מזה שברשימת הפגיעות בפרטיות שבסעיף 2 לחוק הקיים, לא היה צורך להחריג חלק מסעיפי המשנה מן האחריות הפלילית.

(ג) החמרנו את הענישה הפלילית והנזיקית במקרה שהעבירה נעברה או הייתה מכוונת כלפי קטין, קשיש או חסר ישע.

(ד) הוספנו שיקולים לקביעת גובה הפיצוי.

14. סעיף ההגנות

(א) קבענו כי ההגנות יחולו בכל הליך משפטי או משמעתי ולא רק בהליך פלילי או אזרחי – כדי לאפשר פרשנות קוהרנטית של החקיקה.

(ב) הוספנו הגנה כאשר עיבוד מידע נדרש לצורך מילוי חובה על פי דין.

(ג) הותרנו על כנן את ההגנה של פרסום לפי חוק איסור לשון הרע ואת הגנת תום הלב והעניין לציבור – כדי להגן על האפשרות לממש תפקוד של עיתונות חוקרת ופרסום מידע שיש לו ערך ציבורי וחדשותי.

15. ביטול הפטור הגורף מאחריות על פגיעה בפרטיות שנגרמת על ידי כוחות הביטחון

השימוש הגובר בטכנולוגיות למטרות מעקב, אכיפת חוק ומלחמה בפשיעה באמצעות ניתוח מידע אישי בשילוב עם נתוני עתק מגביר את הסכנה לפגיעה חמורה ובהיקף רחב בזכות לפרטיות על ידי גורמי ביטחון ואכיפת חוק. לפיכך חשבנו שלא נכון להסתפק בסעיף המתיר פגיעה בפרטיות על ידי רשות ביטחון על פי המבחן המוצע בסעיף 19(ב) לחוק הגנת הפרטיות הקיים – מבחן סבירות כל עוד הפגיעה נעשית במסגרת התפקיד ולשם מילויו. זאת ועוד, מאז חקיקת סעיף 19(ב) בשנת 1981 עוגנה הזכות לפרטיות כאחת מזכויות היסוד החוקתיות בחוק-יסוד: כבוד האדם וחירותו, ולכן אנו סבורים כי אין להתיר היום פגיעה בחוק בזכות לפרטיות באופן שאינו עומד בדרישות פסקת ההגבלה. יתרה מזו, הענקת סמכות מעקב ופגיעה גורפת בפרטיות לרשויות ביטחון עלולה להפוך לאבן נגף בפני הכרה אירופית (adequacy) בכך שרמת ההגנה על הפרטיות בדין הישראלי תואמת את זו האירופית.[viii] משום כך הצענו למחוק את הפטור הקיים לרשות ביטחון בהצעת החוק. בחרנו בשלב זה שלא לקבוע הסדר מקיף אלא להציע לקבוע הסמכה מפורשת ומידתית בחוק ייעודי. החוק הייעודי יעסוק בשימוש בטכנולוגיות הפוגעות בפרטיות לשם אכיפת חוק, מעקב ומניעת פשיעה.

הערות נוספות

(א) נדרשת עבודה נוספת כדי לסרוק את כלל החקיקה. מטרת הסריקה תהיה לבחון את הצורך בתיקונים עקיפים בחוקים נוספים שבהם יש הפניה לחוק הקיים או הסתמכות עליו.

(ב) מוצע לקבוע בהצעת החוק סעיף תחילה שלפיו החוק ייכנס לתוקף בחלוף שנה מקבלתו. פרק זמן זה מספיק לדעתנו כתקופת היערכות לשינויים המוצעים בחוק, בעיקר לאור ההלימה הרבה עם ה-GDPR. תאגידים וארגונים שמצייתים כבר עתה

viii סמכות המעקב והפגיעה הגורפת בפרטיות על ידי ה-NSA בארצות ברית, כפי שנתגלה מהמסמכים שחשף אדוארד סנאודן, הייתה הסיבה העיקרית לביטול ה-safe harbor, בארצות הברית (*Maximillian Schrems v. Data Protection Commissioner*, Case C–362/14, 6 October 2015, ECLI:EU:C:2015:650), ודיונים על ההכרה בתאימות הדין ביפן ובאנגליה עסקו בסמכות המעקב הניתנת לרשויות הביטחון בכל אחת מן המדינות. ראו Andrew D. Murray, *Data Transfers between the EU and UK Post Brexit?*, 7 (3) INTERNATIONAL DATA PRIVACY LAW 149 (2017); Claude Moraes, Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection of personal data afforded by Japan (2018/2979 (RSP))

משיקולים שונים ל-GDPR לא יידרשו לשנות בהרבה את מדיניות הגנת הפרטיות שהם נוקטים.

(ג) בצד סעיף התחילה יהיה צורך בהוספת סעיף הוראות מעבר. הסעיף החדש יכלול הוראות נדרשות בתקופת המעבר מההסדר הישן להסדר החדש לפי הצעת החוק.

עו"ד רחל ארידור הרשקוביץ, המכון הישראלי לדמוקרטיה

ד"ר תהילה שוורץ אלטשולר, המכון הישראלי לדמוקרטיה

חברות וחברי קבוצת המומחים:

פרופ' בירנהק מיכאל, סגן דיקן למחקר, הפקולטה למשפטים, אוניברסיטת תל אביב

גולדפוס יובל, דוקטורנט, המחלקה לפילוסופיה, האוניברסיטה העברית בירושלים

עו"ד הכהן יורם, מנכ"ל איגוד האינטרנט הישראלי

עו"ד חי דן, משרד עורכי דין דן חי ושות'

עו"ד ליבליך טל, משרד עורכי דין ליבליך מוזר ושות'

עו"ד פודמסקי אורית, יו"ר המועצה להגנת הפרטיות, משרד המשפטים

עו"ד פינצ'וק אבנר, האגודה לזכויות האזרח

עו"ד קלינגר יהונתן, משרד עורכי דין יהונתן קלינגר והיועץ המשפטי של התנועה לזכויות דיגיטליות

עו"ד רביה חיים, משרד עורכי דין פרל כהן צדק לצר ברץ ושות'

השתתפו כמשקיפים:

עו"ד בסמן ריינגולד גילי, היועצת המשפטית של הרשות להגנת הפרטיות, משרד המשפטים

עו"ד גרסון ניר, ממונה משפט וטכנולוגיה, הרשות להגנת הפרטיות, משרד המשפטים

השתתפו חלקית:

עו"ד שחורי אחיעד, סגן היועץ המשפטי של בנק לאומי

שיר ערן, מנכ"ל נקסאר

עריכה לשונית של סעיפי הצעת החוק: עו"ד שריל קמפינסקי.

יוני, 2019

הצעת חוק הגנת הפרטיות, התשע"ט–2019
ודברי הסבר מפורטים

תוכן העניינים

פרק א: מטרה, פרשנות ועקרונות יסוד 27

סעיף 1: מטרת החוק 27

סעיף 2: הגדרות 29

סעיף 3: איסור פגיעה בפרטיות 41

סעיף 4: פגיעה בפרטיות 42

סעיף 5: פרסום תצלומו של נפטר 42

פרק ב: הגנה על הפרטיות במידע אישי 45

סימן א׳: הוראות כלליות לעניין עיבוד מידע אישי 45

סעיף 6: פגיעה מותרת בפרטיות 45

סעיף 7: דרישת קיום המטרה 51

סעיף 8: הסכמה לעניין פגיעה בפרטיותו של קטין 53

סעיף 9: חובת מתן הודעה 56

סימן ב׳: זכויות נושא המידע 61

סעיף 10: זכות החזרה מהסכמה 61

סעיף 11: זכות עיון במידע אישי 63

סעיף 12: זכות לקבל הסבר 69

סעיף 13: זכות תיקון מידע אישי 72

סעיף 14: הזכות לניוד מידע אישי 75

סעיף 15: זכות המחיקה של מידע אישי 78

סעיף 16: מימוש זכויות נושא המידע 83

סעיף 17: תובענה לבית המשפט 83

סימן ג׳: חובות בעל השליטה במידע והמעבד 85

סעיף 18: מעבד המידע 87

סעיף 19: עיצוב לפרטיות 89

סעיף 20: תסקיר השפעה על הפרטיות 91

סעיף 21: אבטחת מידע אישי 96
סעיף 22: תיעוד ודיווח על אודות אירוע אבטחה 99
סעיף 23: ממונה על הגנת הפרטיות במידע 106

סימן ד': שונות 110

סעיף 24: תחולת הוראות פרק ב' 110
סעיף 25: נציגות בעל שליטה במידע או מעבד בישראל 113

פרק ג: הרשות להגנת הפרטיות וסמכויות פיקוח, אכיפה ובירור מינהלי 114

סימן א': הרשות להגנת הפרטיות 114

סעיף 26: ראש הרשות להגנת הפרטיות 114
סעיף 27: תקציב הרשות 114
סעיף 28: עסקאות הרשות 114
סעיף 29: עובדי הרשות להגנת הפרטיות 114
סעיף 30: תפקידי הרשות להגנת הפרטיות 116
סעיף 31: שיתוף פעולה עם רשות חוץ 118
סעיף 32: הוועדה המייעצת 122
סעיף 33: הסמכת חוקר או מפקח 124

סימן ב': סמכויות פיקוח 126

סעיף 34: סמכויות מפקח 126

סימן ג': סמכויות בבירור מינהלי 126

סעיף 35: צו לחיפוש ולחדירה לחומר מחשב 126
סעיף 36: אופן ביצוע חדירה לחומר מחשב והעתקתו 126
סעיף 37: סמכויות אכיפה, חקירה, עיכוב ותפיסה 127

פרק ד: אמצעי אכיפה מינהליים 130

סימן א': עיצום כספי 130

סעיף 38: עיצום כספי 130
סעיף 39: הפרה בנסיבות מחמירות 134
סעיף 40: הודעה על כוונת חיוב 135

סעיף 41: זכות טיעון 135
סעיף 42: החלטת ראש הרשות להגנת הפרטיות ודרישת תשלום 135
סעיף 43: הפרה נמשכת והפרה חוזרת 136
סעיף 44: סכומים מופחתים 136
סעיף 45: סכום מעודכן של הפיצוי הכספי 136
סעיף 46: המועד לתשלום העיצום הכספי 136
סעיף 47: הפרשי ריבית והצמדה 136
סעיף 48: גבייה 136

סימן ב': התראה מינהלית 137

סעיף 49: התראה מינהלית 137
סעיף 50: בקשה לביטול התראה מינהלית 137
סעיף 51: הפרה נמשכת והפרה חוזרת לאחר התראה 137

סימן ג': התחייבות להימנע מהפרה 139

סעיף 52: התחייבות להימנע מהפרה והפקדת עירבון 139
סעיף 53: תוצאות הגשת כתב התחייבות ועירבון או אי הגשתם 139
סעיף 54: הפרת התחייבות 139
סעיף 55: השבת העירבון 140

סימן ד': הוראות כלליות 140

סעיף 56: עיצום כספי בשל הפרה לפי חוק זה ולפי חוק אחר 140
סעיף 57: פרסום לעניין הטלת עיצום כספי 142
סעיף 58: שמירת אחריות פלילית 144
סעיף 59: אישור נהלים ופרסומם 144
סעיף 60: אצילת סמכויות 144

פרק ה: מסירת מידע אישי או ידיעות מאת גופים ציבוריים 146

פרק ו: עוולה אזרחית ועונשין 146

סעיף 61: פגיעה בפרטיות – עוולה אזרחית 146
סעיף 62: פגיעה בפרטיות – עבירה 146
סעיף 63: פיצוי בלא הוכחת נזק 149
סעיף 64: שיקולים בגזירת הדין או גובה הפיצוי 149

פרק ז: הגנות 151

סעיף 65: הגנות מה הן 151

סעיף 66: פטור 155

סעיף 67: הפרכה של טענות הגנה 155

פרק ח: הוראות שונות 156

סעיף 68: דין המדינה 156

סעיף 69: מות הנפגע 156

סעיף 70: סייג לפרסום הליכים 156

סעיף 71: דין שני משפטים 156

סעיף 72: צווים נוספים 156

סעיף 73: חומר פסול לראיה 156

סעיף 74: דו"ח הגנה על הפרטיות 156

סעיף 75: תיקון חוק בתי משפט לענינים מינהליים 156

סעיף 76: שמירת דינים 157

סעיף 77: ביצוע ותקנות 157

סעיף 78: התאמה למדד 157

פרק א: מטרה, פרשנות ועקרונות יסוד

סעיף 1: מטרת החוק

חוק זה מטרתו להגן על פרטיותו של אדם, לשם מימוש האוטונומיה של הפרט, ובכלל זה מתן הגנה על המרחב האישי של אדם, צנעת חייו האישיים, סוד שיחו, וזכותו לשלוט במידע אישי על אודותיו ובעיבודו; לשם הבטחת קיומו של הליך דמוקרטי תקין, ולשם מניעת השפעה בלתי הוגנת המבוססת על עיבוד מידע אישי על אודותיו.

דברי הסבר

<u>סעיף 1:</u> מטרת הסעיף לקדם את ההגנה על פרטיותו של אדם, שהיא זכות אדם חוקתית המעוגנת בחוק-יסוד: כבוד האדם וחירותו.[1]

התפיסה המרכזית בתאוריה של פרטיות היא תפיסת הפרטיות כשליטה: יכולתו של אדם לשלוט במידע אישי עליו.[2] ואולם זו אינה תפיסת הפרטיות היחידה העומדת בבסיס הצעת החוק. בבסיס הצעת החוק עומדת גם התפיסה הרואה בהגנה על הפרטיות תנאי מוקדם למימושו של הליך דמוקרטי תקין.

זאת ועוד, תפיסת הפרטיות כשליטה מתמקדת בקבלת הסכמה מדעת של נושא המידע לכל שימוש שנעשה במידע אישי עליו. ברם בעידן שבו מידע הוא משאב שנעשה בו שימוש למטרות שאת מרביתן לא ניתן לצפות או לתמצת לרשימה מובנית, אי-אפשר לקבל הסכמה מדעת מראש על כל שימוש.

נוסף על כך, תופעת "פרדוקס הפרטיות" מלמדת על פער בין הצהרות משתמשים על החשיבות שהם מייחסים לפרטיותם לבין התנהגותם הלכה למעשה. למשל, בצד הצהרות המשתמשים שהם אינם מעוניינים שגוף כלשהו יחזיק במידע אישי המאפשר יצירת פרופיל אישי (פרופיילינג) עליהם, מחשש פן תיפגע פרטיותם, הם נכונים לוותר עליה כדי ליהנות משירותים המבוססים על המיקום הגאוגרפי שלהם, מהנחות לחברי מועדון ברשתות מסחריות ומפעילות ברשתות החברתיות. פרדוקס הפרטיות מקשה גם על הערכה כלכלית של שווי המידע האישי בעיני המשתמשים עצמם. כתוצאה מכך קובעי מדיניות מתקשים לקבוע מהו היקף ההגנה הראוי לַזכות לפרטיות ומהו האיזון הראוי בין הזכות לפרטיות לבין היעילות הכלכלית שבגילוי מידע אישי והתרת השימוש בו.

ההתפתחות של מערכות בינה מלאכותית מאפשרת שימוש במידע אישי כדי לנתח את אופיו של אדם ולסרטט פרופיל אישי שלו על מנת לקבל החלטות במקומו. מדובר בהחלטות הנוגעות להמלצות צרכניות והתנהגותיות (למשל, מערכות המלצת קנייה באמזון, המלצות צפייה בנטפליקס ומערכות הכוונת נהיגה כמו waze) ואפילו בהחלטה למי להצביע בבחירות. המידע שאדם מוסר עשוי לשמש אחרים גם בלא שיֵדע על כך לניתוח ולהבנת מצבו הבריאותי והנפשי. המשמעות היא שבמסירת מידע אישי נושא מידע מוותר במודע לא רק על הנתונים עליו אלא גם על חלק מתהליכי קבלת ההחלטות לטובת מערכות שיודעות להחליט במקומו (מה כדאי לאכול ולקנות ומאיפה כדאי לנסוע). בכך הוא הופך להיות חשוף למהלכי שכנוע אישיים ותפורים לפי מידה – בעוצמה, בחודרנות וביכולות שלא היו קיימות בעבר.

לכל זה יש השפעות לא רק במישור המסחרי, אלא גם במישור של מימוש הליך הבחירה כחלק בלתי נפרד מן המשטר הדמוקרטי. טכניקות של איסוף מידע אישי לטובת הצעת מוצרים ושירותים עשויות לשמש גם להשפעה על רעיונות וליצירת "מלכודות על אוטונומיה" על אמונות והשפעה על אמון במוסדות דמוקרטיים – או, בפשטות, הנדסת בחירות. פרשת **קיימברידג' אנליטיקה** באביב 2018, שפתחה את תהליך החשיפה של פרקטיקות לניצול

מידע אישי לצורך השפעה על קמפיינים של בחירות במדינות רבות, מלמדת שהזכות לפרטיות גדולה בהרבה משליטה אישית במידע ונוגעת למעשה באיום על עצם קיומה של היכולת לממש הליך דמוקרטי תקין, ומכאן גם להגן על זכויות האדם כולן.

בשל כך אנו מציעים להבהיר בסעיף המטרה שהזכות לפרטיות היא זכות רחבה אשר לא כל מופעיה מוגדרים במפורש בהצעת החוק. מדובר ברשימה פתוחה של אפשרויות לפגיעה בפרטיות שנעה בין מניעת פגיעה בבחירה חופשית והבטחת הליך דמוקרטי תקין ובין הגנה על מרחב שבתוכו אדם זכאי להיות עם עצמו ואשר זכותו לשלוט בתחומו במידע האישי עליו ובעיבודו.[3] כמו כן אנו מציעים להכיר בסעיף המטרה בכך שהזכות לפרטיות יחסית ולא מוחלטת, ככל זכות אדם אחרת. משום כך תיתכן פגיעה בזכות לפרטיות אבל רק בתנאי שהיא תיעשה בהתאם לדרישות פסקת ההגבלה הקבועה בסעיף 8 לחוק-יסוד: כבוד האדם וחירותו ובהתאם להוראות הצעת החוק.

<u>**החוקים שלהלן שימשו השראה לסעיף:**</u>

סעיף 3 לחוקי הפרטיות הקנדי (PIPEDA :(Privacy Act, §3 ;§3

"3. the purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

סעיף 2A לחוק הפרטיות האוסטרלי :(Privacy Act 1988, §2A)

"2A Objects of this Act
The objects of this Act are: to promote the protection of the privacy of individuals; and to recognize that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities; and to provide the basis for nationally consistent regulation of privacy and the handling of personal information; and to promote responsible and transparent handling of personal information by entities; and to facilitate an efficient credit reporting system while ensuring that privacy of individuals is respected; and to facilitate free flow of information across national borders while ensuring that the privacy of individuals is respected; and to provide a means for individuals to complain about an alleged interference with their privacy; and to implement Australia's international obligation in relation to privacy."

סעיף 1 ל-GDPR:

"1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."

סעיף 2:
הגדרות

בחוק זה –

"**אבטחת מידע אישי**" - הגנה על נכונות המידע האישי, סודיותו, זמינותו או שלמותו;

"**אדם**" – לעניין סעיף 1, ההגדרות "חסר ישע", "מידע אישי", "מידע רגיש", "נושא מידע", "קטין" ו-"קשיש" שבסעיף 2, וסעיפים 4, 9, 11, 23(ה), 63(ג), 65(א)(3)(ה), (65)(א)(3)(ז), 69 ו-70 – למעט תאגיד;

"**אירוע אבטחה**" – אירוע שבו נפגעה אבטחת מידע אישי;

"**בעל שליטה במידע**" – אדם הקובע, לבד או ביחד עם אחר, את המטרות והדרכים לעיבוד מידע אישי;

"**בקשה לסיוע**" – בקשה לסיוע לרשות חוץ שהוגשה בכתב לרשות להגנת הפרטיות על ידי רשות חוץ;

"**גוף ציבורי**" –

(1) משרדי הממשלה ומוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין;

(2) גוף אחר ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, ובלבד שבצו ייקבעו סוגי המידע האישי והידיעות שהגוף יהיה רשאי למסור ולקבל;

"**דיני הגנת הפרטיות**" – דינים בתחום הגנת הפרטיות ופרטיות במידע שהרשות להגנת הפרטיות או רשות חוץ מופקדת על ביצועם ואכיפתם, ולעניין זה, משמעותם של מונחים בדיני הגנת הפרטיות במדינת חוץ תהא כמשמעותם בדין שבתחום סמכותה של רשות החוץ;

דברי הסבר

<u>סעיף 2:</u> הגדרת "**אבטחת מידע אישי**" מבוססת על הגדרת המונח בסעיף 7 לחוק הגנת הפרטיות הקיים הקובע כך:

"אבטחת מידע – הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין."

בנוסף, מוצע לכלול בהגדרה את מודל אבטחת המידע המקובל בעולם ובתעשייה והמבוסס על המשולש CIA (Confidentiality, Integrity, Availability): סודיות, נכונות, זמינות המידע האישי. כך יתאים נוסח הצעת החוק לתובנות המקובלות בכל העולם באשר לאבטחת מידע ולשמירה על הפרטיות. סודיות, נכונות וזמינות המידע נדרשות כדי לוודא שהגישה אל המידע האישי תוגבל למי שמורשה לכך.

הגדרת "**אדם**" תואמת את ההגדרה בסעיף 3 לחוק הגנת הפרטיות הקיים, המבחינה, בדומה להבחנה גם ב-GDPR, כפי שמוסבר בסעיף 14 להקדמה ל-GDPR, בין אדם (natural person) לבין כל ישות משפטית (legal person) הכוללת תאגיד. לפיכך סומנו הסעיפים הרלוונטיים שבהם תאגיד אינו נכלל בהגדרת אדם.

סעיף 14 להקדמה ל-GDPR:

"The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person."

הגדרת "**אירוע אבטחה**" מבוססת על הגדרת "**אבטחת מידע אישי**" ונועדה להדגיש שאירוע אבטחה הוא כל פגיעה במודל CIA של אבטחת המידע. ההגדרה

מותירה מקום לתוספת של מדרג אירועי אבטחה, בדומה לַקָבוּע בתקנות אבטחת מידע.

הגדרת "**בעל שליטה במידע**" באה במקום הגדרת "מנהל מאגר מידע" בסעיף 7 לחוק הגנת הפרטיות הקיים, הקובע כך:

"מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה;"

ההגדרה המוצעת מבוססת על סעיף 4(7) ל-GDPR במטרה להגביר את תאימות הצעת החוק ל-GDPR. המודל הקבוע ב-GDPR מטיל חובות מסוימות על בעלי התפקידים "בעל שליטה במידע" ו"מעבד".

סעיף 4(7) ל-GDPR:

"(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;"

הגדרת "**בקשה לסיוע**" מבוססת על הגדרת המונח בסעיף 54יא1 לחוק ניירות ערך, התשכ"ח–1968, הקובע כך:

"בקשה לסיוע – בקשה לסיוע שהוגשה בכתב לרשות על ידי רשות חוץ בהתאם למזכר הבנה;"

ההגדרה בהצעת החוק אינה מתייחסת ל"מזכר הבנה", שכן שיתוף המידע האישי הגנת הפרטיות לבין רשות חוץ אינו מותנה בחתימה על מזכר הבנות לפי סעיף 31 להצעת החוק.

הגדרת "**גוף ציבורי**" זהה להגדרה המופיעה בסעיף 23 לחוק הגנת הפרטיות הקיים.

הגדרת "**דיני הגנת הפרטיות**" מבוססת על הגדרת המונח בסעיף 54יא1 לחוק ניירות ערך, התשכ"ח–1968, והתאמתו להצעת החוק.

"דיני ניירות ערך – דינים בתחום ניירות ערך שהרשות או רשות חוץ מופקדת על ביצועם ואכיפתם."

"הסכמה" - הסכמה מדעת ומרצון חופשי, במפורש או מכללא;

"חוק המחשבים" – חוק המחשבים, התשנ"ה–1995;[4]

"חוק המעצרים" – חוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו–1996;[5]

"חוקר" ו"**מפקח**" – מי שהוסמך לכך לפי סעיף 33;

"חומר מחשב" ו"**מחשב**" – כהגדרתם בחוק המחשבים;

"חסר ישע" – אדם שמחמת מחלתו, ליקויו הרוחני, מעצרו או כל סיבה אחרת אינו יכול לספק לעצמו את צרכי חייו;

"חפץ" – כהגדרתו בפקודת המעצר והחיפוש;

דברי הסבר

הגדרת "**הסכמה**" בהצעת החוק מבוססת על הגדרת המונח בסעיף 3 לחוק הגנת הפרטיות הקיים, הקובע כך:

"הסכמה מדעת, במפורש או מכללא;"

הצעת החוק מוסיפה על ההגדרה בחוק הגנת הפרטיות הקיים את דרישת ה"רצון החופשי" כתנאי לתקפות ההסכמה. תכליתה של תוספת זו היא לחזק את דרישת ההסכמה כדרישה אפקטיבית ולצמצם את השימוש הגובר בהסכמה כדרישה צורנית בלבד. עם זאת, ההגדרה מאפשרת לבית המשפט מרחב תמרון באמצעות המונחים "מדעת" ובאמצעות ההכרה גם בהסכמה מכללא.

קבוצת המומחים התלבטה אם יש מקום להחמיר את דרישת ההסכמה ולהבהיר, בדומה לסעיף 4(11) ל-GDPR, שההסכמה לפגיעה בפרטיות צריכה להיות חד-משמעית ולהתקבל רק לאחר שנושא המידע יָדע והבין, או סביר היה שידע והבין, את מידת הפגיעה בפרטיותו ואת מטרותיה. לבסוף הוחלט שאין מקום להחמיר את דרישת ההסכמה באופן זה אלא יש ליצור הבנה שהסכמה אינה חזות הכול. הדבר נעשה באמצעות הוספת הביטוי "מרצון חופשי", הגדרת בסיסים לגיטימיים לפגיעה בפרטיות נוסף על ההסכמה ואימוץ זכות החֲזרה מהסכמה בסעיפים 6 ו-10 להצעת החוק. מובהר שיש לפרש את המונח "מרצון חופשי" כתנאי לתקפות ההסכמה; כלומר כמחייב שההסכמה ניתנה לאחר שנושא המידע יָדע והבין, או סביר היה שידע והבין, את מטרת הפגיעה בפרטיותו, את מידת הפגיעה, את הסיכונים הכרוכים בה ואת האפשרויות העומדות לפניו ונתן את הסכמתו מרצונו החופשי. פרשנות זו גם עולה בקנה אחד עם תנאיה של דרישת ההסכמה ב-GDPR.

סעיפים 4(11) ו-7 ל-GDPR:

"4(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;"

"Article 7 Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

סעיף 4(7) ל-GDPR - המשך

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

ההגדרות "**חוק המחשבים**", "**חומר מחשב**" ו"**חפץ**" זהות להגדרות בסעיף 23ט להצ"ח תיקון מס' 13.[6]

הגדרת "**חסר ישע**" מבוססת על סעיף 322 לחוק העונשין, התשל"ז–1977: "מי שעליו האחריות לאדם שמחמת גילו, מחלתו, ליקויו הרוחני, מעצרו או כל סיבה אחרת אינו יכול להפקיע עצמו מאותה אחריות ואינו יכול לספק לעצמו את צרכיי חייו – בין שהאחריות מקורה בחוזה או בדין ובין שנוצרה מחמת מעשה כשר או אסור של האחראי – חובה עליו לספק לו את צרכי מחייתו ולדאוג לבריאותו, ויראוהו כמי שגרם לתוצאות שבאו על חייו או על בריאותו של האדם מחמת שלא קיים את חובתו האמורה."

"מידע אישי" – נתונים על אודות אדם מזוהה, לרבות נתונים המאפשרים במאמץ סביר את זיהויו של אדם;

"מידע אישי מדגמי" – מידע אישי אקראי שבעל שליטה במידע ביצע או מבצע בו פעולות עיבוד.

דברי הסבר

הגדרת **"מידע אישי"** מחליפה את הגדרת "מידע" בסעיף 7 לחוק הגנת הפרטיות הקיים, הקובע כך:

"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו;"

ההגדרה המוצעת מאמצת את מסקנות ועדת שופמן[7] ואת הגדרת "מידע מזוהה" בחוק נתוני אשראי, התשע"ו-2016. ההגדרה גם מבקשת ליצור תאימות עם סעיף 4(1) ל-GDPR ואף מוכּרת בחקיקה ההשוואתית (למשל, סעיף 2(1) לחוק הפרטיות הקנדי (PIPEDA) וסעיף 6(1) לחוק הפרטיות האוסטרלי).

ההגדרה מתייחסת לנתונים בלי קשר לפורמט שהם מוצגים בו וכוללת נתונים מזהים, כמו למשל שם פרטי, שם משפחה ומספר זהות, בצד נתונים המאפשרים את זיהויו של אדם מתוך נקיטת פעולות סבירות.

ההגדרה המוצעת קיבלה השראה ממקורות אחדים:

סעיף 2 לחוק נתוני אשראי, התשע"ו–2016:

"מידע מזוהה" – מידע הכולל פרט מזהה של לקוח, או מידע שפרטים מזהים של לקוח הופרדו ממנו אך ניתן במאמץ סביר לזהות את הלקוח שאליו מתייחס המידע.

"פרט מזהה" – שם פרטי, שם משפחה, מספר זהות וכל מידע אחר שיש בו כדי להביא, במישרין או בעקיפין, לזיהוי לקוח מסוים".

סעיף 4(1) ל-GDPR:

"(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

סעיף 2(1) לחוק הפרטיות הקנדי (PIPEDA, §2(1)):

"personal information means information about an identifiable individual."

סעיף 6(1) לחוק הפרטיות האוסטרלי (Privacy Act of 1988, §6(1)):

"personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true of not; and (b) whether the information or opinion is recorded in a material form or not."

הגדרת **"מידע אישי מדגמי"** לקוחה מסעיף 23י להצ"ח תיקון מס' 13. כפי שמוסבר בדברי ההסבר לסעיף 23י להצ"ח תיקון מס' 13, מידע אישי מדגמי הוא עותק מחומר מחשב הכולל שדות אקראיים שמוצג או נמסר לצורך בדיקה מדגמית של המידע האישי המעובד או של אופני הפיקוח, הניהול ואבטחת המידע האישי.

"מידע רגיש" – מידע אישי שיש בו כדי לזהות אחד מאלה:

(1) נתונים על אישיותו של אדם וצנעת חייו האישיים;

(2) נתונים על עברו הפלילי של אדם;

(3) נתונים על דעותיו הפוליטיות ואמונתו הדתית של אדם;

(4) נתונים על מצבו הבריאותי של אדם;

(5) נתוני זיהוי ביומטריים, כהגדרתם בחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע–2009;[8]

(6) מידע גנטי, כהגדרתו בחוק מידע גנטי, התשס"א–2000;[9]

(7) נתונים על מצבו הכלכלי של אדם, לרבות נתוני אשראי כהגדרתם בחוק נתוני אשראי, התשע"ו–2016;[10]

(8) מידע אישי שנקבעה לגביו חובת סודיות בדין;

(9) נתוני תעבורה ונתוני מיקום, כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007,[11] שיש בהם כדי ללמד על אחד מסוגי המידע המנויים בסעיפים קטנים (1)-(8);

(10) מידע אישי ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש.

דברי הסבר

בהגדרת **"מידע רגיש"** אימצנו את התפיסה, שבאה לידי ביטוי בסעיף 9 ל-GDPR, הקובעת שמידע רגיש הוא מידע אישי שיש בו כדי לזהות מידע רגיש. ההגדרה המוצעת כוללת סוגי מידע אישי המופיעים בסעיף 7 לחוק הגנת הפרטיות הקיים, בהגדרת "מידע בעל רגישות מיוחדת", בסעיף 23ביט(א) להצ"ח תיקון מס' 13, וכן סוגי מידע אישי נוספים המופיעים בחקיקה השוואתית מקומית ובינלאומית.

סעיף קטן (1) כולל מידע אישי שיש בו כדי ללמד גם על אישיותו של אדם וגם על נטייתו המינית. בסעיף קטן (3) התלבטו חברי צוות המומחים אם למקד את הגדרת המידע הרגיש לנתונים על אמונותיו הדתיות של אדם או על כל אמונה של אדם באשר היא. לבסוף הוחלט ברוב דעות לצמצם את ההגדרה לנתונים על אמונתו הדתית של אדם.

סעיף קטן (8) קובע שגם מידע אישי אשר קיימת בעניינו חובת סודיות בדין הוא מידע רגיש. אנו מזהים חוסר בהירות לגבי הצורך לקבוע בחקיקה ראשית מהו העיבוד המותר במידע רגיש המוגדר כסודי. לפיכך חוקים שונים המגדירים מידע רגיש כסודי מותירים את השאלה מה אפשר לעשות בו שאלה חסרת מענה ונתונה לפרשנות. כך למשל, בתוכנית הלאומית לבריאות דיגיטלית לא מובהר כי העיבוד של מידע רפואי כפוף להוראות חוק הגנת הפרטיות. התוכנית מדגישה כי יש צורך בהגנה על פרטיות המידע הרפואי שאינו מידע אישי רגיש, אך היא מסתפקת בקביעה כללית שיש צורך באסדרה ושהקו המנחה צריך להיות התממה (אנונימיזציה).[12] התייחסות זו אינה מספיקה בעיקר לנוכח החסרונות הידועים של התממה במתן הגנת פרטיות ראויה.[13] לכן סברנו כי יש צורך בקביעה ברורה שמידע אישי המוגדר כסודי במסגרת החסיונות המקצועיים שהתפתחו בדין הוא מידע רגיש, ועל כן

העיבוד שלו כפוף להוראות הצעת החוק למידע רגיש.

סעיף קטן (9) מפנה לנתוני תעבורה ונתוני מיקום כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007. כשלעצמם אין בנתוני התעבורה כדי להיות מידע רגיש אלא אם הם עלולים ללמד על סוגי מידע המנויים בסעיפים קטנים (1)–(8) להגדרה.

הסעיפים שלהלן היו ההשראה לסעיף:

סעיף 7 לחוק הגנת הפרטיות הקיים:

" "מידע רגיש" –

(1) נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו; (2) מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש;"

סעיף 23ביט(א) להצ"ח תיקון מס' 13:

"מידע בעל רגישות מיוחדת

(1) מידע על צנעת חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד; (2) מידע רפואי או מידע על מצבו הנפשי של אדם; (3) מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א–2000; (4) מידע על אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם; (5) מידע על אודות עברו הפלילי של אדם; (6) נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007; (7) מידע שהוא מאפיין אנושי, פיזיולוגי, ייחודי, הניתן למדידה ממוחשבת, המשמש לזיהוי אדם; (8) מידע על נכסיו של אדם, חובותיו והתחייבויותיו הכלכליות, מצבו הכלכלי או שינוי בו, יכולתו לעמוד בהתחייבויותיו הכלכליות ומידת עמידתו בהן; (9) הרגלי הצריכה של אדם שיש בהם כדי ללמד על מידע לפי פרטים (1) עד (7) או על אישיותו של אדם, אמונתו או דעותיו; (10) מידע נוסף שקבע שר המשפטים, בצו, באישור ועדת חוקה חוק ומשפט של הכנסת."

סעיף 6(1) לחוק הפרטיות האוסטרלי (Privacy Act of 1988, §6(1)):

"(a) sensitive information means:
Information or an opinion about an individual's; racial or ethnic origin; or political opinions; or membership of a political association; or religious beliefs or affiliations; or philosophical beliefs; or membership or a professional or trade association; or membership of a trade union; or sexual orientation or practices; or criminal record; That is also personal information; or (b) Health information about an individual; or (c) Genetic information about an individual that is not otherwise health information; or (d) Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) Biometric templates."

סעיף 9(1) ל-GDPR:

"1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

"מסמך" – לרבות פלט כהגדרתו בחוק המחשבים;

"מעבד" – אדם המורשה על ידי בעל שליטה במידע, לפעול מטעמו בעיבוד של מידע אישי;

"נושא מידע" – אדם שנעשה עיבוד של מידע אישי על אודותיו;

"סיוע לרשות חוץ" – דרישת מידע אישי ומסמכים, עריכת חיפוש, תפיסת מסמכים, ניהול חקירה והעברת מידע אישי ומסמכים, לשם ביצוע ואכיפה של דיני הגנת הפרטיות במדינות חוץ ופיקוח על ביצועם;

דברי הסבר

הגדרת **"מסמך"** זהה להגדרה בסעיף 23ט בהצ"ח תיקון מס' 13.

הגדרת **"מעבד"** מחליפה את ההגדרה בסעיף 3 לחוק הגנת הפרטיות הקיים. היא מבוססת על הגדרת "מעבד" בסעיף 4(8) ל-GDPR.

סעיף 3 לחוק הגנת הפרטיות הקיים:
"מחזיק, לענין מאגר מידע – מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש;".

סעיף 4(א) ל-GDPR:
"(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;"

הנחת היסוד של הצעת החוק היא שאין עוד מקום לחובת רישום מאגרי מידע הקיימת בחוק הגנת הפרטיות הקיים, ולכן גם הגדרת "מאגר מידע" ו"מחזיק" מיותרות.

הגדרת **"נושא מידע"** מבוססת על ההתייחסות ל-"data subject" בסעיף 4(1) ב-GDPR כאל אדם שהמידע בעניינו מזהה או ניתן לזיהוי ("information relating to an identified or identifiable natural person ('data subject')"). התלבטנו אם המונח הנכון הוא "מושא המידע", שכן מדובר במידע על אדם ולא במידע של האדם. לנוכח השימוש שנעשה במונח "נושא המידע" בהנחיות שונות של הרשות להגנת הפרטיות ובעקבות עמדתה של האקדמיה ללשון העברית בנושא החלטנו להשתמש גם אנחנו, בניגוד לעמדתו של פרופ' מיכאל בירנהק, במונח "נושא המידע".

הגדרת **"סיוע לרשות חוץ"** מבוססת על הגדרת המונח בסעיף 54יא1 לחוק ניירות ערך, התשכ"ח–1968, הקובע כך:

"סיוע לרשות חוץ – דרישת ידיעות ומסמכים, עריכת חיפוש, תפיסת מסמכים, ניהול חקירה והעברת ידיעות ומסמכים, לשם ביצוע ואכיפה של דיני ניירות ערך במדינת חוץ ופיקוח על ביצועם;"

"עיבוד" – אחת מהפעולות האלה:

(1) איסוף או תיעוד של מידע אישי בכל דרך, לרבות צילום, הקלטה, העתקה או השגת גישה אליו;

(2) ארגון, החזקה או אחסון של מידע אישי, לרבות הבנייה, שינוי, אחזור, ניתוח, איגום או הצלבה;

(3) גילוי או פרסום של מידע אישי, לרבות העברה, מכירה או העמדה לרשות הציבור;

"פקודת המעצר והחיפוש" – פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט–1969;[14]

"פרסום", לעניין מידע אישי – הבאת מידע אישי לידיעת הציבור בכל דרך;

"קטין" – אדם שטרם מלאו לו שמונה עשרה שנים;

"קשיש" – אדם שמלאו לו 65 שנים.

דברי הסבר

הגדרת **"עיבוד"** מחליפה את הגדרת "שימוש" בסעיף 3 לחוק הגנת הפרטיות הקיים, שאינה מתאימה למכלול הפעולות שאפשר לעשות במידע אישי בעולם דיגיטלי. ההגדרה המוצעת נמצאת בהלימה עם סעיף 4(2) ל-GDPR וכוללת רשימה סגורה של שלושה סוגי פעולות במידע אישי: איסוף, ניתוח והפצה. ההגדרה היא עיוורת למרחב שבו הפעולה מתרחשת, ועל כן גם צילום במרחב הציבורי ייחשב עיבוד של מידע אישי ויעשה בהתאם לדרישות שבהצעת החוק. הגדרה זו מאפשרת הבנה ברורה יותר של סוגי השימושים ומדגישה שמדובר בטיפוסי פעולות שונים. לתפיסתנו, ההגדרה החדשה תקל את יישום החוק בהמשך, ולכן היא עדיפה מהגדרה רחבה וכוללנית.

סברנו כי אם הליבה של תפיסת הפרטיות היא שליטתו של האדם במידע האישי עליו, אין משמעות לזהות של מבצע השימוש במידע האישי. משום כך השאלה אם השימוש נעשה על ידי אדם או מכונה אינה רלוונטית, ולכן לא כללנו אותה כאן.

בחרנו במונח "עיבוד" ולא במונח "שימוש" כדי לחדד את ההבחנה בין המונח השגור לפעולות המבוצעות על ידי משתמשי קצה (end-users) לבין הפעולות הנעשות במידע אישי.

בסעיף קטן (1) השתמשנו במונח "תיעוד" בהתאם להגדרתו בסעיף 2 להלן.

סעיף 3 לחוק הגנת הפרטיות הקיים:
"שימוש" – לרבות גילוי, העברה ומסירה.

סעיף 4(2) ל-GDPR:

"(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"

הגדרת **"פקודת המעצר והחיפוש"** זהה להגדרה בסעיף 23ט בהצ"ח תיקון מס' 13.

הגדרת **"פרסום"** המוצעת מתייחסת לפרסום מידע אישי שלא כמו השימוש במונח "פרסום" בהקשרים אחרים בהצעת החוק ומדגישה שמדובר בהעברת המידע האישי לציבור בכל דרך. ההגדרה מאחדת שני מקורות: (1) הגדרת המונח "פרסום" בסעיף 3 לחוק הגנת הפרטיות הקיים, שמפנה להגדרת המונח "פרסום" בסעיף 2 לחוק איסור לשון הרע, התשכ"ה–1965,

ומדגישה ש"פרסום" אינו מוגבל לטכנולוגיה או למדיום מסוים; ו-(2) המונח "פרסום" ו"מפרסם" בחוק העונשין, התשל"ז–1977, שמדגישה את החשיבות שבחשיפת המידע לציבור, כולו או חלקו, כתנאי ל"פרסום".

סעיף 2 לחוק איסור לשון הרע, התשכ"ה-1965:

"2.(א)פרסום, לענין לשון הרע – בין בעל פה ובין בכתב או בדפוס, לרבות ציור, דמות, תנועה, צליל וכל אמצעי אחר.

(ב)רואים כפרסום לשון הרע, בלי למעט מדרכי פרסום אחרות:

(1)אם היתה מיועדת לאדם זולת הנפגע והגיעה לאותו אדם או לאדם אחר זולת הנפגע;

(2)אם היתה בכתב והכתב עשוי היה, לפי הנסיבות להגיע לאדם זולת הנפגע."

סעיף 34כד לחוק העונשין:

"פרסום" – "כתב, דבר דפוס, חומר מחשב, או כל מצג חזותי אחר וכן על אמצעי שמיעתי העשויים להעלות מילים או רעיונות, בין לבדם ובין בעזרת אמצעי כלשהו;"

"פרסם" – (1) בדברים שבעל פה – להשמיע מלים בפה או באמצעים אחרים, בהתקהלות ציבורית או במקום ציבורי או באופן שאנשים הנמצאים במקום ציבורי יכולים לשמוע אותם, או להשמיען בשידורי רדיו או טלוויזיה הניתנים לציבור, או להפיצן באמצעות מחשב בדרך הזמינה לציבור, או להציען לציבור באמצעות מחשב; (2) בפרסום שאינו דברים בעל פה – להפיצו בקרב אנשים או להציגו באופן שאנשים במקום ציבורי יכולים לראותו, או למכרו או להציעו למכירה בכל מקום שהוא, או להפיצו בשידורי טלוויזיה הניתנים לציבור, או להפיצו לציבור באמצעות מחשב בדרך הזמינה לציבור, או להציעו לציבור באמצעות מחשב;"

הגדרת "**קטין**" זהה להגדרה המוצעת בסעיף 3 להצ"ח פרטיות קטינים, שמטרתה לשפר ולחדד את הגנת הפרטיות על קטינים – הן מצד הורי הקטין והן מצד המדינה – ולהתאימה לאסדרה הנהוגה ברוב שיטות המשפט ההשוואתי.[15]

הגדרת "**קשיש**" מבוססת על ההגדרה המקובלת בארץ ובעולם.

"ראש הרשות להגנת הפרטיות" – מי שהממשלה מינתה אותו, בהודעה ברשומות, לעמוד בראש הרשות להגנת הפרטיות;

"הרשות" או "הרשות להגנת הפרטיות" – הגוף הציבורי המפקח, האוכף והמסדיר את ההגנה על הזכות לפרטיות בהתאם להוראות חוק זה;

"רשות חוץ" – גוף המופקד על ביצוע ואכיפה של דיני הגנת הפרטיות במדינת חוץ ופיקוח על ביצועם;

"שלמות מידע" – שמירה על מהימנות ודיוק המידע האישי במהלך עיבודו, בלא ששונה או הושמד, שלא לפי להוראות חוק זה;

"תיעוד" – לעניין פסקה (1) שבהגדרת "עיבוד" ולעניין סעיפים 4(5) ו-65(א)(3)(ה) – לרבות קליטה או שימור של מידע אישי באמצעות חיישני מיקום, חיישני חום או כל אמצעי טכנולוגי אחר;

דברי הסבר

הגדרת **"ראש הרשות להגנת הפרטיות"** מחליפה את הגדרת ה"רשם" בסעיף 7 לחוק הגנת הפרטיות הקיים.

כבר ב-2007 המליצה ועדת שופמן לצמצם את חובת הרישום.[16] בשנת 2012 פרסם משרד המשפטים תזכיר הצעת חוק לצמצום החובה לרישום מאגרי המידע ולהחלתה רק על גופים ציבוריים ועל מאגרי מידע רגיש במיוחד.[17] הדבר נעשה מתוך ההבנה שהתועלת בחובת הרישום נמוכה, שהיא אינה מבטיחה כלל ציות להוראות החוק ושהעיסוק של הרשות להגנת הפרטיות באכיפה של חובת הרישום מוביל לבזבוז משאבים חשובים, ועל כן יש להמירה בחלופה טובה יותר – שתביא להפנמה אמיתית של חובות הגנת הפרטיות לפי החוק, כגון חובת הניהול התקין. התזכיר לא התגבש לכדי הצעת חוק. לדעתנו, בעולם דיגיטלי שבו מידע אישי נאגם ונשמר כעניין שבשגרה, חובת רישום מטילה נטל רגולטורי בלתי סביר. כל עוסק זעיר שמחזיק ברשימת שמות של לקוחות, צרכנים או משתמשים בשירות שהוא נותן עשוי להיות חייב בחובת רישום לפי החוק הקיים. יתרה מזו, בעידן שלנו היום תחימת החובות להגנת הפרטיות לקיומו או להגדרתו של אוסף הנתונים כמאגר מידע פוגעת בהיקף של הגנת הפרטיות ובעוצמתה. לכן יש לדעתנו לבטל את חובת הרישום בכללותה. מערך הכלים החלופי להגנת פרטיות במידע אישי המוצע בהצעת החוק נותן מענה מקיף ומדויק יותר להגנת פרטיות מהמענה שנותנת החובה לרישום מאגרי מידע.

עם ביטול ההתייחסות בהצעת החוק למאגרי מידע ולחובת רישום אין מקום להתייחסות לתפקיד ספציפי של רישום מאגרי מידע. כמו כן אין צורך בפירוט של תנאי הכשירות לתפקיד ראש הרשות להגנת הפרטיות בהגדרת המונח אלא בסעיף ייעודי לכך. סעיף 7 לחוק הגנת הפרטיות הקיים: "רשם – מי שמתקיימים בו תנאי הכשירות למינוי שופט של בית משפט השלום, והממשלה מינתה אותו, בהודעה ברשומות, לנהל את פנקס מאגרי מידע (להלן – הפנקס) כאמור בסעיף 12;"

הגדרת **"רשות חוץ"** מבוססת על הגדרת המונח בסעיף 54יא1(א) לחוק ניירות ערך, התשכ"ח–1968, והתאמתה להצעת החוק.

סעיף 54יא1(א) לחוק ניירות ערך, התשכ"ח–1968:

"רשות חוץ" – גוף המופקד על ביצוע ואכיפה של דיני ניירות ערך במדינת חוץ ופיקוח על ביצועם, אשר חתם על מזכר הבנה עם הרשות;"

הגדרת **"שלמות המידע"** מבוססת על הגדרת המונח בסעיף 7 לחוק הגנת הפרטיות הקיים ומותאמת לניסוח חקיקה

מודרני ולשימוש הגובר במונח "שלמות המידע" (data integrity) בהקשרים של מחשוב ענן ומכשירי טכנולוגיה מסוג האינטרנט של הדברים. ההגדרה המוצעת משקפת את החשיבות שבשמירה על מהימנות ודיוק המידע האישי בעת עיבודו ומתירה את שינויו לפי הצעת חוק זו ולא על פי כל דין, כפי שמתירה הגדרת המונח בחוק הקיים.

סעיף 7 לחוק הגנת הפרטיות הקיים:
"**שלמות מידע**" – זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין."

הגדרת "**תיעוד**" הוספה כדי להתאים את הצעת החוק למציאות טכנולוגית מתפתחת שיש בכוחה לאפשר עיבוד מידע אישי בדרכים נוספות על צילום, שמופיע בחוק הגנת הפרטיות הקיים, למשל באמצעות חיישנים. ההגדרה אינה מתייחסת לשימוש במונח "תיעוד" בסעיפים 22 ו-38(ב)(5) מאחר שסעיפים אלו עוסקים בתיעוד אירועי אבטחה.

סעיף 3:
איסור פגיעה בפרטיות

לא יפגע אדם בפרטיות של זולתו אלא לפי הוראות חוק זה.

דברי הסבר

<u>סעיף 3:</u> הסעיף מבוסס על סעיף 1 לחוק הגנת הפרטיות הקיים, הקובע כך:

"לא יפגע אדם בפרטיות של זולתו ללא הסכמתו."

ברם דרישת ההסכמה אינה ולא צריכה להיות הכלי היחיד להכשרת פגיעה בפרטיות. כמוסבר בדברי ההסבר לסעיף 6, מוצע למחוק את דרישת ההסכמה כדרישה גורפת לכל פגיעה בפרטיות ולשלבה בנסיבות ובהקשרים ספציפיים כחלק מהגדרת פגיעה בפרטיות שבסעיף 4. כך, לפי הסעיף המוצע, צריך שכל פגיעה בפרטיות, אם היא מתרחשת, תיעשה לפי הצעת חוק זו, בכפוף לסעיף 76 העוסק בשמירת הדינים.

סעיף 4: פגיעה בפרטיות

פגיעה בפרטיות היא אחת מאלה:

(1) בילוש או התחקות אחרי אדם, העלולים להטרידו;

(2) האזנה האסורה על פי חוק;

(3) צפייה או עיון במידע אישי, לרבות קריאה או האזנה;

(4) צילום אדם כשהוא ברשות היחיד שלא לפי הוראות חוק זה;

(5) פרסום של תצלומו של אדם או תוצר של תיעוד אודות אדם בנוגע למצבו או להתנהגותו ברשות הרבים, שלא לפי הוראות חוק זה, בנסיבות שבהן עלול הפרסום להשפילו או לבזותו, ובכלל זה לאחר אירוע פתאומי שבו נגרמה לאותו אדם פגיעה גופנית או נפשית, למעט פרסום תצלום או תוצר של תיעוד בלא השהיות בין רגע הצילום או התיעוד לרגע השידור בפועל שאינו חורג מהסביר באותן נסיבות;

(6) שימוש בשם אדם, בכינויו, בתמונתו או בקולו שלא לפי הוראות חוק זה;

(7) הפרה של חובת סודיות שנקבעה בדין או בהסכם לגבי ענייניו הפרטיים של אדם;

(8) עיבוד של מידע אישי על אודות אדם שלא לפי הוראות חוק זה.

סעיף 5: פרסום תצלומו של נפטר

שאלת קיומה של זכות לפרטיות לאחר המוות דורשת מחקר נפרד, שאינו בליבת עבודתנו הנוכחית לגיבוש הצעה לחוק הגנת פרטיות חדש ומעודכן.

דברי הסבר

<u>סעיף 4:</u> הסעיף המוצע מבוסס על סעיף 2 לחוק הגנת הפרטיות הקיים. הוא מציג רשימה סגורה של פגיעות אפשריות בפרטיות.

נציין שבקבוצת המומחים הוצע תחילה לקבוע בסעיף עיקרון כללי המסביר מהי פגיעה בפרטיות ולהוסיף בצידו רשימה פתוחה של פגיעות אפשריות בפרטיות, בדומה לסעיף 2 לחוק מניעת הטרדה מאיימת, התשס"ב-2011.[18] הנימוק לחלופה זו היה שיש לספק, מחד גיסא, את מידת הוודאות הנדרשת בעיקר משום שפגיעה בפרטיות יכולה להיחשב עבירה פלילית או עוולה אזרחית לפי הוראות סעיפים 61 ו-62 לחוק המוצע; ומאידך גיסא – להותיר בידי בית המשפט מידה מסוימת של גמישות בפרשנות הוראות החוק על מנת להתאימו לטכנולוגיות המשתנות לפגיעות אפשריות בפרטיות, בכלל זה לשימושים עתידיים במידע אישי שעלולים לפגוע בפרטיותו של אדם באופנים שאי-אפשר לצפות אותם כעת.

לבסוף גבר הצורך בקביעת ודאות משפטית, ונוסח הסעיף מציג רשימה סגורה כקבוע בסעיף 2 לחוק הגנת הפרטיות הקיים ("פגיעה בפרטיות היא אחת מאלה:") ובסעיף 3(א) לחוק למניעת הטרדה מינית, התשנ"ח–1998 ("הטרדה מינית היא כל אחד ממעשים אלה").[19]

סעיף קטן (1) מבוסס על סעיף 2(1) בחוק הגנת הפרטיות הקיים, הקובע כך:

"בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת;"

בנוסח המוצע בסעיף קטן (1) הסרנו את צמד המילים "או הטרדה אחרת" – כדי להבהיר שהטרדה, אף אם אינה מאיימת, בכל זאת עלולה לפגוע בפרטיותו של אדם. למשל, מעקב באמצעות מכשיר GPS סמוי אינה מאיימת, שכן האדם אינו מודע לקיומה, ובכל זאת היא מהווה פגיעה בפרטיותו. במובן זה הטרדה מתחברת היטב למובנה של הפרטיות כזכותו של אדם להיעזב במנוחה ולמנוע מאדם אחר כניסה למרחב האישי שלו. נציין כי החוק למניעת הטרדה מאיימת נחקק אחרי שנחקק חוק הגנת הפרטיות בשנת 1981 ומציע אפיק הגנה ספציפי, במקרים המתאימים, כמו החוק למניעת הטרדה מינית.

סעיף קטן (2) זהה לסעיף 2(2) בחוק הגנת הפרטיות הקיים. בחרנו להשאירו כלשונו כדי למנוע חוסר ודאות פרשני ולתת דגש גם לפגיעות "קלסיות" בפרטיות. על פי לשון הסעיף, גם אם מדובר בהאזנה האסורה על פי חוק איסור האזנת סתר, התשל"ט-1979, היא עדיין מהווה פגיעה בפרטיות. נדגיש שכאשר מדובר בהאזנה שאינה אסורה על פי חוק האזנת סתר, היא עדיין יכולה להיכנס תחת הגדרת פגיעה בפרטיות לפי סעיף קטן (8) – עיבוד מידע אישי בניגוד להוראות החוק – הואיל והגדרנו "עיבוד" גם כעצם איסוף המידע.

סעיף קטן (3) קובע שצפייה או עיון במידע אישי הם פגיעה בפרטיות אף אם המידע אינו מפורסם וגם אם לא נעשות בו פעולות עיבוד אחרות.[20]

סעיף קטן (4) זהה לסעיף 2(3) בחוק הגנת הפרטיות הקיים ועוסק בפגיעה בפרטיות במובנה הקלסי. אומנם צילום עשוי גם הוא להיכנס תחת הגדרת פגיעה בפרטיות בסעיף קטן (8) – עיבוד מידע אישי בניגוד להוראות החוק – הואיל והגדרנו "עיבוד" גם כצילום. כדי להימנע מחוסר ודאות פרשני בחרנו להשאיר את הניסוח הנוכחי. כדי להגביר את הוודאות ביישום הוראה זו הבהרנו שמדובר בצילום שנעשה שלא לפי הוראות החוק.

סעיף קטן (5) מחליף את הפגיעות המתוארות בסעיפים 2(4), 2(4א), ו-(10) בחוק הגנת הפרטיות הקיים. הסעיף גם מוסיף פגיעה בפרטיות בעקבות "פרסום תוצר של תיעוד" (למשל, פרסום איכון הטלפון הסלולרי במועדון חשפנות) כשיש בפרסום כדי להשפיל או לבזות את נושא המידע.

סעיף 2(4) לחוק הגנת הפרטיות הקיים:
"פרסום תצלומו של אדם ברבים בנסיבות שבהן עלול הפרסום להשפילו או לבזותו;"

סעיף 2(4א) לחוק הגנת הפרטיות הקיים:
"פרסום תצלומו של נפגע ברבים שצולם בזמן הפגיעה או סמוך לאחריה באופן שניתן לזהותו ובנסיבות שבהן עלול הפרסום להביאו במבוכה, למעט פרסום תצלום בלא השהיות בין רגע הצילום לרגע השידור בפועל שאינו חורג מהסביר באותן נסיבות; לעניין זה, "נפגע" – מי שסבל מפגיעה גופנית או נפשית עקב אירוע פתאומי ושפגיעתו ניכרת לעין;"

סעיף 2(10) לחוק הגנת הפרטיות הקיים:
"פרסומו או מסירתו של דבר שהושג בדרך פגיעה בפרטיות לפי פסקאות (1) עד (7) או (9);"

סעיף קטן (6) מבוסס על סעיף 2(6) בחוק הגנת הפרטיות הקיים, שלשונו:

"שימוש בשם אדם, בכינויו, בתמונתו או בקולו, לשם ריווח;"

מטרת הסעיף היא להבהיר שכאשר נעשה שימוש בשמו של אדם, בכינויו, בקולו או בתמונתו שלא לפי הצעת החוק מדובר בפגיעה בפרטיות. השאלה אם הפעולה נעשית לשם הפקת רווח אינה רלוונטית לשאלת הפגיעה בפרטיות, ועל כן בחרנו להשמיט את צמד המילים "לשם ריווח" מלשון הצעת החוק.

סעיף קטן (7) מבוסס על סעיף 2(7) ו-2(8) בחוק הגנת הפרטיות הקיים, שלשונם:

"(7) הפרה של חובת סודיות שנקבעה בדין לגבי ענייניו הפרטיים של אדם;

(8) הפרה של חובת סודיות לגבי ענייניו הפרטיים של אדם, שנקבעה בהסכם מפורש או משתמע;"

לדעתנו אין מקום לציין שחובת הסודיות נקבעה בהסכם "מפורש או משתמע" ודי בקביעה שמקורה בהסכם.

סעיף קטן (8) נוסף, כאמור, על החקיקה הקיימת, והוא מסדיר אירועי פגיעה בפרטיות במידע בעקבות עיבוד מידע אישי בניגוד להוראות הצעת החוק. הסעיף הוא חלק מחיזוק התאימות עם הוראות ה-GDPR המציגות בסיסים לגיטימיים לפגיעה בפרטיות בצד ההסכמה. נוסף על כך מטרת הסעיף, בין השאר, להחליף את סעיפים 2(9)-(11) לחוק הגנת הפרטיות הקיים ולהדגיש שלפי הצעת החוק לא רק הסכמה יכולה להכשיר פגיעה בפרטיות בעקבות עיבוד מידע אישי ושיש מסלולים נוספים.

חוק הגנת הפרטיות הקיים:
2(9) "שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה;"

2(11) "פרסומו של ענין הנוגע לצנעת חייו האישיים של אדם, לרבות עברו המיני, או למצב בריאותו, או להתנהגותו ברשות היחיד."

סעיף 2(5) לחוק הגנת הפרטיות הקיים לא נכלל בהצעת החוק המוצעת כאן, משום שהפגיעה בפרטיות המפורטת בו נכללת בסעיפים קטנים (4), (6) ו-(7) המוצעים.

סעיף 2(5) לחוק הגנת הפרטיות הקיים קובע כך:
"העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב, והכל אם אין הכתב בעל ערך היסטורי ולא עברו חמש עשרה שנים ממועד כתיבתו; לענין זה, "כתב" – לרבות מסר אלקטרוני כהגדרתו בחוק חתימה אלקטרונית, התשס"א-2001;"

עקרון צמידות המטרה שבסעיף 2(9) לחוק הגנת הפרטיות הקיים מעוגן בסעיף 7 להצעת החוק.

פרק ב: הגנה על הפרטיות במידע אישי

סימן א': הוראות כלליות לעניין עיבוד מידע אישי

סעיף 6: פגיעה מותרת בפרטיות

(א) פגיעה בפרטיות מותרת בהתקיים אחד מאלה:

(1) היא נדרשת לשם מילוי התחייבויות הקבועות בהסכם שנושא המידע הוא צד לו, או לשם נקיטת צעדים המבוקשים על ידי נושא המידע לפני ההתקשרות בהסכם כאמור;

(2) היא נדרשת כדי להגן על אינטרס מהותי של בעל השליטה במידע או צד שלישי שאליו הועבר מידע אישי ובלבד שהיא אינה מבוצעת על ידי גוף ציבורי במסגרת ביצוע משימותיו על פי דין ושנושא המידע היה יכול לצפות באופן סביר בהתחשב בזמן ובנסיבות שתתרחש פגיעה כאמור.

(3) נושא המידע הסכים לפגיעה בפרטיות.

(ב) פגיעה בפרטיות בדרך של עיבוד מידע רגיש מותרת בהתקיים אחד מאלה:

(1) עיבוד המידע הרגיש נחוץ לצורך מימוש זכויותיו של נושא המידע, או לצורך מימוש זכויותיו או מילוי חובותיו של בעל שליטה במידע, במסגרת יחסי העבודה בין בעל שליטה במידע לנושא המידע ובהתאם לחוק המתיר עיבוד מידע רגיש לצורך מטרות אלו.

(2) עיבוד המידע הרגיש מידתי בהיקפו לצורך ביצוע מחקר סטטיסטי, מדעי או היסטורי שיש אינטרס ציבורי בביצועו.

(3) עיבוד המידע הרגיש נדרש כדי להגן על אינטרס מהותי של בעל השליטה במידע או צד שלישי שאליו הועבר המידע הרגיש ובלבד שעיבוד המידע הרגיש אינו מבוצע על ידי גוף ציבורי במסגרת ביצוע משימותיו על פי דין ושנושא המידע הסכים במפורש לעיבוד המידע הרגיש על אודותיו; היה העיבוד לפי פסקה (3) להגדרת עיבוד בסעיף 2 לחוק - נושא המידע הסכים במפורש קודם לביצוע עיבוד כאמור.

דברי הסבר

סעיף 6: הסעיף מגדיר בהצעת החוק מסלולים המתירים פגיעה בפרטיות, לרבות בדרך של עיבוד מידע אישי או מידע רגיש. בדומה לסעיפים 6 ו-9 ל-GDPR, על בעל שליטה במידע לבחון מהי מטרת העיבוד הרצויה לו (או מטרה דומה שלשמה נאסף או נמסר המידע האישי בהתאם לסעיף 7 להלן) ולבחון מהו הבסיס הלגיטימי שיאפשר לו את עיבוד המידע למטרה זו.

חשוב להבהיר שהתממה אינה מהווה בסיס משפטי להתרת עיבוד מידע אישי.[21] קביעה זו אף עולה בקנה אחד עם ההבנה שהתממה אינה מספקת הגנה מושלמת לזכות לפרטיות, בעיקר לא בעידן של נתוני עתק (big data). כמויות המידע האישי הקיימות באינטרנט והתפתחות טכנולוגיות משופרות וזמינות לכריית מידע ולהצלבתו הופכים את הסכנה של זיהוי חוזר גם אחרי התממה לממשית ביותר.[22] גם בסעיף 26 להקדמה ב-GDPR

מובהר שה-GDPR אינו חל על מידע מותמם, אבל מוסבר שהקביעה אם המידע המותמם אינו מאפשר את זיהויו של נושא המידע תיעשה מתוך בחינת כל האמצעים שסביר שייעשה בהם שימוש לשם זיהוי חוזר של מידע לאחר התממתו. סבירות השימוש באמצעים תיקבע לפי מדדים אובייקטיביים, כגון עלות הזיהוי החוזר, פרק הזמן הנדרש לביצוע זיהוי חוזר, הטכנולוגיה הזמינה בזמן עיבוד המידע המותמם והתפתחויות טכנולוגיות צפויות באותה עת. ס"ק (א)(1) מתיר פגיעה בפרטיות כאשר היא נדרשת לשם מילוי מחויבות בהסכם שנושא המידע הוא צד בו או כניסה להסכם כאמור. הסעיף מבוסס על **סעיף 6(1)(b) ל-GDPR** הקובע:

"(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;"

ס"ק (א)(2) מבוסס על סעיף 6(1)(f) ל-GDPR. הסעיף קובע שפגיעה בפרטיות מותרת כאשר היא נחוצה למימוש אינטרס מהותי של בעל השליטה במידע או של צד שלישי, ובלבד שאינטרסים או זכויות יסוד של נושא המידע אינם גוברים על אותו אינטרס מהותי, בייחוד כאשר נושא המידע הוא ילד. עוד מבהיר הסעיף שיישומו מוגבל לבעל שליטה שאינו רשות ציבורית הממלאת את משימותיה – כדי לחייב רשות ציבורית לפעול בהתאם להסמכה בדין ולא על פי איזון בין אינטרס מהותי שלה לבין זכויות נושא המידע.

לפי סעיף 47 לדברי ההקדמה ל-GDPR, המבחן אם אינטרסים או זכויות יסוד של נושא המידע גוברים על האינטרס המהותי של בעל השליטה במידע או של צדדים שלישיים שהמידע האישי מועבר אליהם הוא מבחן הציפייה הסבירה. כלומר – האם נושא המידע יכול לצפות באופן סביר, בהתחשב בזמן ובנסיבות של איסוף המידע האישי, שעיבוד המידע האישי מתבצע למטרות מילוי האינטרס המהותי של בעל השליטה במידע או של צד שלישי.

סעיף 6(1)(f) ל-GDPR:

"6(1)(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."

סעיף 47 להקדמה ל-GDPR:

"The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

סעיפים 48 ו-49 להקדמה ל-GDPR מציגים דוגמאות לאינטרס מהותי של בעל שליטה במידע, למשל העברת מידע אישי בין חברות קשורות או עיבוד מידע אישי בהיקף הנחוץ והמידתי לאבטחת המידע האישי.

"48. Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

49. The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems."

ס"ק (א)(3) מתיר פגיעה בפרטיות בהסכמת נושא המידע. הסעיף מופיע בסוף רשימת הבסיסים הלגיטימיים, ומטרתו לחדד את שינוי התפיסה שבעקבותיו ייטיב בעל שליטה במידע לבדוק אם עומדים לרשותו בסיסים לגיטימיים אחרים לפגיעה בפרטיות קודם שיפנה להכשרת הפגיעה בפרטיות של נושא המידע על ידי קבלת הסכמה. הסעיף מבוסס על סעיף 6(1)(a) ל-GDPR, הקובע:

"6(1)(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;"

ס"ק (ב)(1) מתיר פגיעה בפרטיות בדרך של עיבוד מידע רגיש, כמו למשל נתונים ביומטריים, לצורך מימוש זכויותיהם של בעל שליטה במידע או של נושא מידע או לצורך מילוי חובותיו של בעל שליטה במידע במסגרת יחסי העבודה בין בעל שליטה במידע לנושא המידע. הסעיף מבוסס על סעיף 9(2)(b) ל-GDPR:

"(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;"

ס"ק (ב)(2) מתיר פגיעה בפרטיות בדרך של עיבוד מידע רגיש במידה הדרושה לצורך מחקר מדעי, סטטיסטי או היסטורי שיש אינטרס ציבורי בביצועו. הסעיף מבוסס על הוראת סעיף 9(2)(j) ל-GDPR:

"9(2)(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

ס"ק (ב)(3) מתיר פגיעה בפרטיות בדרך של עיבוד מידע רגיש לפי האיזון שבין האינטרס המהותי של בעל שליטה במידע והאינטרס המהותי של נושא המידע, בדומה לס"ק (א)(2), אך מחייב לקבל הסכמה מפורשת של נושא המידע. רק

כאשר מדובר בגילוי או בפרסום של מידע רגיש, כלומר עיבוד לפי פסקה (3) להגדרת המונח "עיבוד" בסעיף 2 להצעת החוק, נדרשת הסכמתו המפורשת של נושא המידע קודם לביצוע הגילוי או הפרסום – כדי לחזק את שליטתו של נושא המידע במידע רגיש עליו ולהבטיח שהוא מודע למכלול פעולות העיבוד האפשריות במידע הרגיש עליו.

<u>הסעיפים שלהלן מה-GDPR לא נכללו בסעיף המוצע:</u>

סעיף 6(1)(c) העוסק בעיבוד מידע אישי לשם ציות לחובה חוקית. לדעתנו, מקומה של הוראה זו בסעיף ההגנות (סעיף 65 בהצעת החוק) – על מנת שנטל ההוכחה שלה יוטל על בעל השליטה במידע או על המעבד ולא על נושא המידע.

"6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject;"

סעיף 6(1)(d) שמתיר עיבוד מידע אישי לצורך הגנה על אינטרס חיוני של נושא המידע או אדם אחר – כמו, למשל, לפי המתואר בסעיף 46 להקדמה ל-GDPR, במקרה של עיבוד מידע אישי מטעמים הומניטריים או מניעת מגפה – כל עוד עיבוד המידע האישי נדרש לשם הגנה על חייו של אדם אחר או על אינטרס מהותי שלו וכל עוד אין בסיס לגיטימי אחר המתיר את עיבוד המידע האישי. אנו סבורים כי מקומה של הוראה זו גם הוא בסעיף ההגנות (סעיף 65 בהצעת החוק) – כדי להטיל את נטל ההוכחה שלה על בעל שליטה במידע או על מעבד.

"6(1)(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;"

סעיף 46 לדברי ההקדמה ל-GDPR:

"46. The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters."

סעיף 6(1)(e) המתיר עיבוד מידע אישי לצורך ביצוע משימה לטובת הציבור או לצורך מימוש סמכות רשמית הנתונה לבעל שליטה במידע. לדעתנו, הכשרת פגיעה בפרטיות למטרות של "טובת הציבור" היא עמומה מדי, ובכל מקרה די בהגנה הקבועה בסעיף 65(א)(2) המאפשרת עיבוד מידע אישי לשם מילוי חובה על פי דין.

סעיף 9(2)(c) שמתיר עיבוד מידע רגיש לצורך הגנה על אינטרס מהותי של נושא המידע או של אדם אחר כאשר נושא המידע אינו מסוגל פיזית או משפטית לתת את הסכמתו לעיבוד. נושא ההסכמה לעיבוד מידע לצורך הגנה על חייו ועל בריאותו של אדם בעת חירום וכאשר הוא אינו מסוגל פיזית או משפטית להסכים לעיבוד מוסדר בחוקים ספציפיים, למשל סעיף 15 לחוק זכויות החולה, התשנ"ו–1996 ותיקון מספר 26 לחוק העונשין, המסדיר את חובת הדיווח לצורך הגנה על חסרי ישע. לפיכך, ולנוכח הסדרים ספציפיים אלו, אין לדעתנו הצדקה לאימוץ הוראת סעיף 9(2)(c) ל-GDPR המתווה אמת מידה רחבה ומעורפלת בהרבה שאינה מוגבלת לאוכלוסיות מיוחדות או לבעלי תפקידים מסוימים.

"9(2)(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;"

סעיף 9(2)(d) שמתיר עיבוד מידע רגיש מתוך נקיטת אמצעי האבטחה המתאימים במסגרת הפעילות הלגיטימית של ארגון או עמותה שלא למטרות רווח שמטרותיה פוליטיות, פילוסופיות או דתיות, או על

ידי ארגון עובדים, על חבר או חבר לשעבר בהם. היום, לאחר הגילויים בפרשת **קיימברידג' אנליטיקה**, היכולת לפגוע קשות באוטונומיה ובבחירה החופשית באמצעות ניתוח מידע אישי ויצירת מיקרו-טרגטים פוליטי ברורה. ולכן, לדעתנו, אין מקום להתיר עיבוד מידע אישי על ידי גוף שלא למטרות רווח בעל מטרות פוליטיות או דתיות. ייתכן שבעתיד יהיה צורך לאסדר שימושים אלו בדיני תעמולת בחירות, אבל לא כפטור גורף בדיני הגנת הפרטיות.

"9(2)(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;"

סעיף 9(2)(e) המתיר עיבוד מידע רגיש שנושא המידע פרסם במודע בציבור. בפרשנות שניתנה לסעיף בעבר (בדירקטיבה להגנת נתונים של האיחוד האירופי) הוסבר שיש צורך להוכיח שנושא המידע היה מודע לכך שהמידע שהוא מפרסם יהיה זמין לכולם, לרבות לרשויות אכיפת החוק. בקבוצת המומחים הוסכם ברוב דעות שדי בהגדרה של הסכמת נושא המידע ככוללת הסכמה מכללא.

"9(2)(e) processing relates to personal data which are manifestly made public by the data subject; "

סעיף 9(2)(f) המתיר עיבוד מידע רגיש כאשר הוא נחוץ לביסוסה של טענת הגנה משפטית. לדעתנו מקומה של הוראה זו בסעיף ההגנות, בדומה לסעיף 65(א)(3)(ג) המוצע להלן.

"9(2)(f). processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;"

סעיף 9(2)(g) המתיר עיבוד מידע רגיש לטובת אינטרס ציבורי משמעותי, ובלבד שעיבוד המידע הרגיש נעשה לפי חוק ייעודי לַנושא במדינה החברה באיחוד האירופי וכן שאותו חוק ייעודי קובע הסדר מידתי להשגת המטרה של עיבוד המידע הרגיש, מכבד את זכויות נושא המידע ומבטיח נקיטת אמצעי אבטחה מתאימים. לדעתנו, די בהגנה הקובעת שהעיבוד נעשה מכוח סמכות בדין, ואין צורך בקביעת הוראה מורכבת כזו, המכשירה פגיעה בפרטיות למטרות של "אינטרס ציבורי מהותי", שהוא מונח עמום הנתון לפרשנות.

"9(2)(g). processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;"

סעיף 9(2)(h) שמתיר עיבוד מידע רגיש למטרות של רפואה מניעתית או תעסוקתית, להערכת כושר התעסוקה של עובד, לקביעת אבחנה רפואית, למתן שירותי רפואה או שירותי רווחה, לטיפול או לניהול מערכות למתן שירותי רפואה על פי חוק ייעודי במדינה החברה באיחוד האירופי ומתוך נקיטת אמצעי האבטחה הדרושים. חוק זכויות החולה, התשנ"ו–1996 קובע הסדרים ברורים למתן טיפול רפואי, בכלל זה שמירה על פרטיות המטופל, ואין צורך לקבוע הסדר דומה בהצעת החוק. באשר לעיבוד מידע רגיש הדרוש לצורך רפואה תעסוקתית או הערכת כושר העבודה של העובד – לדעתנו די בהוראת סעיף קטן (ב)(1) המתירה עיבוד מידע רגיש לצורך מימוש זכויותיו של בעל שליטה במידע או של נושא המידע ולצורך מימוש חובותיו של בעל שליטה במידע במסגרת יחסי עבודה בין השניים.

"9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working

capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;"

סעיף 9(2)(i) המתיר עיבוד מידע רגיש לצורכי אינטרס הציבור בתחום בריאות הציבור, כמו למשל הגנה מפני איום חוצה גבולות לבריאות או הבטחת נורמת איכות ובטיחות לשירותי רפואה או מוצרים רפואיים ותרופתיים. בסעיפים 53 ו-54 להקדמה ל-GDPR מוסבר שעיבוד מידע רגיש מותר כאשר הוא דרוש למטרות בריאות או רפואה לטובת נושא המידע או הציבור בכללותו. לדעתנו, הגנה על חייו של נושא המידע או מניעת מגפות צריכה להיעשות על ידי המדינה ומכוח חוקים ייעודיים לנושא, כמו למשל חוק זכויות החולה, התשנ"ו–1996. מטעמים אלו אנו סבורים כי עיבוד מידע אישי למטרות אלו על ידי חברה פרטית צריך להיעשות לפי חוק ייעודי לנושא ולא במסגרת קביעת בסיס לגיטימי כללי בהצעת החוק. לפיכך בחרנו לאמץ רעיונית, ובצמצום, את הוראות סעיפים אלו כהגנה בסעיף 65(א)(3)(ז).

סעיפים 53-54 לדברי ההקדמה ל-GDPR:

"53. Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

54. The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council[1], namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies."

סעיף 7: דרישת קיום המטרה

לא יעבד בעל שליטה במידע מידע אישי אלא למטרה שלשמה נאסף או נמסר המידע האישי כמפורט בהודעה לפי סעיף 9 או למטרה הדומה למטרה שלשמה נאסף או נמסר המידע האישי; בבואו לבחון את קיומה של מטרה דומה כאמור, ישקול בעל שליטה במידע, בין השאר, את אלה:

(1) הקשר בין המטרה לשמה נאסף או נמסר המידע האישי לבין מטרת העיבוד שהוא מבקש לבצע;

(2) הנסיבות שבהן נאסף המידע האישי, קיומה של מערכת יחסים בין נושא המידע לבין בעל השליטה במידע ואת ציפייתו הסבירה של נושא המידע בנוגע לעיבוד נוסף של המידע האישי, מעבר למטרה לשמה נאסף או נמסר;

(3) האם המידע האישי כולל מידע רגיש;

(4) השלכות אפשריות של העיבוד הנוסף שהוא מבקש לבצע.

דברי הסבר

<u>סעיף 7:</u> סעיף זה מעגן את דרישת קיום המטרה כתנאי להתרת פגיעה בפרטיות בדרך של עיבוד מידע אישי או מידע רגיש לפי סעיף 6. הסעיף מבוסס על סעיף 2(9) לחוק הגנת הפרטיות הקיים. עם זה, סברנו כי ראוי לעגן את עקרון צמידות המטרה בסעיף נפרד ועל דרך החיוב.

הסעיף מבוסס גם על סעיפים 5(1) ו-6(4) ל-GDPR לעניין המבחנים לקיומה של "מטרה דומה". קריאת כיוון כיצד ליישם מבחנים אלו נמצאת בסעיף 50 לדברי ההקדמה ל-GDPR וכוללת גם התייחסות לכך שעיבוד מידע אישי לצורכי אִרכוב לטובת הציבור או לצורכי מחקר מדעי או היסטורי או למטרות סטטיסטיות ייחשב "מטרה דומה".

ניסוח הדרישה לקיום המטרה וכן קביעת מבחנים לקיומה של "מטרה דומה" באים במקום אימוץ האיסור על התניית מתן שירות או מוצר בקבלת ההסכמה מנושא המידע לפגיעה בפרטיותו, כקבוע בסעיף 7(4) ל-GDPR.

סעיף 2(9) לחוק הגנת הפרטיות הקיים:

"פגיעה בפרטיות היא אחת מאלה:

(9) שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה;"

סעיף 7(4) ל-GDPR:

"Article 7 Conditions for consent

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

סעיף 5(1) ל-GDPR:

"1. Personal data shall be:

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); "

סעיף 6(4) ל-GDPR:

"4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

סעיף 6(4) ל-GDPR - המשך

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

סעיף 50 לדברי ההקדמה ל-GDPR:

"(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy."

סעיף 8: הסכמה לעניין פגיעה בפרטיותו של קטין

(א) פגיעה בפרטיותו של קטין מתחת לגיל 13 לפי סעיף 6(א)(3) תיעשה אך ורק בהסכמת אחד מהוריו או אפוטרופוס שנתמנה לו כדין, או לפי הסמכה מפורשת בדין.

(ב) לא יעבד בעל שליטה מידע רגיש לפי סעיף 6(ב)(3) על אודות קטין מתחת לגיל 16 אלא בהסכמת אחד מהוריו או אפוטרופוס שנתמנה לו כדין, או לפי הסמכה מפורשת בדין.

(ג) ראש הרשות להגנת הפרטיות יקבע הנחיות בדבר הדרכים לאימות גילו של קטין ולווידוא קבלת הסכמת הוריו או האפוטרופוס שלו, כאמור בסעיפים קטנים (א) ו-(ב).

דברי הסבר

<u>סעיף 8:</u> הסעיף מבקש לשקף את האיזון שבין הצורך להגן על ילדים לבין ההכרה ביכולתם של ילדים מעל גיל 13 לקבל החלטות הנוגעות להם עצמם בעניינים שתוצאותיהם אינן גורליות. מטרת חיוב ההסכמה ההורית או הסכמת אפוטרופוס, שנתמנה לו כדין, או לפי הסמכה מפורשת בדין, היא לתמרץ את חברות הטכנולוגיה ליישם טכנולוגיות מתאימות ולהבטיח בכך זהירות יתרה בעת פגיעה בפרטיות של קטינים, בין השאר בדרך של עיבוד מידע אישי ומידע רגיש עליהם. בהצ"ח פרטיות קטינים לא נדונה השאלה אם יש לדרוש שההסכמה תינתן על ידי אפוטרופוס שמונה בחוק, או שניתן להרחיבה גם לאפוטרופוס שנתמנה מכוח הדין. ה-GDPR דורש כי ההסכמה תתקבל על ידי המחזיק ב"אחריות הורית" ("the holder of parental responsibility"), שאינה מונח המוגדר ב-GDPR, וה-COPPA קובע כי ההסכמה צריכה להיות הסכמה הורית מאושרת ("verifiable parental consent"), גם כאן בלי להגדיר במדויק למה הכוונה. בחרנו לקבוע שנדרשת הסכמת הורה או אפוטרופוס שנתמנה בדין, מאחר שהמונח "דין" מוגדר באופן רחב וכולל חיקוק ודינים מסוגים נוספים, כגון דינים דתיים כפי תוקפם במדינה.

סעיף קטן (א): בחרנו לקבוע את גיל 13 כגיל הקובע לעניין הסכמה לפגיעה בפרטיות, שלא כמו סעיף 8 ל-GDPR, שקובע כי רק מעל גיל 16 יוכל קטין לקבל החלטה בעצמו הנוגעת לעיבוד מידע אישי עליו, ובניגוד לעמדת איגוד האינטרנט הישראלי, כפי שהיא באה לידי ביטוי בהצ"ח פרטיות קטינים, אשר סימנה את גיל 12 כגיל הקובע. הרציונל בבסיס קביעתנו הוא הרצון ליישר קו עם הדין האמריקני הוותיק יותר לעניין פגיעה בפרטיותם של קטינים בדרך של עיבוד מידע אישי עליהם, שסברנו שהוא מתאים יותר למציאות הישראלית.

סעיף קטן (ב): קבענו כי הגיל הקובע לעניין הסכמה לעיבוד מידע רגיש יהיה 16 ולא 18 כפי שהוצע בהצ"ח פרטיות קטינים. החל מגיל 16 ועד לגיל 18 יחול ההסדר הקבוע בחוק הכשרות המשפטית והאפוטרופסות, התשכ"ו–1962,[23] הבוחן אם ההסכמה לעיבוד מידע רגיש על קטין בנסיבות המקרה היא פעולה שדרכם של קטינים לעשות.

בסעיף קטן (ג) בחרנו להסמיך את ראש הרשות להגנת הפרטיות לקבוע הנחיות לאימות גילו של הקטין ולווידוא קבלת ההסכמה מהוריו. לא ראינו לנכון לקבוע בהצעת החוק את החובה לעשות מאמצים סבירים כדי לוודא את גילו של נושא המידע, שכן חובה כאמור עלולה להפוך בתוך שנים אחדות לסטנדרט שרק ענקיות טכנולוגיה יוכלו לעמוד בו ואף לכלי להגברת הריכוזיות בשוק הטכנולוגיה במרחב הסייבר.

בחרנו שלא לאמץ את הוראת סעיף 11ב(5) בהצ"ח פרטיות קטינים המחייבת תיעוד של ההסכמה לשימוש במידע אישי על קטין בהתאם לדרישות הסעיף. חששנו

כי דרישה זו תטיל עומס בלתי סביר על בעלי שליטה במידע וכי השלכותיה עלולות להיות זהות לחובת רישום מאגרי מידע הקיימת היום ושלטעמנו יש לבטלה. כמו כן לא מצאנו מקבילה לדרישה זו ב-GDPR וב-COPPA.

בניסוח הסעיף קיבלנו השראה מן המקורות האלה:

סעיף 11ב מהצ"ח פרטיות קטינים:

"11ב. (1) אין לאסוף מידע על אודות קטין מתחת לגיל 12 למאגר מידע אלא בהסכמת הוריו או אפוטרופוס חוקי שנקבע לו או על בסיס סמכות שנקבעה לאוסף מידע על קטינים במפורש בחוק;

(2) אין לאסוף מידע רגיש על אודות קטין מתחת לגיל 18 למאגר מידע, אלא בהסכמת הוריו או אפוטרופוס חוקי שנקבע לו או על בסיס סמכות שנקבעה לאסוף מידע מסוג זה על קטינים במפורש בחוק;

(5) מי שאוסף מידע על אודות קטין למאגר מידע יחזיק תיעוד מפורט ומדויק של תהליכי קבלת ההסכמה לאיסוף המידע ומטרות השימוש בו, ושל השימוש בפועל במידע על ידו."

ה-COPPA האמריקני:

"§ 312.5 Parental consent.

(a)General requirements.

(1) An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

(b)Methods for verifiable parental consent.

(1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. (2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via video-conference;

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or

(vi)Provided that, an operator that does not "disclose" (as defined by § 312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.

(3)Safe harbor approval of parental consent methods. A safe harbor program approved by the Commission under § 312.11 may approve its member operators' use of a parental consent method not currently enumerated in paragraph (b)(2) of this section where the safe harbor program determines that such parental consent method meets the requirements of paragraph (b)(1) of this section.

(c)Exceptions to prior parental consent. Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child except as set forth in this paragraph:

(1) Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent under § 312.4(c)(1). If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;

סעיף 312.5 ל-COPPA האמריקני - המשך

(2) Where the purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2);

(3) Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;

(4) Where the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered;

(5) Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4);

(6) Where the purpose of collecting a child's name and online contact information is to:
(i) Protect the security or integrity of its Web site or online service;
(ii) Take precautions against liability;
(iii) Respond to judicial process; or
(iv) To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; and where such information is not be used for any other purpose;

(7) Where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the Web site or online service. In such case, there also shall be no obligation to provide notice under § 312.4; or

(8) Where an operator covered under paragraph (2) of the definition of Web site or online service directed to children in § 312.2 collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4."

סעיף 8 ל-GDPR:

"Article 8 Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child."

סעיף 9: חובת מתן הודעה

(א) פניה לאדם לקבלת מידע אישי לשם עיבודו תלווה בהודעה בשפה ברורה בה נאסף המידע האישי, על כוונת בעל שליטה במידע לעבד את המידע האישי, תוך ציון כל אלה:

(1) שמו של בעל שליטה במידע, מענו ודרכי ההתקשרות עימו;

(2) אם חלה על אותו אדם חובה חוקית למסור את המידע האישי, או שמסירת המידע האישי תלויה ברצונו ובהסכמתו, ותוצאות אי הסכמה למסירת המידע האישי;

(3) המטרה אשר לשמה מבוקש העיבוד ונחיצות המידע האישי להגשמתה;

(4) זכות החזרה מהסכמה לעיבוד מידע אישי לפי סעיף 10, זכות העיון במידע האישי לפי סעיף 11, הזכות לקבלת הסבר לפי סעיף 12, זכות תיקון המידע האישי לפי סעיף 13, הזכות לניוד מידע אישי לפי סעיף 14 וזכות המחיקה של מידע אישי לפי סעיף 15, והדרכים למימוש הזכויות כאמור;

(5) למי יימסר המידע האישי ומטרות המסירה.

(ב) שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, יקבע את דרכי ההצגה של ההודעה לפי סעיף קטן (א), לרבות הצגתה במתכונת דיגיטלית, אופן ניסוחה ומידת הבלטתה בהתחשב, בין היתר, בקהלי היעד שלה.

דברי הסבר

__סעיף 9:__ הסעיף מבוסס על חובת ההודעה בסעיף 11 בחוק הגנת הפרטיות הקיים ומשלב תיקונים שהציעה ועדת שופמן להרחבת הפרטים שיש לכלול בהודעה, כגון מקור החובה החוקית לאיסוף מידע אישי, במידה שישנה כזו, דרכי ההתקשורת עם אוסף המידע האישי וכן פרטים ברורים על זכויותיו של נושא המידע כלפי המידע האישי שנאסף ממנו.[24]

התבססנו גם על סעיף 11א להצ"ח פרטיות קטינים, שם מוצע להוסיף סעיף ייחודי לעניין "חובות מבקש מידע על אודות קטין". סברנו שאין מקום לייחד סעיף נפרד לעניין חובת ההודעה לקטינים אלא מוטב לשלב את ההוראות הרלוונטיות בגוף הסעיף הכללי.

נדגיש כי לתפיסתנו חובת ההודעה כוללת גם ניסוח ופרסום של מדיניות פרטיות כפי שנדרש למשל **בחוק הפרטיות האוסטרלי** (Privacy Act of 1988, Schedule 1, §1), ועל כן אין מקום לדעתנו לדרישה מיוחדת בנושא זה לעניין קטינים.

כמו כן לא כללנו את הוראות ס"ק 11א(3) ו-(4) להצ"ח פרטיות קטינים, המוסיפות חובות שונות, כגון אזהרה מודגשת שמתן ההסכמה יביא לפגיעה בפרטיות; הבחנה בין הסכמה ויידוע על איסוף מידע אישי לבין ההסכמה הנדרשת לשם העברה לצדדים שלישיים. נושאים אלו מוסדרים בדרישות כלליות יותר או ניתנים לאסדרה בתקנות. בנוסף, לא אימצנו את הוראת סעיף 11א(5) להצ"ח פרטיות קטינים, המחייבת השקעת מאמצים סבירים לשם וידוא שההסכמה ניתנה על ידי גורם המוסמך לכך. הדרישה שיינקטו מאמצים סבירים לקבלת הסכמה מהגורם המוסמך לכך היא תנאי לתקפותה של הסכמת נושא מידע.

הסעיף המוצע אינו כולל הנחיות להעברת מידע אישי למדינה אחרת, כקבוע בסעיף 13(1)(f) ל-GDPR, שכן נושא ההעברה של מידע אישי למדינה אחרת מטופל בתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה),

התשס"א–2001. התלבטנו בקבוצת המומחים אם לאמץ בהצעת החוק הוראות מתוקנות המבוססות על תקנות העברת מידע. לבסוף החלטנו שהוראות אלו יעודכנו בנפרד, במסגרת העדכון לתקנות הללו.

בניסוח הסעיף קיבלנו השראה מהמקורות האלה:

סעיף 11 לחוק הגנת הפרטיות הקיים:

"פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע תלווה בהודעה שיצויינו בה –

(1) אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו;

(2) המטרה אשר לשמה מבוקש המידע;

(3) למי יימסר המידע ומטרות המסירה."

סעיפים 4א ו-5 לחוק הגנת הצרכן, התשמ"א–1981:

"4א. השר, באישור ועדת הכלכלה של הכנסת, רשאי לקבוע בתקנות הוראות לעניין – האותיות, כולן או חלקן, בחוזה אחיד כמשמעותו בחוק החוזים האחידים, התשמ"ג–1982 (בסעיף זה – חוזה אחיד), או בתנאי הכלול במידע אחר המיועד לצרכן, לרבות בפרסומת, ובכלל זה הוראות לעניין הגודל המזערי של האותיות כאמור, היחס בינן לבין השטח שבו כלול המידע, ואופן כתיבתן והצגתן; רשימת תנאים מהותיים בחוזה אחיד, הבלטתם ואופן ניסוחם, לרבות החובה לצרף מסמך נפרד לגביהם; הוראות לפי פסקה זו יכול שיהיו לפי סוגי עוסקים או שירותים.

5. (א) היה לשר יסוד סביר להניח כי הדבר קרוש למניעת הטעיה או ניצול מצוקת הצרכן, רשאי הוא לקבוע בתקנות, לגבי סוגי עסקים או שירותים, כי עוסק חייב לערוך חוזה בכתב עם הצרכן ולציין בו את הפרטים שנקבעו בתקנות.

(ב) עוסק, העומד לחתום על חוזה עם צרכן, חייב לתת לו הזדמנות סבירה לעיון בחוזה לפני חתימתו, וכן למסור לו עותק ממנו לאחר החתימה."

חוק הפרטיות האוסטרלי (Privacy Act of 1988, Schedule 1, §1):

"1.3 An APP entity must have a clearly expressed and up-to-date policy (the APP privacy policy) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form."

סעיף 11א להצ"ח פרטיות קטינים:

"11א. (1) מבקש מידע על אודות קטינים יפרסם מסמכי הצהרה על מדיניות הגנת הפרטיות הננקטת על ידו;

(2) נוסח ההודעה כאמור בסעיף 11 תנוסח באופן ברור, תמציתי והולם. היתה בקשת המידע מופנית לקטינים, תהא צורתה מותאמת לגילם, לרבות תוך שימוש בציורים ושפה גרפית.

(3) נוסח הודעה על פי סעיף 11 כאמור תכלול בנוסף אזהרה מודגשת על כי מתן ההסכמה עשוי להביא לפגיעה בפרטיותו של קטין, והסבר בהיר ותמציתי בדבר ההשלכות האפשריות של מתן ההסכמה.

(4) יידוע וקבלת הסכמה להעברת מידע על אודות קטין לגורמים שלישיים יהיו נפרדים מהיידוע וההסכמה לאיסוף המידע. בתהליך היידוע יפורטו הגורמים אליהם עשוי המידע להיות מועבר והמטרות שלשמן הוא יועבר.

(5) על מבקש מידע על אודות קטינים להשקיע מאמצים סבירים, הולמים ונאותים, ולפעול במגוון דרכים העומדות לרשותו על מנת לוודא כי ההסכמה לאיסוף ושימוש במידע על אודות קטין ניתנה על-ידי הגורם המוסמך להעניק הסכמה זו. השימוש במידע הנאסף והמעובד לצורכי תהליכי וידוא אלה יהא אך רק לצורך זה, ואסור למבקש מידע, או מי מטעמו, לעשות שימוש במידע זה לצרכים אחרים, לרבות לצרכים מסחריים."

חוק הפרטיות הקנדי (PIPEDA, Schedule 1, §§4.2):

"4.2 The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected."

PIPEDA – Schedule 1 – סעיף 4.8:

"An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1 Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2 The information made available shall include

(a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

(b) the means of gaining access to personal information held by the organization;

(c) a description of the type of personal information held by the organization, including a general account of its use;

(d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and

(e) what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3 An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number."

סעיפים 13 ו-14 ל-GDPR:

"Article 13 Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

סעיף 13 ל-GDPR - המשך

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14 Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, if any, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, where applicable;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

סעיף 14 ל-GDPR - המשך

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(e) the right to lodge a complaint with a supervisory authority;
(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:
(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:
(a) the data subject already has the information;
(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy."

סימן ב': זכויות נושא המידע

סעיף 10: זכות החזרה מהסכמה

(א) נושא המידע רשאי בכל עת לחזור בו מהסכמתו לפגיעה בפרטיותו לפי סעיף 6(א)(3) או 6(ב)(3) לעיל;

(ב) מבלי לגרוע מהוראות סעיף קטן (א) לעיל, קטין מעל גיל 13 רשאי לחזור בו מהסכמה לפי סעיף 6(א)(3) וקטין מעל גיל 16 רשאי לחזור בו מהסכמה לפי סעיף 6(ב)(3), בין שההסכמה ניתנה על ידו ובין שניתנה על ידי הורה או אפוטרופוס. היה הקטין מתחת לגיל הכשרות למתן הסכמה לפי סעיף 8 לעיל, רשאי אחד מהוריו או אפוטרופוס שנתמנה לו כדין, או לפי הסמכה מפורשת בדין לחזור מהסכמה כאמור.

(ג) חזר נושא המידע מהסכמה כאמור בסעיף קטן (א) או (ב), לא תפגע חוקיות עיבוד המידע שנעשה על בסיס הסכמת נושא המידע עד לאותו מועד.

דברי הסבר

<u>סעיף 10:</u> הסעיף מעגן בהצעת החוק את זכות החזרה מהסכמה של כל אדם, בכלל זה קטין. הסעיף משקף בכך את חיזוק הזכות לפרטיות במובן של השליטה של אדם על מידע אישי עליו ומגביר את התאימות עם ה-GDPR. מובהר שהחזרה של נושא המידע בו מהסכמתו לא תפגע בחוקיות הפגיעה בפרטיות, שנעשתה על בסיס ההסכמה של נושא המידע עד למועד חזרתו בו מהסכמתו. כמו כן מובהר שהפסקת הפגיעה בפרטיות בעקבות החזרה מהסכמה חלה רק כאשר בעל שליטה במידע אינו יכול להראות בסיסים לגיטימיים אחרים לפגיעה בפרטיות המפורטים בסעיף 6.

בקבוצת המומחים הועלתה הטענה שזכות החזרה מהסכמה אינה יכולה להיות מוחלטת. חיזוק לסברה זו נמצא באמרת אגב של השופט סולברג בע"א 8954/11 **פלוני נ' פלונית**,[25] שיש לאפשר חזרה מהסכמה בדיני הגנת הפרטיות לנוכח אופייה האישי של ההסכמה לוותר על הפרטיות ובשל העלאת הזכות לפרטיות לדרגה של זכות יסוד. אף על פי כן, הסביר השופט סולברג באמירת האגב, יש לבחון את מידת הנזק הנגרם למי שהסתמך על הוויתור על הזכות לפרטיות. מתן אפשרות מוחלטת לחזרה בדיעבד מהסכמה לוויתור על הזכות לפרטיות עלול להביא לתוצאות לא רצויות, למשל בכל הנוגע לפרסומים חשובים שיש בהם ממד של פגיעה בפרטיות, בעיקר במישור העיתונאי, הביוגרפי או התיעודי, שבהם החזרה מההסכמה נעשית בשלבים מאוחרים.

לפיכך הוצע בתחילה להוסיף את סעיף קטן (ג), המעגן את זכותו של בעל שליטה במידע לסרב לבקשת נושא מידע לחזור בו מהסכמתו:

"(ג) על אף האמור בסעיף זה, בעל שליטה במידע רשאי לסרב לבקשת חזרה מהסכמה בהתאם להודעה כאמור בסעיף קטן (א), בהתקיים אחד מאלה:

(1) בעל שליטה במידע הסתמך על הסכמת נושא המידע וחזרה מהסכמה תגרום לו לנזק כלכלי משמעותי;

(2) קיימת מניעה טכנולוגית משמעותית להפסיק את הפגיעה בפרטיות.

לבסוף החלטנו בדעת רוב, בהסתייגות של עו"ד רביה, שלא לאפשר לבעל שליטה במידע לסרב לבקשת נושא מידע לחזור בו מהסכמתו. לדעתנו, וכפי שהדבר גם בא לידי ביטוי ב-GDPR, כדי להביא לשינוי תפיסתי ולהפסקת השימוש בהסכמה ככלי חסר משמעות וכ"מכבסה" להתחמקות

מהדרישות של חוק הגנת הפרטיות יש לעגן בחוק זכות מוחלטת לחזרה מהסכמה ולא לאפשר לבעל שליטה במידע לסרב לקבל את בקשת נושא המידע לחזור בו מהסכמתו. בדרך זו נגרום לכך שבעל שליטה במידע המבקש לפגוע בפרטיות יבחן תחילה אם עומדים לרשותו בסיסים לגיטימיים המתירים לו את הפגיעה בפרטיות של נושא המידע ללא הסכמת נושא המידע עצמו. רק בהיעדרם של בסיסים לגיטימיים כאלה יפנה המבקש לפגוע בפרטיות של נושא המידע לקבל את הסכמתו של נושא המידע. אז גם יהיה עליו להיערך מראש לאפשרות שנושא המידע יחזור בו מהסכמתו.

הסעיף שואב השראה מסעיפים דומים בחוקי הגנת פרטיות במידע במדינות אחרות. דוגמאות:

חוק הפרטיות הקנדי (PIPEDA, Schedule 1, §4.3.8):

"An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal."

סעיף 7(3) ל-GDPR:

"Article 7 Conditions for consent

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it."

סעיף 13ב להצ"ח פרטיות קטינים:

"13ב. (1) לכל אדם, לרבות קטין, תהא הזכות לדרוש את ביטול הסכמה שניתנה לשימוש במידע על אודותיו בעת היותו קטין, וזאת ללא תלות בזהות נותן ההסכמה (ההורה או הקטין) או בסוג המידע;

(2) קבלת דרישתו של אדם לחזור מהסכמה שניתנה בעניינו בעת היותו קטין משמעותה הפסקת השימוש במידע, לרבות הפסקת העברתו לצדדים שלישיים, ומחיקתו ממאגר המידע;

(3) סרוב לבקשה יהא משיקולים עניינים שיפורטו ויהיו בכתב. סרב מי שקיבל את ההסכמה לשימוש במידע לבקשת החזרה מההסכמה של אדם, תהא לאותו אדם זכות לערער על סירוב זה בפני בית המשפט המוסמך."

סעיף 11: זכות עיון במידע אישי

(א) כל אדם זכאי לקבל בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, מבעל שליטה במידע מענה לשאלה האם הוא עושה פעולת עיבוד במידע אישי על אודותיו.

(ב) כל נושא מידע זכאי לקבל לידיו ולעיין בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, בכל אחד מאלה:

(1)עותק מהמידע האישי על אודותיו שנעשתה בו פעולת עיבוד;

(2)מידע בנושאים הבאים:

(א) מטרת עיבוד המידע האישי על אודותיו;

(ב) זהותם של מקבלי המידע האישי על אודותיו או הסוגים של מקבלי המידע האישי על אודותיו, שאליהם הועבר או יועבר המידע האישי, ובפרט בנוגע למקבלי מידע אישי במדינות חוץ ומקבלי מידע אישי שהם ארגונים בינלאומיים;

(ג) אם המידע האישי על אודותיו לא נאסף מהמבקש עצמו – זהותו של מקור המידע האישי;

(ג) הגיש נושא מידע בקשה לעיין במידע אישי על אודותיו כאמור בסעיף זה, יידע אותו בעל השליטה במידע על זכויותיו לפי סימן זה.

(ד) המידע האישי המבוקש וכן פרטי המידע הנוספים המבוקשים יימסרו לעיון המבקש בשפה שבה נאסף המידע האישי ובתבנית דיגיטלית מקובלת.

(ה) על אף האמור בסעיף זה, בעל שליטה במידע רשאי לסרב לבקשה לעיון, בהתקיים אחד מאלה:

(1) המידע האישי מתייחס למצבו הרפואי או הנפשי של מבקש העיון, ולדעת בעל השליטה במידע, עיון בו עלול לגרום נזק חמור לבריאותו הגופנית או הנפשית של המבקש או לסכן את חייו; במקרה זה ימסור בעל השליטה במידע את המידע האישי לרופא או לפסיכולוג מטעמו של המבקש;

(2) מתן זכות העיון כמבוקש עלול לדעת בעל השליטה במידע לפגוע בחיי אדם;

(3) מתן זכות העיון כמבוקש עלול לדעת בעל השליטה במידע לפגוע במידה העולה על הנדרש בזכויותיו של צד שלישי שאינו בעל השליטה במידע או המעבד;

(ו) אין בהוראות סעיף זה כדי לחייב למסור מידע אישי בניגוד לחיסיון שנקבע לפי כל דין, אלא אם כן המבקש הוא מי שהחיסיון נועד לטובתו; בפסקה זו, "דין" – לרבות הלכה פסוקה;

(ז) אין בהוראות סעיף זה כדי לחייב למסור מידע אישי בניגוד לדין.

(ח) אין בהוראות סעיף זה כדי לחייב למסור מידע אישי ממאגר מידע המוחרג מסיבות ביטחוניות. **הנושא מצריך דיון נפרד, שאינו בליבת עבודתנו הנוכחית לגיבוש הצעה לחוק הגנת פרטיות חדש ומעודכן.**

דברי הסבר

סעיף 11: הסעיף מבקש להרחיב את זכות העיון הקיימת בסעיף 13(א) לחוק הגנת הפרטיות הקיים על ידי שילובה עם הוראות חוק מן המשפט ההשוואתי, ובראשן סעיף 4.9 ל-PIPEDA בקנדה וסעיף 15 ל-GDPR.

לא כללנו במסגרת הזכות לעיון את הזכות של נושא המידע לדעת אם עיבוד המידע האישי נעשה אוטומטית אם לאו, כאמור בסעיף 15 ל-GDPR, משום שלא כללנו בהצעת החוק את זכותו של נושא המידע להתנגד להחלטות המתקבלות בעקבות עיבוד אוטומטי של מידע אישי.

כמו כן לא כללנו חובה ליידע את נושא המידע על אמצעי האבטחה של מידע אישי כאשר המידע האישי עליו מועבר לחו"ל, משום שלתפיסתנו הדבר נכלל בזכות של נושא המידע לקבל הסבר, המוסדרת בסעיף 12.

בסעיף קטן (א) התייחסנו – מטעמי בהירות – ל"אדם" ולא ל"נושא מידע", משום שבשלב הראשוני, טרם הידיעה אם מידע אישי עליו מעובד, לא בטוח שהפונה הוא נושא מידע.

ס"ק (ב)(2)(ג) קובע כי זכות העיון חלה גם על מקור המידע האישי כאשר המידע לא נאסף מנושא המידע עצמו. בעת הניסוח עלה אצלנו החשש מפני פגיעה בעבודה עיתונאית ובשמירה על החיסיון של מקורות עיתונאיים. ברם חשש זה מטופל בסעיף קטן (ו), הקובע חריג לזכות העיון שמקורו בקיומם של חסיונות, לרבות החיסיון העיתונאי.

לא כללנו בסעיף הוראה לעניין מחירה של זכות העיון בדומה למנגנון הקבוע בסעיף 13(ד) לחוק הגנת הפרטיות הקיים, המפנה לקביעת האופן, התנאים והתשלום למימושה של זכות העיון בתקנות. תקנה 6 לתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א-1981, קובעת סכום תשלום קבוע, אך סכום זה מעולם לא עודכן.

סעיף 13(ד) בחוק הגנת הפרטיות הקיים קובע:

"האופן, התנאים והתשלום למימושה של זכות העיון במידע ייקבעו בתקנות."

תקנה 6 בתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א–1981:

"המבקש לעיין במידע כאמור בתקנות אלה ישלם לבעל או למחזיק של מאגר המידע תשלום בסך 20 שקלים."

סעיף 15(3) ל-GDPR קובע מנגנון שלפיו אין לגבות תשלום בגין העותק הראשון, אבל על כל עותק נוסף רשאי בעל השליטה במידע לדרוש תשלום סביר בהתאם להוצאותיו המינהליות. לדעתנו מנגנון זה אינו מתאים. ראשית, יש בכוחו לפגוע בבעלי שליטה במידע שאינם חברות טכנולוגיה גדולות בשל הוצאות שיושתו עליהם בגין בקשות עיון. שנית, הוא אינו מביא בחשבון את האפשרות של בקשות עיון חוזרות שייחשבו, כל אחת כשלעצמה, כעותק ראשון בשל הדינמיות של עיבוד המידע האישי.

לפיכך עיגנו בסעיף 16(ב) סמכות כללית לעניין קביעת תשלומים בעד מימוש זכות מזכויותיו של נושא המידע.

ס"ק (ד) מבוסס על סעיף 13(ב) לחוק הקיים, אך כדי להימנע מהטלת עלויות כבדות על בעל השליטה במידע או על המעבד מחקנו את הדרישה לספק את המידע האישי באחת משלוש השפות – עברית, ערבית או אנגלית – וקבענו כי המידע האישי יימסר לעיון בשפה שהוא נאסף בה מלכתחילה. כמו כן, כחלק מהרצון ליצור תאימות עם ה-GDPR ומתוך הבנת החשיבות שבהנגשת המידע האישי בתבנית דיגיטלית, הסעיף דורש כי המידע האישי הנמסר לעיון יונגש גם בתבנית דיגיטלית שמקובלת במשק באותה העת.

סעיף קטן (ה) משקף את התפיסה שזכות העיון אינה מוחלטת כפי שהיא באה לידי ביטוי בסעיף 13 לחוק הגנת הפרטיות הקיים.

ס"ק (ה)(1) מבוסס על סעיף 13(ג) לחוק הקיים בשינויים המתחייבים מהסרת ההתייחסות בהצעת החוק למאגרי מידע.

הסייגים בסעיפים קטנים (ה)(1) ו-(ה)(2) שואבים השראה גם מהוראת סעיף 13(ד) לחוק זכויות החולה, התשנ"ו–1996, העוסקת בקבלת הסכמה מדעת והקובעת כי "על אף הוראות סעיף קטן (ב), רשאי המטפל להימנע ממסירת מידע רפואי מסויים למטופל, הנוגע למצבו הרפואי, אם אישרה ועדת אתיקה כי מסירתו עלולה לגרום נזק חמור לבריאותו הגופנית או הנפשית של המטופל."

ס"ק (ה)(2) וגם ס"ק (ה)(3) משקפים את החריג לזכות העיון הקבוע בסעיף 15(4) ל-GDPR ואת הפרשנות שניתנה לו בסעיף 73 להקדמה. עם זאת סברנו כי ההגבלה על זכות העיון בסעיף 15(4) עלולה לגרום פגיעה בזכויות ובחירויות של צדדים שלישיים. ביקשנו, במכוון, לצמצם את החריג, שכן מתן האפשרות לבעל שליטה במידע לסרב לאפשר עיון במידע אישי בנימוק שהעיון עלול לפגוע בזכויות הקניין הרוחני שלו עלול לרוקן את זכות העיון מתוכן. לכן החריג לזכות העיון שהצענו בסעיף קטן (ה)(3) מצומצם יותר ואינו מכיר באפשרות של בעל השליטה במידע לסרב לעיון במידע אישי במקרה שהעיון עלול לפגוע בזכויותיו של בעל השליטה עצמו, למשל בזכויות הקניין הרוחני שלו או של המעבד.

נעיר כי בתחילה הוצע בקבוצת המומחים לצמצם עוד יותר את החריג המוצע בס"ק (ה)(3) ולקבוע שזכות העיון לא תחול כאשר היא עלולה לפגוע במידה העולה על הנדרש בזכויות של צדדים שלישיים שאינם בעל השליטה במידע, המבקש או **מקור המידע האישי**. ואולם במהלך הדיונים הוחלט שלא לאמץ צמצום שכזה – כדי לאפשר את ההחרגה של זכות העיון במקרים שהיא עלולה לפגוע במקור מידע אישי שאינו נהנה מהגנת החיסיון הקבועה בס"ק (ו) להלן, כמו למשל כותב תגובית אנונימי.

ס"ק (ו) הוסף בעקבות הדרישה בסעיף קטן (ב)(2)(ג), המשקפת את סעיף 15(1)(g) ל-GDPR, שזכות העיון תחול גם על מקור המידע האישי כאשר המידע הזה לא נאסף מנושא המידע עצמו. הדרישה למתן זכות העיון למקור המידע האישי עוררה את החשש שחסינות מקור המידע האישי תיפגע, למשל במקרה של מקור עיתונאי. לפיכך מוצע להוסיף את ס"ק (ו), המבוסס על סעיף 13(ג1) לחוק הגנת הפרטיות הקיים ועל סעיף 3(ד)(7) לחוק סדר הדין הפלילי,[26] והמאפשר סירוב לזכות העיון כאשר יש בה כדי להביא לחשיפת מידע אישי שחל עליו חיסיון לפי הדין, לרבות הלכה פסוקה (שהיא המקור בישראל לחיסיון עיתונאי).

נבהיר כי בנסיבות המפורטות בסעיפים קטנים (ו) ו-(ז), כאשר חל על המידע האישי חיסיון או כאשר מסירתו היא בניגוד לדין, לא ניתן לבעל שליטה במידע שיקול הדעת בשאלה אם להתיר את העיון אם לאו, כפי שניתן לו תחת החריגים לזכות העיון המפורטים בסעיף קטן (ה).

בניסוח הסעיף שאבנו השראה מהמקורות שלהלן:

סעיף 13 לחוק הגנת הפרטיות הקיים:

"13.(א) כל אדם זכאי לעיין בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, במידע שעליו המוחזק במאגר מידע.

(ב) בעל מאגר מידע יאפשר עיון במידע, לפי בקשת אדם כאמור בסעיף קטן (א) (להלן – המבקש), בשפה העברית, הערבית או האנגלית.

(ג) בעל המאגר רשאי שלא למסור למבקש מידע המתייחס למצבו הרפואי או הנפשי אם לדעתו עלול המידע לגרום נזק חמור לבריאותו הגופנית או הנפשית של המבקש או לסכן את חייו; במקרה זה ימסור בעל המאגר את המידע לרופא או לפסיכולוג מטעמו של המבקש.

(ג1) אין בהוראות סעיף זה כדי לחייב למסור מידע בניגוד לחסיון שנקבע לפי

כל דין, אלא אם כן המבקש הוא מי שהחסיון נועד לטובתו.

בסעיף קטן זה, "דין" – לרבות הלכה פסוקה.

(ה) הוראות סעיף זה וסעיף 13א לא יחולו –

(1) על מאגר מידע של רשות בטחון כמשמעותה בסעיף 19(ג);

(1א) על מאגר מידע של שירות בתי הסוהר;

2) על מאגר מידע של רשות מס כמשמעותה בחוק לתיקון דיני מסים (חילופי ידיעות בין רשויות מס), תשכ"ז–1967;

(3) כשבטחון המדינה, יחסי חוץ שלה או הוראות חיקוק מחייבים שלא לגלות לאדם מידע שעליו;

(4) על מאגר מידע של גופים אשר שר המשפטים בהתייעצות עם שר הבטחון או עם שר החוץ, לפי הענין, ובאישור ועדת החוץ והבטחון של הכנסת, קבע כי הוא כולל מידע שבטחון המדינה או יחסי החוץ שלה מחייבים שלא לגלותו (להלן - מידע סודי), ובלבד שאדם המבקש לעיין במידע שעליו המוחזק באותו מאגר יהיה זכאי לעיין במידע שאינו מידע סודי;

(5) על מאגר מידע אודות חקירות ואכיפת החוק של רשות המוסמכת לחקור על פי דין בעבירה, אשר שר המשפטים קבע אותה בצו, באישור ועדת החוקה חוק ומשפט של הכנסת;

(6) על מאגר מידע שהוקם לפי סעיף 28 לחוק איסור הלבנת הון, תש"ס-2000."

סעיף 13א(2) לחוק הגנת הפרטיות הקיים:

"13א. בלי לגרוע מהוראות סעיף 13 – בעל מאגר מידע, המחזיק אותו אצל אחר (בסעיף זה – המחזיק), יפנה את המבקש אל המחזיק, תוך ציון מענו, ויורה למחזיק, בכתב, לאפשר למבקש את העיון;

פנה המבקש תחילה למחזיק, יודיע לו המחזיק אם הוא מחזיק מידע עליו, וכן את שם בעל מאגר המידע ואת מענו."

סעיף 15 ל-GDPR:

"Article 15 Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

סעיף 15 ל-GDPR - המשך

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Recital 73: Restrictions of rights and principles
Restrictions concerning specific principles and concerning the rights of information, access to and rectification or erasure of personal data and on the right to data portability, the right to object, decisions based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms."

סעיף 4.9 ל-PIPEDA הקנדי:

"4.9 Principle 9 — Individual Access
Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
4.9.1
Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.
Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege."

סעיף 12 לחוק הפרטיות האוסטרלי:

"Exception to access—agency
12.2 If: (a) the APP entity is an agency; and
(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:
(i) the Freedom of Information Act; or (ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;
then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.
Exception to access—organisation
12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:
(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

סעיף 12 לחוק הפרטיות האוסטרלי - המשך

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

סעיף 12: זכות לקבל הסבר

קיבל בעל שליטה במידע החלטה שיש לה השלכה משמעותית על זכות או חובה על פי דין של נושא מידע, המבוססת, במלואה או ברובה, על עיבוד מידע אישי על אודותיו באמצעות תהליכים ואמצעים אוטומטיים, יהיה נושא המידע זכאי לקבל מבעל שליטה במידע הסבר בהיקף סביר ובשפה מובנית על אופן קבלת ההחלטה.

דברי הסבר

סעיף 12: לפי סעיף 22 ל-GDPR, לנושא המידע יש הזכות שלא תתקבל החלטה בעלת השלכות משפטיות או משמעותיות אחרות עליו – למשל סירוב למתן אשראי או החלטה על גיוס כוח אדם למשרה מסוימת – המבוססת רק על עיבוד אוטומטי של מידע אישי, לרבות יצירת פרופיל אישיות שלו (פרופיילניג).

מימושה של זכות זו נתון לפרשנות שצריכה לבחון מהי מידת המעורבות האנושית הנדרשת מבעל השליטה במידע כדי להיחלץ מגדרי האיסור על קבלת החלטה המבוססת רק על עיבוד אוטומטי של מידע אישי, וכן מהי החלטה בעלת השלכות משפטיות או השלכות משמעותיות אחרות על נושא המידע. לדוגמה: האם ההחלטה של מַפעילת מנוע חיפוש להציג לפני קבוצת אוכלוסייה מסוימת פרסומות מסוימות (למשל, להציג לפני משתמשים שמוצאם אפרו-אמריקני פרסומות לעורכי דין המסייעים במקרה של מעצר או מאסר או פרסומות הנוגעות למחיקת רישום פלילי) היא החלטה שיש לה השלכות משפטיות או משמעותיות אחרות על נושא מידע מסוים?

לפי סעיף 71 להקדמה ל-GDPR, הזכות להתנגד להחלטה המבוססת על עיבוד אוטומטי של מידע אישי כוללת גם את זכותו של נושא המידע לקבל מבעל שליטה במידע הסבר שיכלול את הפירוט של אופן קבלת החלטה המבוססת על ניתוח אוטומטי של המידע האישי עליו. מתן ההסבר ייעשה לאחר קבלת ההחלטה בעניינו של נושא המידע. עם זאת, מאחר שהזכות למתן הסבר קבועה אך ורק בסעיף ההקדמה היא אינה מחייבת.

בצרפת אימצו, בצד הזכות להתנגד להחלטות המבוססות על עיבוד אוטומטי של מידע אישי, גם זכות רחבה להסבר. זכות זו מחייבת כל רשות מינהלית לתת לנושא מידע הסבר בכל הנוגע להחלטות המבוססות על ניתוח אוטומטי של מידע אישי או הנתמכות על ידו. באופן זה הזכות להסבר רחבה יותר מהזכות המבוקשת על פי ה-GDPR, שהיא מוגבלת רק להחלטות המבוססות בלעדית על עיבוד אוטומטי של מידע אישי. לפי החוק הצרפתי, ההסבר צריך לכלול פרטים על היקף התרומה של העיבוד האוטומטי לקבלת ההחלטה ואופן קבלתה, מהו המידע האישי שעובד לצורך קבלת ההחלטה ומהו מקורו, מהם הפרמטרים שנבחנו על ידי האלגוריתם, ובמידת האפשר – מה המשקל שניתן לכל אחד מהם.[27]

בדיוני קבוצת המומחים הוחלט שאין מקום לאמץ זכות כללית המתירה לנושא המידע להתנגד להחלטה רק משום שהיא מבוססת על עיבוד אוטומטי של מידע אישי עליו. הנימוקים שלנו הם שתכליתה של זכות התנגדות כאמור היא, לדעתנו, הזכות לכבוד ולא הזכות לפרטיות, וכן שזכות כללית כזאת מטילה נטל לא מוצדק על חברות מסחריות, שיחויבו להותיר מעורבות אנושית בתהליכים שאפשר לייעלם ולבצעם על ידי שימוש בטכנולוגיה בלבד.

עם זאת הוחלט, ברוב דעות, לאמץ היבט מסוים של הזכות להתנגד. ההיבט המדובר מתמצה בזכות לקבל הסבר כדי למנוע מצב קפקאי שבו ההחלטה המתקבלת בעניינו של נושא המידע אינה ברורה לו ואין ביכולתו להבינה ויש לה

השפעה משמעותית על זכות או חובה שלו על פי דין. בדרך זו יימנע הוויכוח הפרשני הנלווה ליישום סעיף 22 ל-GDPR ובד בבד תתחזק השקיפות בפעולותיהם של בעלי שליטה במידע. לפי הצעתנו, הזכות לקבל הסבר תעמוד לנושא המידע כאשר ההחלטה בעניינו מבוססת במלואה או ברובה על עיבוד מידע אישי עליו באמצעות תהליכים או אמצעים אוטומטיים. לא מצאנו לנכון להגדיר מהם תהליכים או אמצעים אוטומטיים משום שרצינו להבטיח גמישות ומפני שאנו מעוניינים ליצור דבר חקיקה ניטרלי לטכנולוגיה מסוימת.

עיקרה של הזכות לקבלת הסבר הוא יצירת מנגנון שקיפות שיחלחל לכל שדרת הארגון של בעל השליטה במידע או של מעבד מידע אישי ואשר תחייבם לשקול, ואף להנגיש, את הפרמטרים מתוך המידע האישי שבהם נעשה שימוש בעת קבלת החלטה בעניינו של אדם. גם כאשר ההחלטה מתקבלת על ידי טכנולוגיית בינה מלאכותית, יחויב בעל שליטה במידע לפרט בשפה מובנת למי שאינו בעל השכלה טכנולוגית מהו המידע האישי שהטכנולוגיה התבססה עליו ומהם מאגרי המידע הנוספים שעמדו לרשותה ולפרט נתונים נוספים שעמדו לרשותה בעת קבלת ההחלטה או שהתוו את תכנונה ואת התווייתה של הטכנולוגיה. לא הוספנו חובת יידוע לזכות זו באופן ספציפי מאחר שלדעתנו יידוע נושא המידע על הזכויות הנתונות לו מוסדר בסעיף 9 להצעת החוק.

עם זאת דרשנו שההסבר יהיה מידתי מבחינת היקפו. כלומר, המידע שיינתן במסגרת ההסבר לא יפגע במידה העולה על הנדרש בזכויות של בעל השליטה במידע, של המעבד או של צדדים שלישיים, ומנגד – גם לא בזכויות של נושא המידע המבקש הסבר. בדרך זו ההסבר עשוי לכלול נתוני מערכת אם אין במסירתם לנושא המידע פגיעה במידה העולה על הנדרש בבעל השליטה במידע או במעבד; בה בעת יש באי-הכללתם בהסבר משום פגיעה העולה על הנדרש בזכותו של נושא המידע.

בנוסף, לפי סעיף 22 ל-GDPR וביאורו בסעיף 71 לדברי ההקדמה, זכותו של נושא מידע לקבל הסבר קמה דווקא במקרים שאין לו זכות להתנגד לקבלת החלטות אוטומטית שהן בעלות השלכות משפטיות או אחרות עליו. מאחר שהצעת החוק מצומצמת גם כך רק למתן הסבר ולא לזכות להתנגד לקבלת החלטות המבוססות על עיבוד אוטומטי של מידע אישי, אין צורך לדעתנו לאפשר לבעל שליטה במידע לסרב לדרישת ההסבר.

סעיף 71 להקדמה ל-GDPR:

"Recital 71: Profiling

The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent.

סעיף 71 להקדמה ל-GDPR - המשך

In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions."

סעיף 22 ל-GDPR:

"Article 22 Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

סעיף 13: זכות תיקון מידע אישי

(א) נושא מידע שעיין במידע אישי על אודותיו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל השליטה במידע בבקשה לתקן את המידע האישי.

(ב) הוגשה בקשה כאמור בסעיף קטן (א), על בעל שליטה במידע לנקוט את אחת מהפעולות הבאות, בהתחשב במטרה שלשמה בוצע עיבוד המידע האישי וסוג המידע האישי שבו מדובר:

(1)למחוק את המידע האישי, כולו או חלקו;

(2)לתקן את המידע האישי;

(3)להשלים את המידע האישי שבשליטתו;

(ג) בעל השליטה במידע יודיע על הפעולה שנקט לפי לסעיף זה, בתוך 30 יום ממועד נקיטת הפעולה, לכל מי שקיבל ממנו את המידע האישי במהלך תקופה של שנתיים שקדמו למועד קבלת בקשת התיקון.

(ד) על אף האמור בסעיף זה, מצא בעל שליטה במידע שהמידע האישי שבשליטתו נכון, מעודכן ומלא, רשאי הוא לסרב לבקשה כאמור בסעיף קטן (א) ובלבד שינמק את סירובו בכתב.

(ה) מעבד חייב למחוק, לתקן או להשלים את המידע האישי אם בעל שליטה במידע הסכים לתיקון המבוקש או שבית המשפט ציווה על התיקון.

דברי הסבר

סעיף 13: זכות התיקון המוצעת היא שילוב של זכות התיקון הקבועה בסעיף 14 לחוק הגנת הפרטיות הקיים עם זכות התיקון הקבועה בסעיף 16 ל-GDPR ובסעיף 13 לחוק הפרטיות האוסטרלי. מטרת הסעיף היא לעגן את זכותו של אדם לתקן מידע אישי עליו כחלק מתפיסת הפרטיות כשליטה, בצד הכרה בזכותו של בעל שליטה במידע לסרב לתיקון הנדרש.

בחרנו שלא לאמץ במלואה את לשון סעיף 14(א) לחוק הגנת הפרטיות הקיים, ועל כן הגבלנו את האפשרות של נושא מידע לפנות בבקשה על פי סעיף זה רק למקרים שהוא מבקש לתקן את המידע האישי עליו ולא למקרים שהוא מעוניין למחוק את המידע האישי כליל. לדעתנו, אין להפוך את זכות התיקון לזכות מחיקה.

עם זאת, על פי סעיף קטן (ב) המוצע, לבעל השליטה במידע מסור שיקול הדעת אם למחוק את המידע האישי שבענייננו התבקש התיקון, או לתקנו או להשלימו – הכול בהתאם למטרת העיבוד וסוג המידע האישי.

סעיף קטן (ג) קובע שעל בעל שליטה במידע להודיע על הפעולה שנקט בתגובה לבקשת התיקון לכל מי שקיבל ממנו מידע בפרק זמן של שנתיים מיום קבלת בקשת התיקון. כדי להימנע מעיכוב במימוש הסעיף בחרנו לקבוע בניסוח הסעיף תקופת זמן ולא להותיר את קביעת אורך התקופה לתקנות שיותקנו על ידי שר המשפטים, בדומה להוראה הקבועה בסעיף 14(ב) לחוק הגנת הפרטיות הקיים.

סעיף קטן (ד) מעגן את זכותו של בעל שליטה במידע לסרב לבקשת תיקון מידע אישי מנימוקים שיירשמו בהודעת הסירוב אם מצא שהמידע שברשותו מלא, מעודכן ונכון בלי התיקון המבוקש. ידוע לנו שה-GDPR אינו מתיר לסרב לבקשת נושא

מידע לתקן את המידע האישי עליו, ובכל זאת אנו סבורים, בדומה לקבוע בסעיף 14(ג) לחוק הגנת הפרטיות הקיים ולחקיקה האוסטרלית, כי יש להותיר את השאלה אם לתקן את המידע האישי לשיקול דעתו של בעל שליטה במידע ובלבד שפעולות בעל השליטה במידע נעשות במטרה להבטיח שהמידע שבשליטתו תקין, מעודכן, מלא ונכון, וכן מתוך הידיעה שבידי נושא המידע נתונות אפשרויות נוספות על זכות זו לחיזוק שליטתו במידע האישי עליו.

סעיף קטן (ה) קובע הוראה דומה לסעיף 14(ד) לחוק הגנת הפרטיות הקיים, ולפיה על מעבד לפעול בהתאם לפעולת בעל השליטה במידע לפי סעיף קטן (ב).

בדיוני קבוצת המומחים עלתה הטענה שמחיקת ההתייחסות ל"מאגרי מידע" בסעיף המוצע עלולה לגרום שינוי לרעה מבחינת חובת עיתונים ועיתונאים לתקן מידע שפורסם על ידם. בסופו של דבר סברנו ברוב דעות כי אין מדובר בשינוי משמעותי, משום שמבחינה מהותית כבר היום, ובוודאי בעתיד, עיתונים ייחשבו מאגרי מידע כהגדרתם בחוק הקיים, ועל כן זכות התיקון חלה עליהם כבר על פי חוק הגנת הפרטיות הקיים.

בניסוח הסעיף התבססנו על המקורות האלה:

סעיף 14 בחוק הגנת הפרטיות הקיים:

"(א) אדם שעיין במידע שעליו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל מאגר המידע, ואם הוא תושב חוץ – למחזיק מאגר המידע, בבקשה לתקן את המידע או למוחקו.

(ב) הסכים בעל מאגר המידע לבקשה כאמור בסעיף קטן (א), יבצע את השינויים הנדרשים במידע שברשותו ויודיע עליהם לכל מי שקיבל ממנו את המידע בתקופה שנקבעה בתקנות.

(ג) סירב בעל מאגר המידע למלא בקשה כאמור בסעיף קטן (א), יודיע על כך למבקש, באופן ובדרך שנקבעו בתקנות.

(ד) מחזיק חייב לתקן מידע, אם בעל מאגר המידע הסכים לתיקון המבוקש או שבית משפט ציווה על התיקון."

סעיף 16 ל-GDPR:

"Article 16 Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."

סעיף 13 לחוק הפרטיות האוסטרלי:

"13 Australian Privacy Principle 13—correction of personal information

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

סעיף 13 לחוק הפרטיות האוסטרלי - המשך

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information."

סעיף 14: הזכות לניוד מידע אישי

(א) כל נושא מידע זכאי, בהתאם לבקשה שהגיש לבעל שליטה במידע, שבשליטתו המידע האישי על אודותיו, לקבל לידיו מבעל שליטה במידע, את המידע אישי כאמור, בתבנית דיגיטלית מקובלת, ולהעבירו, על פי שיקול דעתו, בעצמו או לפי הוראת סעיף קטן (ד), לכל בעל שליטה במידע אחר (להלן – הזכות לניוד מידע אישי).

(ב) הזכות לניוד מידע אישי חלה על מידע אישי שעובד לפי הוראות סעיף 6 על אודות נושא המידע.

(ג) הזכות לניוד מידע אישי אינה חלה על מידע אישי שבעל שליטה במידע או המעבד הסיקו באמצעות עיבוד שנעשה לפי הוראות סעיף 6.

(ד) הוגשה בקשה לניוד מידע אישי כאמור בסעיף קטן (א), יעביר בעל שליטה במידע את המידע האישי על אודות מבקש הניוד לבעל שליטה במידע המבוקש על ידו, בהתאם לבקשה ובכפוף למגבלות טכנולוגיות. בעל שליטה במידע שאליו ינויד המידע האישי על פי סעיף זה, יהיה כפוף להוראות חוק זה במלואן.

(ה) בעל שליטה במידע שהוגשה לו בקשה לנייד מידע אישי כאמור בסעיף קטן (א), יידע את מבקש הניוד שאין בניוד המידע האישי לפי סעיף זה כדי להביא להפסקת עיבוד מידע אישי על אודותיו, וכי יש באפשרותו של מבקש הניוד לחזור בו מהסכמתו, במידה שניתנה, לפי סעיף 10 לחוק, או לפנות אל בעל השליטה במידע בבקשה למחוק את המידע האישי על אודותיו לפי סעיף 15.

(ו) על אף האמור בסעיף זה, בעל שליטה במידע רשאי לסרב לבקשה לפי סעיף קטן (א), אם לדעתו יש בניוד המידע האישי בהתאם לבקשה כדי לפגוע במידה העולה על הנדרש בזכויותיו של צד שלישי או במילוי חובותיו לפי דין.

(ז) שר המשפטים רשאי לקבוע בתקנות סוגים של בעלי שליטה במידע שהוראות סעיף זה לא יחולו עליהם.

דברי הסבר

<u>סעיף 14:</u> הזכות לניוד מידע אישי היא זכות חדשה. היא עוגנה לראשונה בסעיף 20 ל-GDPR כדי לחזק את שליטתו של נושא המידע במידע אישי עליו, לשכלל את השוק על ידי עידוד התחרות בין בעלי שליטה שונים במידע, להקטין את תלותם של נושאי מידע בפלטפורמות שירותי מידע אחת או בבעל שליטה אחד במידע ולמנוע את הגבלתם לאותה הפלטפורמה או לאותו בעל שליטה במידע.

על פי סעיף 20 ל-GDPR זכות הניוד כוללת שני רכיבים עיקריים: הזכות לקבל עותק מהמידע האישי והזכות להעביר את המידע האישי ממערכת עיבוד אחת לאחרת. זכותו של נושא המידע לקבל עותק מהמידע האישי אינה מותנית בהעברת המידע האישי לספק אחר מסוים. כך נושא המידע יכול לקבל לידיו עותק ולהעבירו למספר ספקים ככל שירצה ולהבטיח את התאימות ביניהם. בנוסף, זכות הניוד מוגבלת למידע אישי שסופק על ידי נושא המידע עצמו בהסכמתו או נוצר על ידי בעל השליטה מתצפית על התנהגותו ופעולותיו של נושא המידע. כלומר, זכות הניוד אינה כוללת את מסקנותיו של בעל השליטה במידע מעיבוד המידע האישי, למשל מידע אישי שבעל השליטה במידע הסיק כתוצאה מניתוח התנהגותו של נושא המידע. על פי פרשנות זו, למשל, הדירוג

של מוכר או קונה באתר אי-ביי הוא מידע אישי שהתגבש בעקבות תצפית על נושא המידע ועל כן ניתן לניוד, אבל הממוצע של הניקוד של כל מוכר או קונה, המחושב על ידי אי-ביי על בסיס הדירוג שניתן לו על ידי קונה או מוכר בעסקה, אינו ניתן לניוד.

הצעת החוק כוללת גם את הזכות לניוד מידע אישי. נעיר כי המונח ניוד אינו מתאר במדויק את מהותה של הזכות, משום שהמידע האישי אומנם מועבר ממקום למקום אך עותק ממנו נשאר בידי בעל השליטה במידע המנייד, והלה יכול אף להמשיך בעיבודו אלא אם (1) נושא המידע חוזר בו מהסכמתו, אם ניתנה, ואין בסיס לגיטימי אחר לפי סעיף 6 לחוק המאפשר את המשך עיבוד המידע האישי; או (2) נתבקשה מחיקת המידע האישי לפי סעיף 15 להצעת החוק. ואולם הואיל והמונח ניוד השתרש כמונח המקובל ב-GDPR ובפרשנות שניתנה לו, מצאנו לנכון להשתמש באותו המונח.

סעיף קטן (א) מחייב את ניוד המידע האישי ישירות לנושא המידע מבקש הניוד או לבעל שליטה במידע אחר על פי בקשת נושא המידע. המידע האישי ינויד על פי סעיף קטן (א) "בתבנית דיגיטלית מקובלת". בכך מתכתב סעיף קטן (א) עם הדרישה בסעיף 20(1) ל-GDPR. ניוד המידע האישי ייעשה בפורמט בשימוש מקובל המוגדר בסעיף 20(1) במילים "structured, commonly used and machine-readable format". נעיר כי הסעיף אינו מבהיר מהו הסטנדרט הטכני הנדרש, ויש להניח כי זהו מושג שיחייב פרשנות של בית המשפט. על פי ההבהרה שסיפקה הוועדה המייעצת ל-GDPR, כאשר אין פורמט בשימוש מקובל בתעשייה מסוימת או בהקשר מסוים, על בעל שליטה במידע לספק את המידע האישי בפורמט פתוח מקובל, כמו למשל XML, בשילוב עם מטה דאטה שימושי ברמת הפירוט הגבוהה ביותר האפשרית.[28]

סעיף קטן (ב) מרחיב את תחולת זכות הניוד מעבר לזו הקבועה בסעיף 20(1) ל-GDPR וקובע כי זכות הניוד תחול על כל מידע אישי על נושא המידע שעובד לפי הוראות סעיף 6 להצעת החוק. לטעמנו, בהיעדר הרחבה זו, זכות הניוד בנוסחה האירופי מצומצמת יתר על המידה. צמצום זה עלול לפגוע בהגשמת המטרה המרכזית של הזכות – שהיא הגברת התחרות בין בעלי שליטה במידע ומניעת מצב של הגבלת נושאי מידע לפלטפורמה אחת בלבד ונעילתם בה.

עם זאת, סעיף קטן (ג) מאמץ את ההגבלה הקבועה בסעיף 20(1) ל-GDPR ומבהיר שזכות הניוד חלה רק על המידע האישי הגולמי על נושא המידע ולא על תוצרי העיבוד. כלומר, זכות הניוד אינה חלה על מידע אישי שבעל השליטה במידע או שהמעבד הסיקו באמצעות עיבוד מידע אישי לפי סעיף 6 להצעת החוק.

סעיף קטן (ד) מתכתב עם הדרישה המופיעה בסעיף 20(2) ל-GDPR שלפיה בעל שליטה במידע יעביר את המידע האישי שלגביו התבקש ניוד לבעל שליטה אחר, בהתאם לבקשת נושא המידע ורק כאשר ההעברה אפשרית מבחינה טכנית (technically feasible). בנוסח המוצע כיוונו לאותו המבחן במילים "אין מניעה טכנולוגית". על פי הפרשנות שניתנה עד כה למבחן ה"אפשרי מבחינה טכנולוגית" הקבוע ב-GDPR, הכוונה היא למצב שאפשר לבצע העברה ישירה בין שני בעלי שליטה במידע בדרך מאובטחת ורק כאשר לבעל השליטה המקבל יש היכולת הטכנית לקבל את המידע האישי. סעיף קטן (ד) מבקש להבהיר עוד כי בעל שליטה במידע שאליו ינויד המידע האישי יהיה כפוף לכלל הוראות הצעת החוק.

סעיף קטן (ה) משקף את דעתנו שצריך לחייב את בעל השליטה במידע ליידע את נושא המידע מבקש הניוד שאין בניוד המידע האישי כדי להביא להפסקת עיבודו או למחיקתו ושלשם כך עליו לחזור בו מהסכמתו, אם ניתנה, לפי סעיף 10 להצעת החוק או לפנות בבקשה למחיקת המידע לפי סעיף 15 להצעת החוק. לחובה זו אין מקבילה ב-GDPR. לדעתנו, היעדר

היידוע עלול ליצור רושם מוטעה שהמידע האישי אינו נמצא עוד בידי בעל השליטה במידע.

סעיף קטן (ו) משקף את סעיף 20(4) ל-GDPR, המגביל את תחולת זכות הניוד ומתיר לבעל השליטה במידע לסרב לבקשת ניוד כאשר היא עלולה לפגוע בזכויותיהם של צדדים שלישיים או במילוי חובותיו של בעל שליטה במידע לפי דין. כדי שלא לאפשר לבעל השליטה במידע או למעבד להתנער בקלות מנתינת זכות הניוד ולהפוך בכך את זכות הניוד לאות מתה, מוצע להבהיר כי החריג המתיר לבעל השליטה או למעבד לסרב לניוד ייקבע לפי מבחן מידתיות.

בקבוצת המומחים עלה החשש שזכות הניוד כפי שהיא מנוסחת היום ב-GDPR עלולה להביא לפגיעה חמורה דווקא בעסקים קטנים ובינוניים, שלא יוכלו להתמודד עם העברת מידע אישי מהם בשלבי הפעילות הראשונית שלהם. לפיכך הזכות עלולה לגרום לחיזוק כוחן של החברות הגדולות ולהחלשת התחרות. משום כך בחרנו לאפשר לשר המשפטים, בסעיף קטן (ז), לקבוע שבעלי שליטה במידע מסוימים יוחרגו מתחולת הסעיף מסיבות הקשורות בגודלם, במשך הזמן שחלף מרגע היווסדם או בנתח השוק שהם מחזיקים בו.

לשון סעיף 20 ל-GDPR:

"Article 20 Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others."

סעיף 15: זכות המחיקה של מידע אישי

(א) כל נושא מידע זכאי לדרוש מבעל שליטה במידע למחוק מידע אישי על אודותיו בהתקיים אחד מאלה:

(1) המידע האישי אינו נחוץ עוד למילוי המטרה שלשמה נאסף;

(2) נושא המידע חזר בו מהסכמתו לעיבוד מידע אישי לפי סעיף 10 ולא מתקיים אף אחד מהתנאים לפי סעיף 6(א)(1)-(2) או 6(ב)(1)-(2) המתירים את המשך עיבוד המידע האישי;

(3) עיבוד המידע האישי נעשה בניגוד להוראות חוק זה.

(ב) בעל שליטה במידע שהתבקש למחוק מידע אישי לפי סעיף קטן (א), ינקוט את הצעדים הסבירים בנסיבות העניין ובהתחשב בטכנולוגיה הקיימת באותה עת ובעלותה, על מנת למחוק את המידע האישי שבשליטתו, ואם העביר את המידע האישי - ליידע כל בעל שליטה אחר אליו העביר את המידע האישי שנושא המידע ביקש למחוק את המידע האישי וכל קישור אליו או העתק שלו;

(ג) על אף האמור בסעיף זה, בעל שליטה במידע רשאי לסרב לבקשת מחיקה לפי סעיף קטן (א), בהתקיים אחד מאלה:

(1) מחיקת המידע האישי תפגע במידה העולה על הנדרש בזכות לחופש ביטוי או בזכות הציבור לדעת;

(2) עיבוד המידע האישי דרוש לשם מילוי חובה חוקית;

(3) מחיקת המידע האישי תפגע במידה העולה על הנדרש ביכולתו של בעל השליטה במידע או המעבד להתגונן בתביעות משפטיות, או לבצע משימה המוטלת עליו למטרות אירכוב, מחקר מדעי, מחקר סטטיסטי שיש אינטרס ציבורי בביצועם.

דברי הסבר

<u>סעיף 15:</u> זכות המחיקה, שבאה במנותק מזכות התיקון, היא זכות חדשה. הזכות עוגנה לראשונה כ"זכות להישכח" בפסיקת בית הדין האירופי לזכויות אדם בשנת 2014 בפרשת **קוסטחה-גונזלס**.[29] באותה פרשה פירש בית הדין בהרחבה את זכות התיקון שהייתה נתונה עד אותו הזמן לנושא המידע מכוח הדירקטיבה.[30] בית הדין פסק שזכות זו כוללת גם את זכותו של נושא המידע לבקש ממנוע חיפוש למחוק את תוצאות החיפוש המתקבלות מחיפוש שמו במנוע החיפוש בנימוק שהמידע המתקבל אינו ראוי, אינו רלוונטי או אינו רלוונטי עוד או מוגזם בהתחשב במטרותיו ובזמן שחלף מאז הפרסום. בהחלטתו התווה בית הדין את מכלול השיקולים שעל מנוע חיפוש לשקול בבואו לבחון בקשה למימוש הזכות להישכח, אם כי ככלל העניק בית הדין למנוע החיפוש שיקול דעת נרחב להכריע בחוסר שקיפות בבקשה.

לפי פסק הדין, על מנוע החיפוש להחליט אם לקבל את הבקשה על בסיס איזון ראוי בין זכותו של נושא המידע לפרטיות לבין האינטרסים של מנוע החיפוש וזכותם של משתמשי האינטרנט להיחשף למידע מתוך התחשבות באופי המידע הנדון, מידת רגישותו לחייו הפרטיים של נושא המידע, התפקיד שנושא המידע ממלא בחברה או חייו הציבוריים של נושא המידע ומשך הזמן שחלף למן מועד ההרשעה ומועד השחרור (אם פרטים אלו רלוונטיים) ועד ליום הגשת הבקשה למחיקה. במסגרת איזון זה מנוע החיפוש יכול להיענות לבקשה להסיר קישור גם אם המידע המופיע באתר המקור שתוצאת החיפוש מקשרת אליו אמיתי, נכון ופורסם באופן חוקי. עם זאת, הזכות

להישכח על פי פסק הדין מוגבלת טריטוריאלית למדינת מגוריו של נושא המידע.

בפרשת **קוסטחה-גונזלס** ייחס בית הדין משקל רב בנימוקיו לחשיבות מנוע החיפוש ככלי בלעדי להנגשת מידע. עוד הוא ייחד משקל רב לעובדה שבאמצעות חיפוש שמו של אדם במנוע חיפוש ניתן ליצור פרופיל מדויק של נושא המידע על ידי חיבור פרטי מידע שונים המפורסמים עליו במקורות שונים ולאורך זמן.

זכות המחיקה שאומצה בסעיף 17 ל-GDPR חלה על המידע האישי שנאסף מנושא המידע וכן המסקנות או התובנות שהוסקו בעניינו,[31] ולא רק על הקישור למידע אישי, כפי שנפסק בפרשת **קוסטחה-גונזלס**. עם זאת, הסעיף מבהיר שזכות המחיקה אינה מתירה לנושא המידע לבקש את מחיקת המידע האישי עליו בכל מקרה שהוא מרגיש שהוא אינו ראוי או אינו רלוונטי יותר, אלא היא מצומצמת למקרים מסוימים המנויים שם: המידע האישי אינו נחוץ עוד להשגת המטרה שלשמה הוא נאסף או עובד; נושא המידע חזר בו מהסכמתו; נושא המידע מתנגד לעיבוד מידע אישי עליו, ואין בסיסים לגיטימיים אחרים המתירים לבעל השליטה במידע להמשיך בעיבוד המידע האישי על פי ה-GDPR; נושא המידע הסכים לעיבוד מידע אישי עליו כאשר היה קטין ולא היה מודע לגמרי לסכנות הנלוות לעיבוד ולאחר מכן מבקש להסיר את המידע האישי; המחיקה נדרשת על פי חוק; או כאשר עיבוד המידע האישי אינו עומד בדרישות ה-GDPR.

הרחבת זכות המחיקה – שהייתה קבועה עוד קודם לכן בדירקטיבה להגנת נתונים של האיחוד האירופי, אבל כחלק מזכות התיקון – ואימוצה של הזכות להישכח באים לידי ביטוי בסעיף 17(2) ל-GDPR. סעיף זה מחייב בעל שליטה במידע שפרסם את המידע האישי בציבור ליידע בעלי שליטה אחרים המעבדים את אותו מידע אישי כי עליהם למחוק את המידע האישי, לרבות כל קישור או העתק שלו. ואולם חובת היידוע כפופה לנקיטת אמצעים סבירים, בכללם אמצעים טכנולוגיים, ומתוך התחשבות בטכנולוגיה הזמינה ובעלות הכספית של יישום חובה זו.

יתר על כן, על פי סעיף 17(3) ל-GDPR, זכות המחיקה אינה מוחלטת אלא נסוגה כאשר המידע האישי נחוץ למימוש הזכות לחופש ביטוי; לציות לחוקים אחרים באיחוד האירופי או במדינה החברה באיחוד האירופי; למשימות שיש אינטרס ציבורי בביצוען, למימוש אינטרס הציבור בתחום בריאות הציבור, למימוש אינטרס הציבור למטרות ארכוב או למימוש אינטרס הציבור למטרות מחקר מדעי, היסטורי או סטטיסטי; לצורך מימוש סמכות רשמית של בעל השליטה במידע; או לצורך ביסוס טענה משפטית או הגנה על טענה משפטית.

בצד היתרונות לכאורה שזכות המחיקה מציגה בבחינת מתן הזדמנות שנייה לאדם ששגה והשתקם והגנה על אדם מפני עימות עם היבטים מסוימים בעברו באופן לא מידתי, הוגן או סביר, נמתחה עליה גם לא מעט ביקורת. נטען כי זכות המחיקה כפי שהוכרה על ידי בית הדין האירופי לזכויות אדם בפרשת **קוסטחה-גונזלס** וכפי שעוגנה בהמשך בסעיף 17 ל-GDPR מעבירה את שיקול הדעת הרגולטורי בביצוע האיזון שבין זכות הציבור לדעת לבין הזכות לפרטיות של נושא המידע לידיים פרטיות בהליך שאינו שקוף. כאשר מדובר במנוע חיפוש, הרי שהוא לא מקור המידע ואין לו אינטרס בהגנה על חופש הביטוי, שכן זה לא תחום פעילותו או שליטתו. למעשה החברה הפרטית – מנוע החיפוש – הופכת לצנזור שעוסק בתוכן המידע המוצג בתוצאות החיפוש.[32] כמו כן הועלה חשש אמיתי שאי-אפשר ליישם הלכה למעשה את הזכות להישכח שכן טכנולוגיות המידע המורכבות דהיום הופכות את מחיקת המידע לכמעט בלתי אפשרית.

עוד נטען כי זכות המחיקה לא בהכרח תורמת לאינטרס של הציבור. ההפך הוא הנכון – היא עלולה לאפשר את שכתוב ההיסטוריה ויצירת מצב שבו המידע שיוצג במנועי החיפוש לא יהיה מהימן ומדויק ולא ישקף כלל את המציאות. פרופ' אמיתי עציוני, למשל, סובר, על בסיס מחקרים

אמפיריים בתחום, שכאשר מדובר בעבריינים המבקשים הזדמנות שנייה, התועלת במידע עמום עליהם היא קטנה שכן רובם מורשעים שוב ושוב. לדעתו, התועלת לחברה בהעלאת הנתונים ובהנגשת המידע באינטרנט גדולה, בעיקר כאשר מדובר בעברייני מין או ברופאים המורשעים בעבירות של רשלנות רפואית. לדוגמה, בית המשפט יכול לדעת אם אחות בבית ספר היא עבריינית מין ומשרד רואה חשבון יכול לדעת מראש אם עובד חדש הורשע בעבר במעילה. לשיטתו של עציוני, אפילו באינטרנט יש תועלת רבה למידע אישי, למשל בהבטחה שמוכר או קונה באי-ביי הוא בעל מוניטין חיובי טוב מסיבות אמיתיות ונכונות ולא שמוניטין זה הושג על ידי שכתוב המידע האישי הקיים עליו באינטרנט.[33]

בקנדה, למשל, לנוכח הביקורת על הזכות להישכח, הוצע לאמץ את הזכות להישכח, אבל במסגרת מינהלית אחרת. נושא מידע המבקש למחוק מתוצאות חיפוש קישור למידע אישי עליו יפנה לנציבות הפרטיות הקנדית בבקשה להישכח. על הנציבות לבחון את הבקשה, ובמסגרת בחינה זו לאזן בין זכותו של נושא המידע לפרטיות לבין זכות הציבור לדעת. אם נציבות הפרטיות תחליט שיש מקום להיעתר לבקשה להישכח, היא תורה למנוע החיפוש להסיר את הקישור האישי.[34]

בישראל הוגשו שתי הצעות חוק פרטיות שביקשו לעגן את הזכות להישכח, אך הן לא הבשילו לכדי חוק.[35] הצעת החוק שהגישו חבר הכנסת אורי מקלב וחבר הכנסת עופר שלח ביולי 2016 ביקשה לאפשר לנושא מידע "הרואה עצמו נפגע" מפרסום לפנות לבית המשפט לקבלת צו להסרת פרסום. אם מתברר שצו שכזה אינו בר אכיפה, הוצע להסמיך את בית המשפט להורות למנוע החיפוש להסיר את הפרסום מתוצאות החיפוש.

"17י. א. נעשה פרסום שיש בו פגיעה בפרטיות באתר המצוי ברשת תקשורת אלקטרונית (בסעיף זה – האתר המפרסם), רשאי אדם הרואה עצמו נפגע מהפרסום לפנות לבית המשפט בבקשה שיורה לאתר המפרסם להסיר את הפרסום הפוגעני.

ב. לא ניתן לבצע צו של בית המשפט כלפי האתר המפרסם, כאמור בסעיף קטן (א), רשאי בית המשפט להורות לספק שירותי אינטרנט על הסרה או חסימה של הקישור לפרסום הפוגעני."

הצעת החוק שהגישה חברת הכנסת מירב בן ארי בפברואר 2017 ביקשה לאפשר לאדם "הרואה עצמו נפגע מפרסום מידע אישי" לפנות ישירות למנוע החיפוש בבקשה להסיר את ההפניה מתוצאות החיפוש.

הצעת חוק הגנת הפרטיות (תיקון – הזכות להישכח), התשע"ז–2017

"17יא. אדם הרואה עצמו נפגע מפרסום מידע אישי ברשת תקשורת אלקטרונית (להלן – מבקש), רשאי לפנות למפעיל מנוע החיפוש שבאמצעות מנוע החיפוש שלו או שבהפעלתו אותר המידע האמור, בבקשה להסיר את המידע.

17יב. סירב מפעיל מנוע חיפוש לבקשה להסיר מידע אישי לפי סעיף 17יא, או לא השיב לפנייה, רשאי המבקש לפנות לבית המשפט בבקשה שיורה למפעיל מנוע החיפוש להסיר את המידע.

17יג. (א) הוכח להנחת דעתו של בית המשפט כי מוצדק בנסיבות העניין להסיר את המידע האישי שלגביו הוגשה בקשה לפי סעיף 17יב, רשאי הוא להורות למפעיל מנוע החיפוש להסיר את המידע האמור.

(ב) לצורך החלטתו לפי סעיף קטן (א) ישקול בית המשפט את מידת הפגיעה שנגרמה או עלולה להיגרם למבקש כתוצאה מפרסום המידע האישי לעומת הפגיעה שנגרמה או עלולה להיגרם לעניין הציבורי כתוצאה מהסרתו בהתחשב, בין השאר, בזהותו של המבקש ובאופיו ורגישותו של המידע האישי.

(ג) הורה בית המשפט כאמור בסעיף קטן (א), יסיר מפעיל מנוע החיפוש את המידע האישי שלגביו הוגשה הבקשה."

שתי הצעות החוק אינן מבהירות את היקפה של הזכות. למשל, לא ברור מתי אדם "רואה עצמו נפגע". בעוד לפי הצעתם של ח"כ מקלב וח"כ שלח

ההחלטה נתונה בידי בית המשפט, הצעתה של ח"כ בן ארי מעניקה דה פקטו סמכות מעין-שיפוטית לפגיעה בזכות לחופש ביטוי לגורמי ביניים, כגון החברות השולטות במנועי חיפוש. עם זאת, בעוד הצעתם של ח"כ מקלב וח"כ שלח מאפשרת את הסרת המידע האישי עצמו, בדומה לקבוע ב-GDPR, הצעת החוק של ח"כ בן ארי מוגבלת להסרת קישור למידע אישי מתוצאות מנוע חיפוש ואינה רחבה כמו זכות המחיקה המעוגנת ב-GDPR.

לאחר בחינת יתרונותיה וחסרונותיה של זכות המחיקה הוחלט בקבוצת המומחים להמליץ על אימוץ מודל מוגבל של הזכות לנוכח יתרונותיה, בגלל העובדה שהיא מיושמת כבר בחלקה על ידי חברות טכנולוגיה שונות כגון גוגל ולשם הגברת התאימות עם ה-GDPR.

סעיף קטן (א) מבוסס על לשון סעיף 17(1) ל-GDPR אך אינו דורש את מחיקת המידע האישי "ללא דיחוי". הסיבה לכך היא ההבנה שביישומה של זכות המחיקה יש לתת את הדעת לאפשרויות הטכנולוגיות העומדות לפני בעל השליטה במידע ולמחירן.

סעיף קטן (א)(1) מבוסס על סעיף 17(1)(a) ל-GDPR ומתכתב עם סעיף 7 בהצעת החוק המגביל את עיבוד המידע האישי לפי דרישת קיום המטרה.

סעיף קטן (א)(2) מבוסס על סעיף 17(1)(b) ל-GDPR ומאפשר את מחיקת המידע האישי במקרה שנושא המידע חוזר בו מהסכמתו לעיבוד המידע, אלא אם יש בסיס לגיטימי אחר לפי סעיף 6 להצעת החוק להמשיך עם עיבוד המידע האישי.

לא אימצנו את אפשרות המחיקה כאשר נושא המידע מתנגד לעיבוד מידע אישי עליו לפי סעיף 17(1)(c) ל-GDPR, משום שבחרנו שלא לאמץ את הזכות להתנגד לעיבוד אוטומטי של מידע אישי.

סעיף קטן (א)(3) משקף את סעיף 17(1)(d) ל-GDPR וקובע שהזכות למחיקה קמה כאשר עיבוד המידע האישי נעשה באופן לא חוקי. עם זאת, בחרנו לקבוע במפורש בנוסח המוצע על ידינו כי זכות המחיקה קמה כאשר נעשה עיבוד מידע אישי בניגוד להוראות הצעת החוק. המניע להצעתנו הוא הרצון לבסס את מרכזיותה של הצעת החוק באסדרת עיבוד מידע אישי ולמקד את המקרים שהמחיקה מותרת בהם למקרים של הפרת הוראות הצעת החוק בלבד.

בחרנו שלא לאמץ את סעיף 17(1)(e) ל-GDPR הקובע שזכות המחיקה תחול כאשר המחיקה נדרשת לשם ציות לחוק במדינת האיחוד. הסיבה לבחירה שלנו היא שהוראה שכזו עלולה להרחיב את מגוון המקרים שתתאפשר בהם בקשת מחיקה למקרים שאינם מצוינים בהצעת החוק, ועל כן היא עלולה גם לפגוע בוודאות המשפטית.

סעיף 17(1)(f) ל-GDPR מתייחס לקיומה של זכות המחיקה כאשר נושא המידע הוא קטין והמידע האישי הושג מתוקף הסכמה שנתן בעודו קטין. לטעמנו, אין לייחד לכך סעיף נפרד בהצעת החוק מאחר שזכות החזרה מהסכמה של קטין מוסדרת במאוחד עם זכות החזרה מהסכמה של כלל נושאי המידע בסעיף 10, וזכות המחיקה הקמה מכוחה של חזרה מהסכמה מוסדרת על ידינו גם בסעיף קטן (א)(2) להלן.

סעיף קטן (ב) מבוסס בחלקו על סעיף 17(2) ל-GDPR. לפי ה-GDPR, ההתחשבות בנסיבות העניין ובטכנולוגיה הקיימת בשאלת הצעדים הסבירים שעל בעל השליטה במידע לנקוט מוגבלת רק למקרים שהוא פרסם את המידע האישי ועליו ליידע בעלי שליטה אחרים על בקשת המחיקה. לדעתנו, בהתחשב בחסרונות וביתרונות של זכות המחיקה, הצעדים שעל בעל שליטה לנקוט עם קבלת בקשת מחיקה – מחיקה, סירוב לפי התנאים המפורטים בסעיף קטן (ג) או יידוע בעלי שליטה נוספים – צריכים להיות כפופים למבחן הסבירות לפי נסיבות העניין, לטכנולוגיה הקיימת באותה העת ולמחירה. הסיבה לכך לדעתנו היא שזכות המחיקה עלולה להתברר בעתיד כנטל לא סביר על חברות הטכנולוגיה.

סעיף קטן (ג) עוסק במקרים שבעל שליטה במידע רשאי לסרב לבקשת

מחיקה והוא מציג גרסה מצומצמת של סעיף 17(3) ל-GDPR.

סעיף קטן (ג)(1) חורג מהוראת סעיף 17(3)(a) ל-GDPR, הקובעת שזכות המחיקה לא תחול כאשר יהיה בה כדי לפגוע בחירויות ובזכויות של צדדים שלישיים. לשיטתנו, הוראה זו אינה מתאימה לתנאי הארץ ותושביה ואף יוצרת כר רחב מידי לפרשנויות. משום כך ביקשנו לעגן את מבחן המידתיות ולצמצם את הפגיעות האפשריות לזכויות לחופש ביטוי ולזכות הציבור לדעת.

סעיף קטן (ג)(2) ו-(3) משקפים באופן מצומצם את הוראת סעיף 17(3)(b) ל-GDPR. בחרנו להתמקד בסעיף קטן (ג)(2) אך ורק בקיומה של חובה חוקית המחייבת את אי-מחיקת המידע האישי. בסעיף קטן (ג)(3) צמצמנו את הסיפא של סעיף 17(3)(b) ואת סעיפים 17(3)(c),(d) ו-(e) בשל החשש שקביעה שהזכות למחיקה תיסוג לעומת אינטרס ציבורי מעורפל ולא ברור די צורכו וכן מפני שמדובר במונח הלקוח מתחום המשפט המינהלי שאינו מתאים למערכת היחסים שבין נושא מידע לבעל שליטה במידע. הנוסח המוצע על ידינו מחדד את הסירוב לזכות המחיקה לנימוקים של התגוננות משפטית, ארכוב, מחקר מדעי או מחקר סטטיסטי שיש אינטרס ציבורי בביצועם ובה בעת מכפיף אותם למבחן של מידתיות.

סעיף 17 ל-GDPR:

"Article 17 Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims."

סעיף 16: מימוש זכויות נושא המידע

(א) בעל שליטה במידע ינקוט אמצעים סבירים כדי לוודא שהמבקש לחזור בו מהסכמתו לפי סעיף 10, לעיין במידע אישי לפי סעיף 11, לקבל הסבר לפי סעיף 12, לתקן מידע אישי לפי סעיף 13, לנייד מידע אישי לפי סעיף 14 או למחוק מידע אישי לפי סעיף 15 (להלן – "זכויות נושא המידע"), הוא אכן נושא המידע, בטרם מתן מענה לבקשה.

(ב) על בעל שליטה במידע לאפשר מימוש זכויות נושא המידע בכתב או בפורמט דיגיטלי ובתבנית מקובלת בתוך 14 ימים ממועד קבלת בקשה למימוש זכות מזכויות נושא המידע. בגין מימוש זכות מזכויות נושא המידע רשאי בעל שליטה במידע לגבות סכום שלא יעלה על ____ שקלים חדשים.

(ג) פנה נושא המידע למעבד בבקשה למימוש זכות מזכויות נושא המידע, יעביר לו המעבד בתוך 14 ימים מיום קבלת הבקשה את שם בעל השליטה במידע שבשליטתו מצוי המידע האישי נשוא הפנייה ואת דרכי הפנייה אליו. אין בהוראת סעיף קטן זה כדי לחייב למסור מידע אישי בניגוד לחיסיון שנקבע לפי כל דין, אלא אם כן המבקש הוא מי שהחיסיון נועד לטובתו. בסעיף קטן זה, "דין" – לרבות הלכה פסוקה.

(ד) סירב בעל שליטה במידע לבקשת נושא מידע למימוש זכות מזכויות נושא המידע, כאמור בסעיפים 11(ה)-(ח), 13(ד), 14(ו), או 15(ג), יודיע על כך למבקש בכתב או בפורמט דיגיטלי ובתבנית מקובלת בתוך 14 ימים ממועד קבלת הבקשה למימוש זכות מזכויות נושא המידע, תוך פירוט הנימוקים לסירוב.

סעיף 17: תובענה לבית המשפט

על סירובו של בעל שליטה במידע לבקשת נושא מידע למימוש זכות מזכויות נושא המידע, כאמור בסעיפים 11(ה)-(ח), 13(ד), 14(ו), או 15(ג), רשאי נושא המידע להגיש תובענה לבית המשפט באופן ובדרך שנקבעו בתקנות.

דברי הסבר

<u>סעיף 16:</u> סעיף קטן (א) מבוסס על חובת הזהירות הקבועה בחוק הפרטיות הניו זילנדי שלפיה טרם מתן מענה לזכות העיון והתיקון יש לוודא שהמבקש הוא אכן נושא המידע.

סעיף 45 לחוק הפרטיות הניו זילנדי (Privacy Act 1993):

"45 Precautions

Where an information privacy request is made pursuant to subclause (1)(b) of principle 6, the agency—

(a) shall not give access to that information unless it is satisfied concerning the identity of the individual making the request; and

(b)shall ensure, by the adoption of appropriate procedures, that any information intended for an individual is received—

(i)only by that individual; or

(ii)where the request is made by an agent of the individual, only by that individual or his or her agent; and

(c)shall ensure that, where the request is made by an agent of the individual, the agent has the written authority of that individual to obtain the information or is otherwise properly authorised by that individual to obtain the information."

סעיף קטן (ב) מבוסס על סעיף 13(ד) לחוק הגנת הפרטיות הקיים הקובע כי "האופן, התנאים והתשלום למימושה של זכות העיון במידע ייקבעו בתקנות." עם זה, הסעיף מרחיב את הוראתו לכלל זכויות נושא המידע ולא רק לזכות העיון. נוסף על כך, כדי להימנע מעיכוב במימוש הוראות החוק עקב המתנה להתקנת תקנות נקבעו בסעיף קטן (ב) המוצע פרקי זמן למימוש כל אחת מזכויותיו של נושא המידע. הסעיף קובע גם מנגנון לגביית תשלום בגין מימוש הזכויות של נושא המידע. מנגנון זה מבוסס על שילוב ההוראות הקבועות בתקנה 6 לתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי דין בערעור על סירוב לבקשת עיון), התשמ"א–1981, ועל סעיף 29א(ד) לחוק הגנת הפרטיות הקיים.

סעיף קטן (ג) מבוסס על סעיף 13א(2) לחוק הגנת הפרטיות הקיים ומבקש להרחיבו לכלל הזכויות הנתונות לנושא מידע על פי הצעת החוק. לפי הסעיף, כאשר נושא המידע פונה למעבד ולא לבעל שליטה במידע בבקשה למלא זכות מזכויותיו לפי הצעת חוק זו, על המעבד להפנותו לבעל שליטה במידע על ידי העברת פרטי יצירת הקשר עם בעל השליטה במידע.

בקבוצת המומחים עלה החשש כי סעיף קטן (ג), חרף היותו סעיף פרוצדורלי, עלול להביא לחשיפת מידע אישי שחל עליו חיסיון, למשל כאשר המעבד הוא חוקר פרטי או עיתונאי עצמאי. במקרה כזה עצם ההעברה של פרטי יצירת הקשר עם בעל שליטה במידע יכולה להיות הודאה בכך שהמעבד אכן מעבד מידע אישי על נושא המידע. משום כך מוצע לכלול סעיף חריג שיתיר למעבד להימנע ממענה הנדרש על פי הסעיף אם המענה יביא לחשיפת מידע שחל עליו חיסיון.

סעיף 13א(2) לחוק הגנת הפרטיות הקיים: "פנה המבקש תחילה למחזיק, יודיע לו המחזיק אם הוא מחזיק מידע עליו, וכן את שם בעל מאגר המידע ואת מענו."

מטרת סעיף קטן (ד) לקבוע הליך זהה למתן הודעת סירוב על ידי בעל השליטה במידע בתגובה לבקשת נושא המידע לממש זכות מזכויות נושא המידע.

<u>סעיף 17:</u> מוצע לקבוע זכות ערעור לבית המשפט על החלטת בעל שליטה לסרב לכל אחת מזכויות נושא המידע (עיון, קבלת הסבר, תיקון, ניוד, מחיקה) – בדומה לסעיף 15 לחוק הגנת הפרטיות הקיים: "על סירובו של בעל מאגר מידע לאפשר עיון כאמור בסעיף 13 או בסעיף 13א ועל הודעת סירוב כאמור בסעיף 14(ג), רשאי מבקש המידע להגיש תובענה לבית המשפט באופן ובדרך שנקבעו בתקנות." בעתיד נידרש לקבוע אם יש להסדיר בחוק עצמו את הערכאה המתאימה לתובענה.

בקבוצת המומחים הוצע לאמץ כלל ברירת מחדל שיקבע כי דיוני בית המשפט בתביעות מכוח הצעת החוק יתקיימו בדלתיים סגורות. בחקיקה זרה אין הוראה דומה, והוחלט להמתין להמלצות ועדת אנגלרד, העוסקת בפומביות הדיון בבית המשפט לעומת הזכות לפרטיות.

סימן ג': חובות בעל השליטה במידע והמעבד

דברי הסבר

לסימן ג': חובות בעל השליטה במידע והמעבד

התפיסה העומדת ביסוד סימן ג' להצעת החוק היא איחוד בין חובות בעל שליטה במידע והמעבד, לפי העניין, בכל הקשור להגנת הפרטיות במידע אישי לבין חובותיהם בעניין אבטחת מידע אישי. תפיסה זו משקפת את הקבוע ב-GDPR. עם זאת, כמפורט להלן, מצאנו לנכון שלא לאמץ את כל ההוראות הקבועות ב-GDPR.

בראש ובראשונה בחרנו שלא לאמץ את סעיפים 24(2)-(3), 40-43 ל-GDPR המעגנים מנגנון של קו-רגולציה. מדובר במנגנון מקובל יחסית במדינות אירופה שאין לו הצלחה בישראל. ה-GDPR מחייב אימוץ קוד התנהגות שיתווה מסגרת לציות ל-GDPR ויאושר על פי הפרוצדורה הקבועה בסעיפים 40-43 על ידי נציבות הפרטיות בכל מדינה. לדעתנו, די בסעיף 19 להצעת החוק המאמץ את סעיף 25 ל-GDPR והמעגן את עקרון הפרטיות באמצעות עיצוב לפרטיות (Privacy By Design). יתר על כן, בישראל החשיבות שבבחינה של השפעת העיבוד על תושבי מדינות אחרות קטנה. כמו כן סברנו שהקמת תתי-גופי אכיפה וולונטריים באמצעות קודים של התנהגות ואישורם יגרום לסרבול בירוקרטי.

לשון סעיף 24 ל-GDPR:

"Article 24 Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller."

בחרנו שלא לאמץ את סעיף 26 ל-GDPR, הקובע שכל אחד מבעלי שליטה במידע במשותף אחראי לקיום הוראות חוק זה ושעליהם לחלק ביניהם מראש ובאופן שקוף את הסמכויות והחובות. אנו סבורים כי הנושא מוסדר בדיני הנזיקין הקיימים.

סעיף 26 ל-GDPR:

"Article 26 Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers."

לא אימצנו את הוראת סעיפים 5(2) ו-30 ל-GDPR הדורשות מבעל שליטה במידע להחזיק בתיעוד של עיבוד המידע האישי כחלק מהוכחת אחריותיות ועמידה בדרישות ה-GDPR. לדעתנו, די בדרישות לתיעוד הגישה ואירועי אבטחה הקבועות בתקנות אבטחת מידע ובסעיף 22. הוספת דרישות תיעוד נוספות תגדיל את הנטל הבירוקרטי המוטל על בעל שליטה במידע ותהא שקולה להחזרת החובה לרישום מאגרי מידע.

סעיף 5(2) ל-GDPR:

"Article 5 Principles relating to processing of personal data

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

סעיף 30 ל-GDPR:

"Article 30 Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;
(f) where possible, the envisaged time limits for erasure of the different categories of data;
(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
(b) the categories of processing carried out on behalf of each controller;
(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;
(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10."

לא אימצנו גם את סעיף 31 ל-GDPR, המטיל חובה לשתף פעולה עם נציבות הפרטיות המדינתית. אנו סבורים כי סעיף שכזה מתאים לדירקטיבה שיש ליישמה בחוק מדינתי ולא לחוק המוצע כאן.

לשון סעיף 31 ל-GDPR:

"Article 31 Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks."

סעיף 18: מעבד המידע

(א) מעבד יפעל על פי הוראות חוק זה ועל פי הנחיות בעל שליטה במידע.

(ב) על בעל שליטה במידע להבטיח שהמעבד נקט את כל האמצעים הדרושים לעיבוד מידע אישי וכיבוד זכויותיו של נושא המידע לפי חוק זה.

דברי הסבר

סעיף 18: מטרת סעיף זה להבהיר שבעל שליטה במידע חייב להבטיח שמעבד מידע אישי שהוא מתקשר עימו נוקט את כל האמצעים הנדרשים על מנת לכבד את זכויותיו של נושא המידע לפי הצעת החוק ולוודא שעיבוד המידע האישי ייעשה לפי הוראות הצעת החוק.

סעיף קטן (א) מבוסס בחלקו על סעיף 29 ל-GDPR, הקובע כי על המעבד לפעול על פי הוראות בעל שליטה במידע, אלא אם נקבע אחרת בחוק במדינה החברה באיחוד האירופי.

סעיף קטן (ב) מבוסס על סעיף 28(1) ל-GDPR, המחייב את בעל השליטה במידע לוודא שהמעבד נקט אמצעים טכניים וארגוניים מספקים על מנת להבטיח שעיבוד המידע האישי ייעשה על פי הוראות ה-GDPR ומתוך הגנה על זכויות נושאי המידע. לא אימצנו את הוראות סעיפים קטנים (2)–(10) לסעיף 28, המחייבות חתימה על חוזה מחייב בין בעל שליטה במידע ובין מעבד, קבלת הוראות בכתב מבעל שליטה במידע והכפפת נושאי תפקידים במעבד לחובת סודיות, משום שלשיטתנו נושאים אלו מוסדרים ממילא בהצעת החוק ובהגדרת המעבד כפועֵל מטעמו ועל פי הוראותיו של בעל השליטה ולכן אין צורך בהתערבות יתרה בניהול מערכת היחסים שבין בעל שליטה במידע למעבד.

סעיף 28 ל-GDPR:

"Article 28 Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

סעיף 28 ל-GDPR - המשך

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing."

סעיף 29 ל-GDPR:

"Article 29 Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law."

סעיף 19: עיצוב לפרטיות

(א) בעל שליטה במידע יתכנן, יעצב ויפעיל, ככל שניתן, באמצעות הטמעת אמצעים טכנולוגיים וכן כללים פנים-ארגוניים, מערכות לעיבוד של מידע אישי, באופן שיבטיח את התאמתן להוראות חוק זה.

(ב) תכנון, עיצוב והפעלה של מערכות לעיבוד של מידע אישי כאמור בסעיף קטן (א), ייעשו בהתחשב בכל אלה: הטכנולוגיות הזמינות באותה עת ועלותן; אופי העיבוד של המידע האישי, וכן היקפו ומטרתו של העיבוד; והסכנות הצפויות לפגיעה בפרטיותו של נושא המידע עקב עיבוד המידע האישי על אודותיו.

דברי הסבר

<u>סעיף 19:</u> מטרת הסעיף היא להטיל על בעל שליטה במידע את החובה להבטיח הטמעה של אמצעי הגנה על פרטיות במידע אישי כבר משלבי התכנון והפיתוח של המערכות לעיבוד מידע אישי, עבור בהטמעתן וכלה בהפעלתן – הכול באמצעות אימוץ הדרישות ל"פרטיות כברירת מחדל" ("privacy by default") ול"עיצוב לפרטיות" ("privacy by design").

עקרונות עיצוב לפרטיות ופרטיות כברירת מחדל אומצו ב-2010 על ידי נציבי הגנת הפרטיות בעולם בכנס ה-32 שהתקיים באותה שנה בירושלים.[36] בבסיסם של העקרונות מונחת ההבנה שיש להטמיע את ההגנה על הפרטיות כברירת מחדל למן העיצוב של מערכות טכנולוגיות המעבדות מידע אישי ועד לתפעול ולניהול של מערכות תקשורת ומידע ממוחשבות, לאורך כל מעגל החיים של המידע האישי. הטמעה זו חיונית להגנה על הפרטיות וצריכה להיעשות באופן יזום מניעתי ולא רק כסעד שלאחר מעשה כשמחדל אבטחה או פגיעה בפרטיות כבר התרחש.

העקרונות לעיצוב פרטיות ופרטיות כברירת מחדל אומצו בסעיף 25 ל-GDPR כדרישות חדשניות שלא היו כלולות במסגרת משטר הגנת פרטיות במידע שקדם להן. בסעיף 78 להקדמה ל-GDPR הוסבר כי אימוץ אמצעים טכנולוגיים וארגוניים המיישמים את עקרונות עיצוב לפרטיות ופרטיות כברירת מחדל הוא הכרחי להגנה נאותה על זכויותיו של אדם בכל הקשור לעיבוד מידע אישי עליו. לדוגמה, על בעל שליטה במידע למזער ככל האפשר את עיבוד המידע האישי, לפעול להתממת מידע אישי, לעבד מידע אישי בשקיפות, לאפשר לנושא המידע לנטר את עיבוד המידע האישי עליו ולשפר תדיר את אמצעי האבטחה. כמו כן, בעיצוב, בתכנות ובבחירת אפליקציות, שירותים או מוצרים המבוססים על עיבוד מידע אישי על בעל שליטה במידע או המעבד להתחשב בזכויותיו של נושא המידע ולוודא שהעיצוב, התכנות, האפליקציות, השירותים או כל טכנולוגיה אחרת המשמשת אותם לעיבוד מידע אישי מסייעים או אינם פוגעים במילוי חובותיהם לפי הצעת החוק.

אימוץ העקרונות של עיצוב לפרטיות ופרטיות כברירת מחדל בחוק הישראלי הוא בעל חשיבות גם באשר לאפשרותה של מדינת ישראל לזכות בהכרה בתאימות (adequacy) הדין הישראלי למשטר הגנת הפרטיות באירופה. על פי סעיף 108 להקדמה ל-GDPR, דווקא במדינה אשר אינה מוכרת כמעניקה הגנה נאותה לפרטיות במידע, יישום אמצעים טכנולוגיים וארגוניים המאמצים את עקרונות עיצוב לפרטיות ופרטיות כברירת מחדל על ידי בעל שליטה במידע ומעבד ישמש מדד להגנה נאותה מצידם על הפרטיות במידע.

סעיף 25 ל-GDPR:

"Article 25 Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article."

סעיף 78 להקדמה ל-GDPR:

"Recital 78: Appropriate technical organizational measures

The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders."

סעיף 108 להקדמה ל-GDPR:

"Recital 108: Appropriate safeguards

In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding."

סעיף 20: תסקיר השפעה על הפרטיות

(א) בעל שליטה במידע יכין תסקיר השפעה על הפרטיות (בסעיף זה – תסקיר ההשפעה על הפרטיות) כאשר בכוונתו לעשות אחד מאלה:

(1) לבצע עיבוד מידע אישי, שבהתחשב בהיקפו ומטרתו, סביר שיביא לפגיעה בזכויות צדדים שלישיים;

(2) לבצע עיבוד מידע אישי בהיקף נרחב העשוי להשפיע על מספר רב של נושאי מידע;

(3) לבצע עיבוד מידע אישי באופן אוטומטי או בעיקר אוטומטי לשם הערכת מאפייני האישיות של נושא המידע וקבלת החלטות בעלות השלכות משמעותיות על זכויות או חובות לפי דין של נושא המידע;

(4) לבצע עיבוד מידע רגיש בהיקף נרחב;

(ב) תסקיר ההשפעה על הפרטיות יכלול התייחסות, בין השאר, להיקף המידע האישי הנאסף, לעיצוב לפרטיות לפי סעיף 19 ולאמצעי אבטחת מידע אישי שינקטו על ידי בעל שליטה במידע לפי סעיף 21.

(ג) תסקיר ההשפעה על פרטיות לפי סעיף קטן (א) יוכן לפני תחילת העיבוד של המידע אישי, לפני אימוץ טכנולוגיה חדשה לעיבוד המידע אישי, וכן אחת ל-18 חודשים לפחות.

דברי הסבר

<u>סעיף 20:</u> החובה לערוך סקר סיכונים לפגיעה בפרטיות קיימת כיום חלקית – בתקנות אבטחת מידע – ומוגבלת אך ורק למאגרי מידע שנדרשת בהם רמת אבטחה גבוהה.[37] בסעיף 20 המוצע בחרנו לעגן בהצעת החוק, נוסף על החובה הקבועה בתקנות אבטחת מידע, חובה כללית על בעל שליטה במידע לערוך סקר סיכונים. בעתיד נפעל להצעת תיקון לתקנות אבטחת מידע לפי המוצע בסעיף זה. ואולם לעת עתה, על מנת להציג את התמונה המלאה של מכלול התיקונים המוצעים, בחרנו להציג את הסעיף הזה כחלק מהצעת החוק.

סעיף 35 ל-GDPR מטיל על בעל שליטה במידע את החובה לערוך סקר סיכונים לפגיעה בפרטיות אם יש סבירות גבוהה לסיכון זכויותיו וחירויותיו של אדם, ובהתחשב באופי, בהיקף, בהקשר ובמטרה של עיבוד המידע האישי, וכאשר העיבוד נעשה בטכנולוגיות חדשות. הסעיף גם מפרט רשימה פתוחה של מקרים שנדרשת בהם עריכת סקר סיכונים לפגיעה בפרטיות: (1) הערכה שיטתית ומקיפה של מאפייני האישיות של נושא המידע, המבוססת על עיבוד אוטומטי, לרבות פרופיילינג, ואשר על בסיסה מתקבלות החלטות בעלות השלכות משפטיות או השלכות משמעותיות ברמה דומה על נושא המידע; (2) עיבוד בהיקף נרחב של מידע רגיש; או (3) ניטור שיטתי ובהיקף נרחב של אזורים ציבוריים.

בסעיף 91 להקדמה ל-GDPR מוסבר שסקר סיכונים נדרש בעיקר כאשר עומד להתבצע עיבוד מידע אישי בהיקפים נרחבים שעשוי להשפיע על מספר רב של נושאי מידע ואשר יש סבירות גבוהה שהוא יסכן את זכויותיהם. עוד מוסבר בהקדמה כי אין לערוך סקר סיכונים כאשר מדובר בעיבוד מידע אישי על מטופלים או לקוחות על ידי מטפל יחיד או עורך דין.

בסעיף קטן (א) בחרנו לעגן חובה כללית על בעל שליטה במידע לערוך תסקיר השפעה על הפרטיות בהתאם לפעולות

העיבוד שבעל השליטה במידע מבקש לעשות, בדומה למפורט בסעיף 35(1) ו 35(3) ל-GDPR: על פי מבחן סבירות שיתחשב במטרת העיבוד, בהיקפו ובסוג המידע האישי המעובד; כאשר נעשה עיבוד שיטתי ובהיקף נרחב של מידע אישי ומידע רגיש, בכלל זה ניטור נושא המידע ברשות הציבור וברשות היחיד, שסביר שיוביל לפגיעה בזכויות צדדים שלישיים או שישפיע על מספר רב של נושאי מידע; או כאשר נעשה עיבוד שיטתי ובהיקף נרחב של מידע אישי למטרת קביעת פרופיל אישיותי של נושא המידע ושעל בסיסו מתקבלות החלטות הנוגעות לו.

בדומה להוראת ה-GDPR, המחילה את החובה לעריכת תסקיר השפעה על פרטיות רק על בעל שליטה במידע, ובהתאם להוראת סעיפים 5 ו-19 לתקנות אבטחת מידע, המחילות את חובת עריכת סקר הסיכונים ותסקיר הפרטיות על בעל ומנהל מאגר מידע אך לא על מחזיק המאגר, בחרנו לקבוע שהוראת סעיף זה חלה על בעל שליטה במידע. החלת ההוראה על מעבד תיעשה מכוח חובתו של בעל שליטה במידע להבטיח כי המעבד יפעל בהתאם להוראות הצעת החוק לפי סעיף 18 להצעת החוק.

סעיף קטן (ב) מבקש להבהיר שבביצוע תסקיר ההשפעה על הפרטיות ייבחנו, בין השאר, אמצעי הנדסת הפרטיות ואבטחת מידע אישי שבעל שליטה במידע מיישם כפי שנדרש ממנו לפי סעיפים 19 ו-21.

בניסוח הסעיף התבססנו על דברי החקיקה שלהלן:

סעיף 5 לתקנות אבטחת מידע:

"מיפוי מערכות המאגר וביצוע סקר סיכונים

5. (א) בעל מאגר מידע יחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, ובכלל זה:

(1) תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע;

(2) מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו;

(3) תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן;

(4) תרשים הרשת שפועל בה המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה;

(5) תאריך העדכון האחרון של המסמך ושל רשימת המצאי.

(ב) המסמך המעודכן של מבנה מאגר המידע ורשימת המצאי יישמרו כך שפרטים מהם יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.

(ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן – סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשר חודשים לפחות.

(ד) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערכו מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, אחת לשמונה עשר חודשים לפחות; בעל המאגר ידון בתוצאות מבדקי החדירות ויפעל לתיקון הליקויים שהתגלו, ככל שהתגלו.

(ה) ארגון שהוא בעל כמה מאגרי מידע, רשאי לקבוע את רשימת המצאי כאמור בתקנת משנה (א), במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה וכן רשאי לקיים את החובות הקבועות בתקנות משנה (ג) ו-(ד) בסקר סיכונים או במבדק חדירות, לפי העניין, אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת האבטחה."

סעיף 19 לתקנות אבטחת מידע:

"19. (א) החובות החלות בתקנות אלה על בעל מאגר מידע, יחולו גם על מנהל המאגר, ולמעט החובות הקבועות בתקנות 2 ו-15(א) – הן יחולו גם על מחזיק המאגר, בשינויים המחויבים ולפי העניין.

(ב) מי שמוטלת עליו בתקנות אלה חובה או אחריות לביצוע פעולה שאינה יצירת מסמך, נדרש לתעד באופן סביר את אופן ביצוע הפעולה לפי העניין; הרשם רשאי לתת הוראות לעניין אופן תיעוד כאמור."

סעיף 35 ל-GDPR:

"Article 35 Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

סעיף 35 ל-GDPR - המשך

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations."

סעיף 36 ל-GDPR:

"Article 36 Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health."

סעיף 91 להקדמה ל-GDPR:

"Recital 91: Necessity of a data protection impact assessment

This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory."

סעיף 21: אבטחת מידע אישי

בעל שליטה במידע או מעבד יהיו אחראים, ביחד ובנפרד, לאבטחת המידע האישי שבשליטתם או ברשותם וינקטו אמצעים סבירים לצורך אבטחתו, בהתאם לתקן מקובל של אבטחת מידע ולעלותו הכספית, ובהתחשב בסוג המידע האישי, מטרת העיבוד, היקפו, הסכנות הצפויות לפגיעה בפרטיות עקב שימוש לרעה בו, אובדן, שינוי, גילוי, גישה בלתי מורשית אליו או מחיקה בלתי חוקית או מקרית שלו.

דברי הסבר

סעיף 21: הסעיף המוצע מבוסס על סעיף 17 לחוק הגנת הפרטיות הקיים. הוא מבקש לעגן חובת אבטחת מידע כללית בהתאם לתקן המקובל של אבטחת מידע, כמו למשל התקנים המוגדרים בתקנה 1 לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001, וכן לפי מבחן סבירות שיתחשב גם בסוג המידע האישי, מטרת העיבוד והיקפו ובסכנות הצפויות לפגיעה בפרטיות – בדומה למבחן שמשתמשים בו בחוק הפרטיות הקנדי וב-GDPR. כמו כן, בדומה לנוסח המקובל בסעיף 32(1)(b) ל-GDPR, שילבנו את חובת השמירה על סודיות המידע האישי כחלק מהחובה לאבטחת המידע האישי – על מנת להגדיל את תאימותה של הצעת החוק ל-GDPR.

במסגרת החובה הכללית המוצעת בסעיף יוכל בעל שליטה במידע או מעבד לפעול על פי הנדרש בתקנות אבטחת מידע, המטילות על מחזיק או מנהל מאגר מידע חובות אבטחת מידע בחלוקה לשתי רמות של אבטחת מידע: בינונית וגבוהה. ברמה הבינונית יש מאגרי מידע המיועדים למסירת מידע אישי לאחֵר, בכלל זה לדיוור ישיר, מאגרי מידע בבעלות ציבורית ומאגרי מידע המכילים מידע רגיש. הרמה הגבוהה נבדלת מן הרמה הבינונית במספר מורשי הגישה או במספר נושאי המידע.

אנו סבורים כי יהיה צורך להתאים את רמות האבטחה הקבועות בתקנות אבטחת מידע להצעת החוק, אשר אינה מאזכרת מאגרי מידע. היות שהתהליך של התקנת התקנות לאבטחת מידע נמשך שנים רבות, אנו מוצאים שהתקנות היום אינן צופות פני עתיד. לכן צריך לתקן גם אותן, ובעתיד נפעל להציע הצעת תיקון לתקנות אבטחת מידע בהתאם למוצע בסעיף זה. באיחוד האירופי נקבע שיש לנקוט את האמצעים הטכנולוגיים והארגוניים המתאימים על מנת להבטיח רמת אבטחה מתאימה לסיכון. סעיף 32(1) ל-GDPR מפרט רשימה פתוחה של אמצעים הנחשבים מתאימים. אנו סבורים כי אין עוד משמעות לכמות המידע האישי שעובר עיבוד או לעיבוד בקטגוריות מידע אישי מסוימות בלבד כדי לשמש אבן הבוחן לרף האבטחה הרצוי. באוסטרליה ובניו זילנד רף אבטחת המידע נקבע על פי מבחן סבירות ההגנה נגד אירועי אבטחה מסוימים. בקנדה רמת האבטחה נקבעת על פי רגישות המידע, כמותו, הפצתו, הפורמט שהוא נשמר בו וצורת שמירתו. החוק הקנדי קובע רף מינימלי שלפיו אמצעי האבטחה צריכים לכלול אמצעים פיזיים, ארגוניים וטכנולוגיים.

סעיף 17 לחוק הגנת הפרטיות הקיים:
"בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע."

סעיף 19 לתקנות אבטחת מידע קובע שחובות אבטחת המידע המפורטות בתקנות חלות על בעל מאגר מידע, מחזיק או מנהל מאגר מידע וכי על הנושא בנטל חובות אלו לתעד באופן סביר את דרך ביצוע הפעולות, לפי העניין.

תקנות אבטחת המידע התוספת הראשונה והשנייה:

"תוספת ראשונה – מאגרי מידע שחלה עליהם רמת האבטחה הבינונית:

מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק, לרבות שירותי דיוור ישיר.

מאגר מידע שבעליו הוא גוף ציבורי כמשמעותו בסעיף 23 לחוק;

מאגר מידע הכולל מידע שהוא אחד מאלה:

מידע על צנעת חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד;

מידע רפואי או מידע על מצבו הנפשי של אדם;

מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א–2000;

מידע אודות דעותיו הפוליטיות או אמונתיו הדתיות של אדם;

מידע אודות עברו הפלילי של אדם;

נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007;

מידע ביומטרי;

מידע כלכלי על אדם לרבות אודות הרגלי הצריכה של אדם.

על אף האמור בפרט 1(3), על מאגר המקיים אחד מאלה, לא חלה רמת האבטחה הבינונית;

המאגר כולל מידע מן הסוגים המפורטים בפרט 1(3)(ב), (ה), (ו) ו-(ז) לעניין תמונות פנים בלבד, (ח), אודות המועסקים או הספקים של בעל מאגר המידע, ובלבד שהמידע משמש למטרות ניהול העסק בלבד, ואינו כולל מידע מן הסוגים המפורטים בפרט 1(3)(א), (ג), (ד) ו-(ז) לעניין מידע שאינו תמונות פנים;

מספר המועסקים אצל בעל המאגר אינו עולה על עשרה.

תוספת שנייה – מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה:

מאגר כאמור בפרט 1(1) או (3) בתוספת הראשונה, שיש בו מידע אודות 100,000 אנשים ומעלה;

מאגר מידע כאמור בפרט 1(1) או (3) בתוספת הראשונה שמספר מורשי הגישה למידע בו עולה על 100."

חוק הפרטיות הקנדי PIPEDA – Schedule 1 – סעיף 4.7:

"Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3 The methods of protection should include

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3)."

סעיף 11.1 לחוק הפרטיות האוסטרלי:

"11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure."

סעיף 5 לחוק הפרטיות הניו זילנדי:

"An agency that holds personal information shall ensure—
that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—
loss; and
access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
other misuses; and
that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information."

סעיף 32 ל-GDPR:

"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law."

סעיף 22: תיעוד ודיווח על אודות אירוע אבטחה

(א) בעל שליטה במידע אחראי לתיעוד כל אירוע אבטחה שאירע בנוגע למידע האישי שבשליטתו; תיעוד כאמור יבוסס, ככל האפשר, על רישום אוטומטי.

(ב) בעל שליטה במידע ידווח לרשות להגנת הפרטיות על אירוע אבטחה תוך זמן סביר מהמועד שנודע לו על התרחשותו, בהתקיים אלה:

(1) אירוע האבטחה הוביל לעיבוד לא מורשה של מידע אישי או לנסיבות שסביר להניח שיגרמו לעיבוד לא מורשה של מידע אישי;

(2) סביר להניח שאירוע האבטחה יגרום נזק חמור לנושא המידע;

(3) בעל השליטה במידע אינו יכול למנוע את הנזק החמור לנושא המידע באמצעות נקיטת פעולה מתקנת;

בסעיף זה, "פעולה מתקנת"– פעולה שעל בעל שליטה במידע לנקוט לבירור הסיבות שהובילו לאירוע האבטחה, למניעת הישנות אירוע האבטחה ולמיזעור השלכות אירוע האבטחה על זכויות של נושא המידע לפי חוק זה.

(ג) לאחר הדיווח לרשות להגנת הפרטיות כאמור בסעיף קטן (ב), יודיע בעל שליטה במידע לנושא המידע, תוך זמן סביר, על אירוע האבטחה, אלא בהתקיים אחד מאלה:

(1) מתן ההודעה עלול להביא לחשיפת מידע אישי שחל לגביו חיסיון לפי כל דין, אלא אם כן נושא המידע הוא מי שהחיסיון נועד לטובתו; בפסקה זו, "דין" – לרבות הלכה פסוקה;

(2) מתן הודעה כאמור לכל נושא מידע העלול להיפגע מאירוע האבטחה מטיל על בעל שליטה במידע נטל בלתי סביר; במקרה זה, יפרסם בעל שליטה במידע הודעה לכלל הציבור על אודות אירוע האבטחה.

(ד) אירע אירוע אבטחה, יודיע על כך המעבד לבעל שליטה במידע באופן מיידי.

(ה) שר המשפטים יקבע תקנות בעניינים הבאים:

(1) סוגי אירועי אבטחה וסוגי בעלי שליטה במידע הפטורים מחובת הדיווח לפי סעיף קטן (ב);

(2) אופן מתן ההודעות לפי סעיפים קטנים (ב) עד (ד) ותוכנן.

(3) מהן הפעולות המתקנות שעל בעל שליטה במידע לנקוט במקרה של אירוע אבטחה.

דברי הסבר

סעיף 22: הסעיף מעגן בחקיקה ראשית את החובה לתעד אירועי אבטחת מידע אישי הקבועה כיום בתקנה 11 לתקנות אבטחת מידע ואף להוסיף עליה, בהתבסס על עקרונות מרכזיים המופיעים בסעיפים 33 ו-34 ל-GDPR ובתיקון לחוק הגנת הפרטיות במידע האוסטרלי.[38] בעתיד נפעל לקדם הצעת תיקון לתקנות אבטחת מידע בהתאם למוצע בסעיף זה. ואולם לעת עתה, כדי להציג את התמונה המלאה של מכלול התיקונים המוצעים, בחרנו להציג את הסעיף הזה כחלק מהצעת החוק.

סעיפים 33 ו-34 ל-GDPR מטילים על המעבד את החובה לדווח לבעל שליטה במידע על פרצת אבטחה הפוגעת במידע אישי ועל בעל שליטה במידע את החובה לדווח לרשות האחראית על פרצת אבטחה הפוגעת במידע אישי בתוך 72 שעות מגילויה, אלא אם פרצת האבטחה אינה צפויה לפגוע בזכויותיו של מאן דהוא.

על פי סעיף 34(1) ל-GDPR, על בעל שליטה במידע לדווח ללא דיחוי לנושא המידע על פרצת האבטחה אם פרצת האבטחה עלולה, בסבירות גבוהה, להביא לפגיעה בזכויותיו. סעיף 34(2) ל-GDPR מפרט מה צריך לכלול דיווח כאמור לנושא המידע. חובת הדיווח לנושא המידע לא תקום בהתקיים אחת מהנסיבות המפורטות בסעיף 34(3) ל-GDPR, כמו למשל כאשר בעל שליטה במידע יישם אמצעים טכנולוגיים או ארגוניים להגנה על המידע האישי שנפרץ, בייחוד אמצעים ההופכים את המידע האישי למידע שאי-אפשר לקשרו לנושא מידע מסוים או שאינם מתירים גישה לא-מורשית למידע האישי; או כאשר הדיווח לנושא המידע יחייב מאמץ לא סביר מצד בעל שליטה במידע. במקרה כזה על בעל שליטה במידע לדווח בפומבי על פרצת האבטחה. אם בעל שליטה במידע לא דיווח לנושא המידע על פרצת האבטחה, הנציבות האחראית רשאית לדרוש זאת ממנו.

סעיף 33(5) ל-GDPR מחייב את בעל השליטה במידע לתעד את כל פעולותיו מרגע גילוי פרצת האבטחה אגב הסתרת מידע אישי. התיעוד ישמש את הנציבות האחראית בבדיקה אם בעל שליטה במידע ציית להוראות ה-GDPR.

חוק הגנת הפרטיות במידע באוסטרליה תוקן בחודש פברואר 2017, והוספו בו הוראות לעניין דיווח על פרצת אבטחה. על פי התיקון, יש חובת דיווח על אירוע אבטחה כאשר: (1) אירוע אבטחה הוביל לחשיפה לא-מורשית של מידע אישי או לגישה לא-מורשית אליו שסביר שיגרמו נזק חמור לנושא המידע; או (2) המידע האישי אבד בנסיבות שסביר שתתרחש בהן גישה לא-מורשית למידע האישי או חשיפה לא-מורשית של המידע האישי, וסביר שהיא תגרום נזק גדול לנושא המידע.

לפי החוק האוסטרלי חובת הדיווח נסוגה כאשר בעל השליטה במידע מבצע פעולות מתקנות. פעולות מתקנות הן פעולות מניעה שננקטות כלפי הגישה למידע האישי או החשיפה הלא-מורשית של המידע האישי קודם שנגרם נזק חמור לנושא מידע.

הצורך בהוראה ברורה בישראל למקרים שבהם יש לדווח לרשות להגנת הפרטיות ולנושא המידע מתחדד לנוכח גילוי פרצת האבטחה החמורה במערכות של חברת איתוראן בחודש מאי 2018, שם לא דיווחה החברה לרשות להגנת הפרטיות על פרצת האבטחה.[39]

הסעיף המוצע מבקש לתקן את ההסדר הקבוע בתקנות אבטחת מידע בעניין מתן הודעה לנושא מידע ולראש הרשות להגנת הפרטיות. תקנות אבטחת מידע מטילות את חובת הדיווח לנושא מידע רק במקרה של אירוע אבטחה חמור ורק כאשר ראש הרשות להגנת הפרטיות, לאחר היוועצות עם ראש מערך הסייבר, הורה על מתן

הודעה כאמור. בקבוצת המומחים הועלה החשש שחובת ההיוועצות עם ראש מערך הסייבר תגרום סרבול בירוקרטי מיותר ובה בעת שחובת דיווח מיידית לנושאי המידע עלולה להוביל לחשיפת אירועי סייבר באופן שעלול לפגוע בהתמודדות עם האירוע בזמן אמת. ביקשנו אפוא להימנע מהטלת נטל לא סביר על בעלי שליטה במידע לדווח על כל אירוע אבטחה שלא הוביל לפגיעה בזכות לפרטיות (למשל, כאשר עובד לקח לביתו בטעות התקן נייד הנושא מידע אישי אך לא השתמש בו והחזירו למוחרת היום למקום העבודה). כמו כן ביקשנו להימנע מהפיכת פעולת הדיווח לפעולה טכנית בעיקרה ומהצפת הרשות להגנת הפרטיות.

לפיכך מוצע לקבוע שחובת הדיווח לרשות להגנת הפרטיות תקום רק כאשר מתקיימים התנאים המפורטים בסעיף קטן (ב), בדומה לקבוע בתיקון לחוק הפרטיות האוסטרלי. עו"ד רביה סבר, בדעת מיעוט, שניסוח סעיף קטן (ב)(1) עדיין רחב מדי ושיש להגביל את הדיווח לרשות להגנת הפרטיות רק לאירוע אבטחה המביא לעיבוד לא-מורשה של מידע אישי בהיקף משמעותי. לדעתנו, החשש מפני הצפת הרשות להגנת הפרטיות בדיווחים על אירועי אבטחה מינוריים מקבל מענה בסעיף קטן (ה) המוצע.

מוצע גם לקבוע בסעיף קטן (ג) שחובת דיווח לנושא מידע תקום בתוך זמן סביר לאחר הדיווח לרשות להגנת הפרטיות, לפי סעיף קטן (ב). לחלופין מוצע שחובת מתן הודעה פומבית תחול רק כאשר הודעה לכל נושא מידע שעלול להיפגע מאירוע האבטחה תחייב מאמץ לא סביר מבעל שליטה במידע.

סעיף קטן (ד) מבהיר שעל המעבד לדווח לבעל שליטה במידע, בדומה למוצע בסעיף 33(2) ל-GDPR. לדעתנו, חיוב המעבד לדווח לבעל שליטה במידע ולא ישירות לרשות להגנת הפרטיות עולה בקנה אחד עם חלוקת החובות המוצעת בהצעת החוק והדומה לזו הקבועה ב-GDPR.

לא החרגנו גופים ציבוריים המנויים בסעיף 13 לחוק הגנת הפרטיות הקיים מחובת מתן הודעה משום שהנושא טרם נדון בקבוצת המומחים.

סעיף קטן (ה)(1) מיועד לתת מענה למצבים שבהם אין טעם להחיל חובת תיעוד ודיווח, כמו למשל כאשר פרצת האבטחה הובילה לחשיפת פרטים אישיים של מספר לקוחות מועט של מכון היופי השכונתי. הסעיף מתכתב עם ההבחנה הקיימת בתקנות אבטחת מידע שלפיה חובת התיעוד והדיווח תחול רק במקרים של "אירוע אבטחה חמור". בחרנו שלא לאמץ מונח זה מאחר שהצעת החוק אינה מתייחסת למאגרי מידע ולבחינה כמותית של המידע האגור בהם, וכן מכיוון שביקשנו להותיר את שיקול הדעת בידי שר המשפטים כדי שהוא שיקבע רשימה ברורה של עוסקים ושל אירועי אבטחה שיש להחריג מגדר תחולת הסעיף.

כדי להגביר את הגמישות בהחלת חובת הדיווח לפי הוראת סעיף 22 הותרנו בסעיפים קטנים (ה)(2) ו-(ה)(3) את הקביעה מה יכלול דיווח על אירוע אבטחה ומהי פעולה שתיחשב "פעולה מתקנת" לתקנות. ככלל, דיווח כאמור צריך לכלול פרטים מזהים ופרטי יצירת קשר עם בעל שליטה במידע, תיאור של אירוע האבטחה ונסיבותיו, תיאור של המידע האישי שעובד או סביר שיעובד ללא הרשאה בעקבות אירוע האבטחה ופירוט הפעולות המתקנות שביצע בעל שליטה במידע עד למועד הדיווח ואלו שהוא עתיד לבצע. בדיווח לנושא המידע יש לכלול גם את פרטי הפעולות שרצוי שנושא המידע יבצע עקב אירוע האבטחה.

המקורות ששימשו אותנו בניסוח הסעיפים:

סעיף 11 לתקנות אבטחת מידע:

"תיעוד של אירועי אבטחה

11.(א)בעל מאגר מידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לעיבוד בו בלא הרשאה או לחריגה מהרשאה (להלן –

אירועי אבטחה); ככל האפשר יבוסס התיעוד האמור על רישום אוטומטי.

(ב)בנוהל האבטחה יקבע בעל מאגר מידע גם הוראות לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

(ג)במאגר מידע שחלה עליו רמת האבטחה הבינונית, יקיים בעל המאגר דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל האבטחה; במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור אחת לרבעון לפחות.

(ד) אירע אירוע אבטחה חמור –

(1) יודיע על כך בעל המאגר לרשם באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע;

(2) רשאי הרשם להורות לבעל מאגר המידע, למעט לבעל מאגר מידע מן המנויים בסעיף 13(ה) לחוק, לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע."

סעיף 33 ל-GDPR:

"Article 33 Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

סעיף 34 ל-GDPR:

"Article 34 Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

סעיף 34 ל-GDPR - המשך

(a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met."

סעיף WE26 לחוק הפרטיות האוסטרלי (Privacy Act 1988) – הגדרת אירוע אבטחה המקים חובת דיווח:

"Eligible data breach
(2) For the purposes of this Act, if:
(a) both of the following conditions are satisfied:
(i) there is unauthorised access to, or unauthorised disclosure of, the information;
(ii) a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or
(b) the information is lost in circumstances where:
(i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
(ii) assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates;"

סעיף WF26 לחוק הפרטיות האוסטרלי – הגדרת פעולות מתקנות הפוטרות מחובת דיווח:

"Exception – remedial Action, Access to, or disclosure of, information
(1) If:
(a) an access to, or disclosure of, information is covered by paragraph 26WE(2)(a); and
(b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the access or disclosure; and
(c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so before the access or disclosure results in serious harm to any of the individuals to whom the information relates; and
(d) as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of those individuals;
the access or disclosure is not, and is taken never to have been:
(e) an eligible data breach of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or
(f) an eligible data breach of any other entity.
(2) If:
(a) an access to, or disclosure of, information is covered by paragraph 26WE(2)(a); and
(b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the access or disclosure; and
(c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so before the access or disclosure results in serious harm to a particular individual to whom the information relates; and
(d) as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the individual;
this Part does not require:
(e) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or
(f) any other entity;

to take steps to notify the individual of the contents of a statement that relates to the access or disclosure."

סעיף WG26 לחוק הפרטיות האוסטרלי – מתי אירוע אבטחה יגרום נזק חמור:

"Whether access or disclosure would be likely, or would not be likely, to result in serious harms – relevant matters

For the purposes of this Division, in determining whether a reasonable person would conclude that an access to, or a disclosure of, information:

(a) would be likely; or

(b) would not be likely;

to result in serious harm to any of the individuals to whom the information relates, have regard to the following:

(c) the kind or kinds of information;

(d) the sensitivity of the information;

(e) whether the information is protected by one or more security measures;

(f) if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome;

(g) the persons, or the kinds of persons, who have obtained, or who could obtain, the information;

(h) if a security technology or methodology:

(i) was used in relation to the information; and

(ii) was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information;

the likelihood that the persons, or the kinds of persons, who:

(iii) have obtained, or who could obtain, the information; and

(iv) have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;

have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;

(i) the nature of the harm;

(j) any other relevant matters."

סעיף WR26 לחוק הפרטיות האוסטרלי - מתי נציב הפרטיות יורה על חובת דיווח לנושאי המידע:

"26WR Commissioner may direct entity to notify eligible data breach

(1) If the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity, the Commissioner may, by written notice given to the entity, direct the entity to:

(a) prepare a statement that complies with subsection (4); and

(b) give a copy of the statement to the Commissioner.

(2) The direction must also require the entity to:

a) if it is practicable for the entity to notify the contents of the statement to each of the individuals to whom the relevant information relates—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates; or

b) if it is practicable for the entity to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach; or

c) if neither paragraph (a) nor (b) applies:

(i) publish a copy of the statement on the entity's website (if any); and

(ii) take reasonable steps to publicise the contents of the statement.

Note: See also subsections 26WF(2) and (5), which deal with remedial action.

(3) Before giving a direction to an entity under subsection (1), the Commissioner must invite the entity to make a submission to the Commissioner in relation to the direction within the period specified in the invitation.

(4) The statement referred to in paragraph (1)(a) must set out:

(a) the identity and contact details of the entity; and

(b) a description of the eligible data breach that the Commissioner has reasonable grounds to believe has happened; and

(c) the kind or kinds of information concerned; and

(d) recommendations about the steps that individuals should take in response to the eligible data breach that the Commissioner has reasonable grounds to believe has happened.

(5) A direction under subsection (1) may also require the statement referred to in paragraph (1)(a) to set out specified information that relates to the eligible data breach that the Commissioner has reasonable grounds to believe has happened.

סעיף WG26 לחוק הפרטיות האוסטרלי – המשך:

(6) In deciding whether to give a direction to an entity under subsection (1), the Commissioner must have regard to the following:

(a) any relevant advice given to the Commissioner by:

(i) an enforcement body; or

(ii) the Australian Signals Directorate of the Defence Department;

(b) any relevant submission that was made by the entity:

(i) in response to an invitation under subsection (3); and

(ii) within the period specified in the invitation;

(c) such other matters (if any) as the Commissioner considers relevant.

(7) Paragraph (6)(a) does not limit the advice to which the Commissioner may have regard.

(8) If the Commissioner is aware that there are reasonable grounds to believe that the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities, a direction under subsection (1) may also require the statement referred to in paragraph (1)(a) to set out the identity and contact details of those other entities.

Method of providing a statement to an individual

(9) If an entity normally communicates with a particular individual using a particular method, the notification to the individual mentioned in paragraph (2)(a) or (b) may use that method. This subsection does not limit paragraph (2)(a) or (b).

Compliance with direction

(1) An entity must comply with a direction under subsection (1) as soon as practicable after the direction is given."

סעיף 23: ממונה על הגנת הפרטיות במידע

(א) בעל שליטה במידע ומעבד ימנו, כל אחד מטעמו, ממונה על הגנת פרטיות במידע העומד בתנאי הכשירות שנקבעו לפי סעיף קטן (ו), בהתקיים אחד מאלה:

(1) בעל שליטה במידע או המעבד, לפי העניין, הוא גוף ציבורי;

(2) בעל שליטה במידע או המעבד, לפי העניין, מבצע עיבוד מידע אישי על 200,000 נושאי מידע לפחות;

(3) בעל שליטה במידע או המעבד, לפי העניין, מבצע עיבוד מידע רגיש על 100,000 נושאי מידע לפחות.

(ב) הממונה על הגנת הפרטיות במידע יפעל להבטחת קיום הוראות חוק זה על ידי בעל שליטה במידע או המעבד, לפי העניין, ויהיה אחראי לטיפול בפניות הציבור וכן בפניות של ראש הרשות להגנת הפרטיות, בנוגע לקיום הוראות חוק זה.

(ג) בעל שליטה במידע או המעבד, לפי העניין, יספק לממונה על הגנת הפרטיות במידע את התנאים הדרושים למילוי תפקידו, לרבות עצמאות בביצוע תפקידיו לפי חוק זה.

(ד) לא ימונה כממונה על הגנת הפרטיות במידע מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה.

(ה) פרטי יצירת הקשר עם הממונה על הגנת הפרטיות במידע ימסרו על פי דרישה או יפורסמו בהתאם להחלטת בעל שליטה במידע או המעבד, לפי העניין. לכל אדם הזכות לפנות לממונה על הגנת הפרטיות במידע בכל הקשור לעיבוד מידע אישי על אודותיו ומימוש זכויות נושא המידע לפי חוק זה.

(ו) שר המשפטים יקבע בתקנות את תנאי הכשירות הנדרשים למינוי ממונה על הגנת הפרטיות במידע ואת הפעולות שעליו לבצע למילוי תפקידו לפי חוק זה, וכן רשאי שר המשפטים, בתקנות, לשנות את מספר נושאי המידע הקבועים בפסקאות (2) או (3) של סעיף קטן (א), לפטור סוגים מסוימים של בעלי שליטה או מעבדים מחובת מינוי ממונה על הגנת פרטיות במידע לפי סעיף קטן (א) או לחייבם במינוי כאמור.

דברי הסבר

<u>סעיף 23:</u> הסעיף המוצע מבקש לשלב בין החובה למנות ממונה אבטחת מידע על פי חוק הגנת הפרטיות הקיים ותקנות אבטחת מידע לבין החובה בסעיף 37 ל-GDPR למנות ממונה פרטיות בכל בעל שליטה במידע או מעבד. בעתיד נפעל לקדם הצעת תיקון לתקנות אבטחת מידע בהתאם למוצע בסעיף זה. לעת עתה, כדי להציג את התמונה המלאה של מכלול התיקונים המוצעים, בחרנו להציג את הסעיף הזה כחלק מהצעת החוק.

בחרנו לשנות את כינויו של בעל התפקיד מ"ממונה אבטחת מידע" בחוק הגנת הפרטיות הקיים ובתקנות אבטחת מידע ל"ממונה על הגנת הפרטיות במידע". הכינוי שאנו מציעים משקף משרעת תפקידים רחבה יותר, הקושרת בין אבטחת המידע להגנה על הזכות לפרטיות.

סעיף קטן (א) המוצע תוחם את היקף החובה למנות ממונה על הגנת הפרטיות במידע בהתאם למיהות הגוף המבצע עיבוד (גוף ציבורי) ולהיקף העיבוד של

מידע אישי או מידע רגיש, בדומה לקבוע בסעיף 17ב לחוק הגנת הפרטיות הקיים ובסעיף 37(1) ב-GDPR. לדעתנו, החובה למנות ממונה על אבטחת מידע בחוק הגנת הפרטיות הקיים מצומצמת מדי ואינה כוללת גופים רבים המבצעים פעולות עיבוד מידע אישי בהיקף נרחב. מנגד, חובה כללית של מינוי אחראי ציות על הוראות החוק, כפי שנעשה למשל בחקיקה הקנדית, היא כוללנית מדי ועלולה להטיל נטל לא סביר על גופים קטנים. בנוסף, חובת הציות להוראות החוק והאחריות למילויה מוטלות על פי דיני החברות בין כך ובין כך על נושאי המשרה בחברה. הניסוח המוצע מבקש להטיל חובה מאוזנת למינוי ממונה על הגנת פרטיות במידע המבוססת על ההנחה שבעל שליטה במידע או מעבד, לפי העניין, האוגמים כמות גדלה והולכת של מידע אישי חייבים במינוי ממונה על הגנת הפרטיות במידע אפילו אם המידע האישי שהם אוגמים אינו מידע רגיש.

סעיפים קטנים (א) ו-(ו) קובעים כי האדם הממונה לתפקיד חייב להיות בעל הכישורים המתאימים לביצועו מבחינת השכלתו וכישוריו המשפטיים והטכנולוגיים. בחרנו שלא לפרט את הכישורים הנדרשים לתפקיד כפי שמופיע למשל בסעיף 37(5) ל-GDPR, מכיוון שלדעתנו מיומנותו ומקצועיותו של הממונה על הגנת הפרטיות ייגזרו מהגדרת תפקידיו, ולפי סעיף קטן (ו) שר המשפטים הוא שיקבע בתקנות את תנאי הכשירות הנדרשים. בדומה לסעיף 37 ל-GDPR, הצעת החוק מתירה מינוי של תאגיד לתפקיד הממונה על הגנת הפרטיות כל עוד פרטי יצירת הקשר עימו ברורים כנדרש לפי סעיף קטן (ה).[40]

בחרנו שלא לאמץ את סעיפים 37(2) ו-37(2) ל-GDPR, הקובעים שקבוצת חברות בנות או קבוצת גופים ציבוריים רשאים למנות ממונה על הגנת פרטיות משותף, מאחר שלדעתנו אלו נושאים שאפשר לקבוע בתקנות ובכללים ואין צורך לכלול אותם בגדר הצעת החוק.

סעיף קטן (ב) מפרט מסגרת כללית לתפקידי הממונה על הגנת הפרטיות במידע בדומה לסעיף 23 לחוק הפרטיות בניו זילנד ולסעיף 39 ל-GDPR. במסגרת אחריותו הכללית של הממונה על הגנת הפרטיות במידע עליו לבצע כל פעולה הקשורה להגנת הפרטיות במהלך עיבוד מידע אישי שמבצעים בעל שליטה במידע או המעבד, לרבות כל פעולה הדרושה כדי להבטיח שבעל שליטה במידע או מעבד מקיימים את הוראות חוק זה, ובכלל זה עריכת ביקורת, ביצוע סקר סיכונים לפגיעה בפרטיות, יידוע בעל שליטה במידע או מעבד ועובדיהם על חובותיהם על פי חוק זה ומתן ייעוץ לעובדים של בעל שליטה במידע או של המעבד והבטחת הכשרתם המתאימה.

סעיף קטן (ג) מבוסס על סעיף 38(3) ל-GDPR. מטרתו להטיל על בעל שליטה ועל מעבד את האחריות לתת לממונה על הגנת הפרטיות במידע את תנאי ההעסקה המתאימים, לרבות פניות לביצוע התפקיד מבחינת עומס המשימות שיוטל עליו וכן עצמאותו בביצוע תפקידו – כל אלו כדי להבטיח שיפעל למילוי הוראות חוק זה בלי לחשוש למעמדו בחברה או להמשך העסקתו. לדעתנו, בניגוד ל-GDPR, מספיקה הקביעה שיש צורך בעצמאותו של בעל התפקיד, ואין מקום לקבוע בחוק הוראות מפורטות לעניין תנאי העסקתו משום שאז תהיה זו התערבות יתר של המחוקק באופן הניהול של בעל השליטה במידע או המעבד.

סעיף קטן (ד) מבוסס על סעיף 17ב(ג) לחוק הגנת הפרטיות הקיים.

סעיף קטן (ה) מבוסס על סעיף 4.1.2 לחוק הפרטיות הקנדי וקובע שפרטי יצירת הקשר עם הממונה על הגנת הפרטיות יימסרו על פי דרישה או יפורסמו לפי החלטת בעל שליטה במידע או מעבד. השארנו את הבחירה כיצד לפרסם את החלטת בעל שליטה במידע או מעבד כדי להבטיח שההחלטה תיעשה בדרך זהה לדרך איסוף המידע האישי וכדי שלא תתקבע דרך פרסום שעלולה להיחשב

בעתיד מיושנת טכנולוגית, כמו למשל פרסום בשלושה עיתונים יומיים. העדפנו ניסוח זה על פני הוראת סעיף 37(7) ל-GDPR, המחייב לעדכן את נציבות הפרטיות בפרטי הממונה על הגנת הפרטיות. לדעת חברי קבוצת המומחים, חיוב מסירת הפרטים לנציב הפרטיות כמוהו כהחזרת החובה לרישום מאגרי מידע, שהטעמים להסרתה הוסברו בדברי ההסבר להגדרת "ראש הרשות להגנת הפרטיות" בסעיף 2 לעיל.

סעיף קטן (ו) מסמיך את שר המשפטים לקבוע תנאים שונים הקשורים בחובה למנות ממונה על הגנת הפרטיות וכן לפרט את הכישורים הנדרשים להתאמה של הממונה על הגנת הפרטיות לתפקיד – כדי להבטיח גמישות ושיקול דעת ביישומה של חובה זו והתאמתה לתנאים, לשווקים ולמקצועות שונים. הסעיף גם קובע שלשר המשפטים סמכות שברשות לשנות את התנאים לכינונה של החובה למנות ממונה על הגנת הפרטיות בחברה. בחרנו להסמיך את שר המשפטים לקבוע את תנאי הכשירות בתקנות ולא להסמיך לעניין זה בכללים את ראש הרשות להגנת הפרטיות משום שמדובר בנושא מהותי שקשור לעצם תחולת הסעיף ולחופש העיסוק.

המקורות ששימשו בסיס לניסוח הסעיף:

סעיף 17ב לחוק הגנת הפרטיות הקיים:

"17ב. (א) הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן – הממונה):

(1) מחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8א;

(2) גוף ציבורי כהגדרתו בסעיף 23;

(3) בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.

(ב) בלי לגרוע מהוראות סעיף 17, הממונה יהיה אחראי לאבטחת המידע במאגרים המוחזקים ברשות הגופים כאמור בסעיף קטן (א).

(ג) לא ימונה כממונה מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה."

PIPEDA – Schedule 1 – סעיף 4.1:

"An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request."

סעיף 23 לחוק הפרטיות הניו זילנדי:

"Privacy officer

It shall be the responsibility of each agency to ensure that there are, within that agency, 1 or more individuals whose responsibilities include—

(a) the encouragement of compliance, by the agency, with the information privacy principles:

(b) dealing with requests made to the agency pursuant to this Act:

(c) working with the Commissioner in relation to investigations conducted pursuant to Part 8 in relation to the agency:

(d) otherwise ensuring compliance by the agency with the provisions of this Act."

סעיף 37 ל-GDPR:

"Article 37 Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

סעיף 37 ל-GDPR - המשך

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority."

סעיף 38 ל-GDPR:

"Article 38 Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfill other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests."

סעיף 39 ל-GDPR:

"Article 39 Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing."

סימן ד': שונות

סעיף 24: תחולת הוראות פרק ב'

הוראות פרק ב' יחולו על אלה:

(1) בעל שליטה במידע או מעבד המאוגדים או פועלים במדינת ישראל, בין אם עיבוד המידע האישי נעשה בתחומי מדינת ישראל ובין אם לאו;

(2) כל פעולת עיבוד של מידע אישי על אודות נושא מידע הנמצא במדינת ישראל, בין אם בעל השליטה במידע או המעבד נמצאים או מאוגדים בישראל ובין אם לאו, ובלבד שמטרת עיבוד המידע האישי היא אחת מאלה:

(א) מתן טובין או שירות לנושא מידע הנמצא בישראל;

(ב) ניטור התנהגות של נושא מידע המתבצעת במדינת ישראל.

דברי הסבר

סעיף 24: במרוצת השנים הולך ומתרחב העיבוד של מידע אישי על ידי תאגידים בינלאומיים שאינם כפופים לדין המדינתי. מדובר בתופעה כלל-עולמית המטרידה את רוב מדינות המערב, שכן, לפחות לכאורה, עיבוד מידע אישי על נושאי מידע בישראל שנעשה על ידי חברה בינלאומית או מחוץ לישראל עלול שלא להיות כפוף לדרישות הגנת הפרטיות במידע על פי הצעת החוק.

במאי 2018 נדרש בית המשפט העליון לשאלה. הוא פסק כי התניית השיפוט הזר וברירת הדין בתנאי השימוש של חברת פייסבוק היא תְּנָיָה מקפחת בחוזה אחיד.[41]

יש חשיבות לא מעטה לקביעת תחולה חוץ-טריטוריאלית בישראל, בדומה ל-GDPR, כדי למנוע מבעלי שליטה במידע להתחמק מציות להוראות הצעת החוק על ידי העברת מידע אישי על נושאי מידע ישראלים לחוות שרתים הממוקמות במדינות שאינן מחייבות הגנת פרטיות ברמה דומה לזו המוגדרת בהצעת החוק. כיום לא ניתן להגן על הזכות לפרטיות במידע בדרך אחרת בד בבד עם הגבלת המדיניות של הגנת הפרטיות לגבולות הגאוגרפיים של המדינה.

העברת מידע אישי כאמור אינה תאורטית גרידא. באפריל 2018 התעורר דיון בנושא כאשר נודע שחברת פייסבוק שוקלת להעביר את המידע האישי על משתמשי הרשת החברתית הישראלים מן השרתים הממוקמים באירלנד לשרתים הממוקמים בארצות הברית. לטענת פייסבוק, לא היה בכוונתה לנסות להימלט מהחלת דרישות ה-GDPR על המשתמשים הישראלים על ידי העברת המידע האישי עליהם. עוד טענה פייסבוק כי ממילא היא מתעתדת לאמץ כלפי כלל משתמשיה סטנדרט הגנת פרטיות במידע דומה לסטנדרט הנדרש באיחוד האירופי. ברם אפילו אם פייסבוק נוהגת כך, היא עושה זאת מרצונה החופשי ואין בידי המשתמש הישראלי שום כלי שיכול להכריח אותה להגן על פרטיותו במידה דומה להגנה הניתנת למשתמש תושב האיחוד האירופי.

באיחוד האירופי פתרו סוגיה זו בסעיף 3 ל-GDPR, הקובע שתחולת ה-GDPR היא

חוץ-טריטוריאלית. אם בעל שליטה במידע או מעבד פועלים בתחומי האיחוד האירופי, הם חייבים לציית ל-GDPR, בין שהעיבוד מבוצע בתחומי האיחוד ובין שאינו מבוצע שם. כמו כן, בעל שליטה במידע שאינו פועל או מאוגד כלל בתחומי האיחוד האירופי אך מעבד מידע אישי על נושאי מידע מהאיחוד, חייב לעמוד בדרישות ה-GDPR אם עיבוד המידע האישי נעשה לשם מתן שירות או מוצר לנושא מידע שנמצא באיחוד, או כאשר עיבוד המידע האישי נעשה כחלק ממעקב וניטור התנהגותם של נושאי המידע, כאשר זו מתרחשת בתחומי האיחוד, לשם יצירת פרופיל אישיותי של נושאי המידע והסקת מסקנות על העדפותיהם האישיות.

לפיכך בחרנו לאמץ סעיף דומה גם בהצעת החוק ולקבוע כי הוראות פרק ב יחולו בהתקיים אחד משני התנאים:

האחד – בעל שליטה במידע או מעבד שמאוגדים או שפועלים בתחומי מדינת ישראל ואפילו כאשר פעולת העיבוד עצמה תיעשה מחוץ לתחומי מדינת ישראל.

השני – המידע האישי המעובד הוא על נושאי מידע שנמצאים במדינת ישראל, בין שבעל השליטה במידע או המעבד מאוגדים או פועלים בישראל ובין שאינם מאוגדים או פועלים בישראל, ורק כאשר עיבוד המידע האישי נעשה לאחת משתי מטרות: (1) מתן שירות או טובין לנושאי המידע הנמצאים בישראל; או (2) ניטור התנהגותם של נושא מידע, למשל באמצעות מצלמות במעגל סגור (CCTV), מכוניות חכמות או מוצרי בית חכם, ורק כאשר ההתנהגות המנוטרת מתרחשת בישראל.

כדי לקבוע שהמטרה של עיבוד המידע האישי היא מתן טובין או שירות לנושאי מידע בישראל או לשם ניטור התנהגותם אין די בכך שאתר האינטרנט או כתובת הדוא"ל של בעל השליטה במידע או של המעבד זמינים לקהל בישראל או שהעיבוד נעשה בשפה העברית. לעומת זאת, מתן האפשרות ליצור קשר עם בעל השליטה במידע או המעבד דרך אתר אינטרנט בשפה העברית; מתן האפשרות להזמין טובין או שירות בשפה העברית או באמצעות תשלום במטבע ישראלי; הצגת פרסומות המדגישות שלבעל שליטה במידע או למעבד יש לקוחות או משתמשים של השירות או הטובין בתחומי מדינת ישראל; תשלום למנוע חיפוש בתמורה לכך שהאתר יוצג במקום גבוה בתוצאות החיפוש בתגובה לשאילתות חיפוש מישראל – כל אלה מלמדים על כוונתו של בעל שליטה במידע או של מעבד להציע שירות או טובין לנושאי מידע בישראל.

סעיף 3 ל-GDPR:

"Article 3 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

סעיף 23 להקדמה ל-GDPR:

"Recital 23: Applicable to processors not established in the Union if data subjects within the Union are targeted

In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

סעיף 24 להקדמה ל-GDPR:

Recital 24: Applicable to processors not established in the Union if data subjects within the Union are profiled

The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

סעיף 25: נציגות בעל שליטה במידע או מעבד בישראל

(א) בעל שליטה במידע או מעבד, לפי העניין, המבצע עיבוד מידע רגיש על אודות 500,000 נושאי מידע לפחות, או המבצע עיבוד מידע אישי על אודות 1,000,000 נושאי מידע לפחות, ומתקיימים תנאי סעיף 24(2), חובה עליו למנות בכתב נציג שמקום מושבו במדינת ישראל ואשר ישמש כתובת לפניות הרשות להגנת הפרטיות או נושאי המידע בכל הקשור ליישום הוראות חוק זה.

(ב) חובת מינוי נציג לפי סעיף קטן (א) לעיל לא תחול כאשר בעל שליטה במידע או המעבד, לפי העניין, הוא גוף ציבורי.

דברי הסבר

<u>סעיף 25</u>: הסעיף שואב השראה מסעיף 27 ל-GDPR ומבקש להקל על אכיפת הוראות הצעת החוק גם על תאגידי ענק בינלאומיים שאין להם נציגות משפטית מקומית. שלא כמו סעיף 27 ל-GDPR, תחולת הסעיף מוגבלת אך ורק לעיבוד מידע אישי או מידע רגיש בהיקפים גדולים. בכך מכוון הסעיף לתאגידי הענק הבינלאומיים ומבקש להקל על אכיפת הגנת הפרטיות בכל הנוגע לפעילותם בד בבד עם הימנעות מפגיעה בתחרות והדרת שחקנים בינלאומיים מתחומי מדינת ישראל. לא אימצנו את הסייג הקבוע בסעיף 27(2)(a) ל-GDPR שלפיו אין צורך בנציגות כאשר בהתחשב בהיקף עיבוד המידע האישי, הקשרו ומטרתו עיבוד המידע האישי אינו צפוי לסכן זכויות אדם; אינו קבוע; אינו כולל עיבוד בהיקף נרחב של מידע רגיש; או אינו כולל עיבוד בהיקף נרחב של מידע על הרשעות. בחרנו שלא לאמץ את סייג זה לחובה למנות נציגות בישראל, מכיוון שלדעתנו חובת מינוי נציג בישראל צריכה לחול רק על בעל שליטה במידע או מעבד שעושים עיבוד בהיקפים גדולים במיוחד. כמו כן לא חשבנו שיש צורך לציין בדבר חקיקה שאין במינוי נציג בישראל כדי לגרוע מן הזכות לנקוט פעולה משפטית נגד בעל שליטה במידע או מעבד, כלשון סעיף 27(5) ל-GDPR.

סעיף 27 ל-GDPR:

"1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union. 2. This obligation shall not apply to: (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or (b) a public authority or body. 3. The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored. 4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation. 5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves."

פרק ג: הרשות להגנת הפרטיות וסמכויות פיקוח, אכיפה ובירור מינהלי

סימן א': הרשות להגנת הפרטיות

סעיף 26: ראש הרשות להגנת הפרטיות

מי שמתקיימים בו תנאי הכשירות להתמנות לשופט של בית משפט מחוזי ומונה על ידי הממשלה, בהודעה ברשומות, לנהל את הרשות להגנת הפרטיות.

סעיף 27: תקציב הרשות

תקציב הרשות להגנת הפרטיות ייקבע בחוק התקציב השנתי, בסעיף תקציב נפרד, כמשמעותם בחוק יסודות התקציב, התשמ"ה-1985;[42] הממונה על סעיף תקציב זה לעניין החוק האמור יהיה ראש הרשות להגנת הפרטיות.

סעיף 28: עסקאות הרשות

לצורך ביצוע הוראות חוק זה, מורשה ראש הרשות להגנת הפרטיות, יחד עם חשב הרשות, לייצג את הממשלה בעסקאות כאמור בסעיפים 4 ו 5 לחוק נכסי המדינה, התשי"א–1951,[43] למעט עסקאות במקרקעין, ולחתום בשם המדינה על מסמכים הנוגעים לעסקאות כאמור.

סעיף 29: עובדי הרשות להגנת הפרטיות

(א) עובדי הרשות להגנת הפרטיות יהיו עובדי המדינה ויחולו עליהם הוראות חוק שירות המדינה (מנויים), התשי"ט–1959,[44] ואולם ראש הרשות מורשה, באישור שר המשפטים, יחד עם חשב הרשות, לייצג את המדינה בעשיית חוזים מיוחדים עם עובדים.

(ב) עובדי הרשות יפעלו לפי הוראות ראש הרשות להגנת הפרטיות ובפיקוחו.

דברי הסבר

סעיפים 26-29:

תכלית פרק זה היא לתת בידי ראש הרשות להגנת הפרטיות כלים שיאפשרו לו וליחידתו חופש פעולה מינהלי ותקציבי ויסייעו לו בביצוע תפקידיו המורכבים. תקציב הרשות ייקבע בחוק התקציב בסעיף נפרד. ראש הרשות להגנת הפרטיות יהיה הממונה על ביצועו של התקציב כך שתובטח עצמאותם של הרשות ושל ראש הרשות בניהול הרשות ובהפעלת התקציב שיוקצה לפעולותיה. ראש הרשות יוסמך להתקשר בעסקאות ככל הדרוש לפעולת הרשות. לבסוף, ראש הרשות יוסמך לטפל בענייניה המינהליים של הרשות, אך עובדי הרשות יהיו עובדי מדינה, כפי שקבוע בסעיף 10(ד) לחוק הגנת הפרטיות הקיים. כך, עובדי הרשות יחויבו בנורמות המהותיות והאתיות של עובדי המדינה ויהיו כפופים לחוק שירות המדינה (מינויים), התשי"ט–1959. בד בבד, לרשות להגנת הפרטיות תוקנה יכולת ניהול אוטונומית מסוימת.

מעמד הרשות המוצע כאן מכיל יסודות הקיימים באשר לרשות להגבלים עסקיים, כאמור בסעיפים 41, 41א, 41ב לחוק ההגבלים העסקיים, התשמ"ח–1988, וכן יסודות הקיימים באשר לרשות להגנת הצרכן וסחר הוגן, כאמור בסעיפים 19א-19ג לחוק הגנת הצרכן, התשמ"א–1981.

סעיפים 41, 41א ו-41ב לחוק ההגבלים העסקיים, התשמ"ח–1988:

"41. (א) הממשלה תמנה, לפי הצעת השר, ממונה על הגבלים עסקיים; הממונה יהיה עובד המדינה.

(ב) הודעה על המינוי תפורסם ברשומות.

41א. (א) מוקמת בזאת רשות הגבלים עסקיים (להלן – הרשות).

(ב) הממונה יהיה מנהל הרשות.

(ג) תקציב הרשות ייקבע בחוק התקציב בסעיף תקציב נפרד כמשמעותו בחוק יסודות התקציב, תשמ"ה–1985. הממונה על סעיף תקציב זה, לענין החוק האמור, יהיה מנהל הרשות.

(ד) מנהל הרשות יהיה מורשה, ביחד עם חשב הרשות, לייצג את הממשלה בעסקאות כאמור בסעיפים 4 ו-5 לחוק נכסי המדינה, תשי"א–1951, למעט עסקאות במקרקעין, למטרת ביצוע הוראות חוק זה, ולחתום בשם המדינה על מסמכים הנוגעים לעסקאות כאמור.

41ב. (א) עובדי הרשות יהיו עובדי המדינה ויחולו עליהם הוראות חוק שירות המדינה (מינויים), תשי"ט–1959, ואולם מנהל הרשות מורשה, באישור השר, יחד עם חשב הרשות, לייצג את המדינה בעשיית חוזים מיוחדים עם עובדים.

(ב) עובדי הרשות יפעלו לפי הוראות מנהל הרשות ובפיקוחו."

סעיפים 19, 19א-19ג לחוק הגנת הצרכן, התשמ"א–1981

"19. הממשלה תמנה, לפי המלצת השר, ממונה על הגנת הצרכן והסחר ההוגן; הודעה על המינוי תפורסם ברשומות.

19א. (א)מוקמת בזה הרשות להגנת הצרכן ולסחר הוגן.

(ב)הממונה יהיה מנהל הרשות.

19ב. תקציב הרשות ייקבע בחוק התקציב השנתי, בסעיף תקציב נפרד, כמשמעותם בחוק יסודות התקציב, התשמ"ה–1985; הממונה על סעיף תקציב זה לענין החוק האמור יהיה הממונה.

19ג. לצורך ביצוע הוראות חוק זה, מורשה הממונה, יחד עם חשב הרשות, לייצג את הממשלה בעסקאות כאמור בסעיפים 4 ו-5 לחוק נכסי המדינה, התשי"א–1951, למעט עסקאות במקרקעין, ולחתום בשם המדינה על מסמכים הנוגעים לעסקאות כאמור".

סעיף 30: תפקידי הרשות להגנת הפרטיות

(א) תפקידי הרשות יהיו –

(1) לפקח על ביצוע הוראות חוק זה;

(2) לחקור חשד לביצוע עבירה לפי חוק זה ולהביא את העבריין לדין;

(3) לנקוט הליכי אכיפה מינהלית נגד מפר לפי הוראות חוק זה;

(4) לטפח תודעה ציבורית להגנת הפרטיות באמצעות חינוך, הדרכה והסברה, ככל שתפקיד זה אינו מוטל על רשות ציבורית אחרת הפועלת על פי דין;

(5) לטפל בתלונות שיש בהן ממש על הפרת הוראות חוק זה או על פגיעה אחרת בפרטיות נושא מידע;

(6) לערוך וליזום סקרים ומחקרים בענייני הגנת הפרטיות;

(7) לייעץ לממשלה בכל הקשור ביישום מטרות חוק זה;

(8) לטפל בכל עניין אחר הקשור להגנת הפרטיות ואשר לא הוטל בדין על רשות אחרת.

(ב) הגיעה לראש הרשות להגנת הפרטיות תלונה בעניין שבו לפי חיקוק יש לרשות אחרת סמכות לפיקוח ולנקיטת אמצעים בעקבות בירור תלונה, ייוועץ באותה רשות לפני שיטפל בתלונה, ורשאי הוא אף להעביר את התלונה אליה; העביר ראש הרשות להגנת הפרטיות את התלונה כאמור, תודיע הרשות אליה הועברה התלונה לראש הרשות להגנת הפרטיות על תוצאות הטיפול.

(ג) ראה ראש הרשות להגנת הפרטיות כי מטרות החוק לפי סעיף 1 מושפעות, כרוכות או עלולות להיות מושפעות או כרוכות בהליך פלוני שלפני בית משפט, רשאי הוא, לפי ראות עיניו, להתייצב באותו הליך ולהשמיע דברו, או להסמיך במיוחד את נציגו לעשות זאת מטעמו;

דברי הסבר

<u>סעיף 30</u>: הסעיף מבוסס ברובו על סעיף 20 לחוק הגנת הצרכן, התשמ"א–1981, מתוך הבנה שיש דמיון רב בין הרשות להגנת הצרכן וסחר הוגן לבין הרשות להגנת הפרטיות. דמיון זה מתבטא בקהלי היעד שמולם פועלות הרשויות, בסוג ההליכים שהן מוסמכות לנהל ובטיפוסי הזכויות שהן אמורות להגן עליהן.

תהליך השינוי שעוברת הרשות להגנת הצרכן וסחר הוגן בעקבות תיקון מס' 39 לחוק הגנת הצרכן משנת 2014 הוא התהליך שיהיה על הרשות להגנת הפרטיות לעבור גם כן.

שלא כמו חוק הגנת הצרכן בחרנו לקבוע בסעיף את תפקידי הרשות ולא רק את תפקידי ראש הרשות, בדומה לסעיף 18ח לחוק שוויון הזדמנויות בעבודה, התשמ"ח–1988, וסעיף 5 לחוק הרשות השניה לטלויזיה ורדיו, התש"ן-1990.

חוק הגנת הצרכן, התשמ"א–1981:

"20.(א)תפקידי הממונה יהיו –

(1) לפקח על ביצוע הוראות חוק זה;

(1א) לחקור חשד לביצוע עבירה לפי חוק זה ולהביא את העבריין לדין;

(1ב) לנקוט הליכי אכיפה מינהלית נגד מפר לפי הוראות חוק זה;

(2) לטפל בתלונות שראה בהן ממש על הפרת הוראות חוק זה או על פגיעה אחרת בצרכן;
(3) לערוך וליזום סקרים ומחקרים בעניני צרכנות;
(3א) לטפל בכבילות בין עוסק לצרכן, הפוגעות ביכולת הצרכן לעבור מעוסק לעוסק;
(4) לטפל בכל ענין אחר הקשור להגנת הצרכן ואשר לא הוטל בדין על רשות אחרת.
(ב)הגיעה לממונה תלונה בענין שבו לפי חיקוק יש לרשות אחרת סמכות לפיקוח ולנקיטת אמצעים בעקבות בירור תלונה, ייוועץ באותה רשות לפני שיטפל בתלונה, ורשאי הוא אף להעביר את התלונה אליה; העביר הממונה את התלונה כאמור, תודיע הרשות לממונה על תוצאות הטיפול."

סעיף קטן (7) המוצע מבקש להעמיק את המתאם בין מדיניות הממשלה לפעילות הרשות להגנת הפרטיות, הן ברמה הכללית והן ברמה היישומית הפרטנית, באמצעות הסמכת הרשות להגנת הפרטיות לייעץ לממשלה בכל הקשור ליישום מטרות החוק. הוראה דומה נמצאת גם בסעיף 8 לחוק לעידוד מחקר, פיתוח וחדשנות טכנולוגית בתעשיה, התשמ"ד–1984, המפרט את תפקידיו של המדען הראשי ברשות החדשנות.

סעיף 8 לחוק לעידוד מחקר, פיתוח וחדשנות טכנולוגית בתעשיה, התשמ"ד–1984:

"תפקידי המדען הראשי יהיו, בין השאר –

(1) לייעץ לממשלה בכל הקשור ליישום מטרות חוק זה;
(2) לעקוב אחר התהליכים והשינויים בחדשנות הטכנולוגית בתעשייה בישראל ומחוצה לה, לרבות השפעתם על יצירת מקומות עבודה וצמצום פערים חברתיים-כלכליים;
(3) להמליץ לפני כל רשות המוסמכת לכך בדבר מתן הטבות העשויות לסייע בהגשמת מטרות החוק בתחומים שבסמכות אותה רשות או בתחומים שהיא ממונה על ביצועם;
(4) לדווח לממשלה, ובכלל זה לוועדת השרים לענייני מדע טכנולוגיה וחלל שקבעה הממשלה, אחת לשנה, על מימצאיו והמלצותיו בנוגע לקידום החדשנות הטכנולוגית בתעשייה, והמלצותיו באשר לפעולות של הרשות והממשלה הנדרשות כדי להגשים את מטרות החוק, בהתחשב בהשפעתן על יצירת מקומות עבודה ועל צמצום פערים חברתיים-כלכליים."

סעיף קטן (ג) שואב השראה מסעיף 1 לפקודת סדרי הדין (התייצבות היועץ המשפט לממשלה) [נוסח חדש] ומיועד לתת מענה לצורך, שמתעורר לא אחת בהליכים משפטיים, גם אלו המתנהלים נגד הרשות המחוקקת או המבצעת, להצגת האינטרס הציבורי שבהגנה על הזכות לפרטיות בידי אנשי מקצוע מומחים בתחום. אכן מדובר בסמכות חריגה, ובכל זאת, לדעתנו, רגישותה וחשיבותה של הזכות לפרטיות מצדיקות מתן אפשרות לראש הרשות להגנת הפרטיות לומר את דברו בהליכים משפטיים שתוצאתם עלולה לפגוע בזכות לפרטיות.

סעיף 1 לפקודת סדרי הדין (התייצבות היועץ המשפט לממשלה) [נוסח חדש]:

"ראה היועץ המשפטי לממשלה, כי זכות של מדינת ישראל או זכות ציבורית אחרת או עניין ציבורי מושפעים או כרוכים, או עלולים להיות מושפעים או כרוכים, בהליך פלוני שלפני בית משפט או לפני פקיד מסדר כמשמעותו בפקודת הקרקעות (סידור זכות הקניין) רשאי הוא, לפי ראות עיניו, להתייצב באותו הליך ולהשמיע את דברו, או להסמיך במיוחד את נציגו לעשות זאת מטעמו".

סעיף 31: שיתוף פעולה עם רשות חוץ

(א) מצא ראש הרשות להגנת הפרטיות כי התקיימו כל אלה:

(1) רשות חוץ הגישה לרשות להגנת הפרטיות בקשה לסיוע;

(2) נושא הבקשה לסיוע עשוי להיות הפרה של דיני הגנת הפרטיות שרשות חוץ, שהגישה את הבקשה, מופקדת על ביצועם, אכיפתם ופיקוחם;

רשאי הוא לקבוע כי על הבקשה לסיוע יחולו הוראות סעיף זה.

(ב) לא תיעשה פעולה מכוח הוראות סעיף זה אם היא עלולה, לדעת היועץ המשפטי לממשלה, לפגוע בריבונות מדינת ישראל, בביטחונה, באינטרס החיוני לה, בתקנת הציבור או בחקירה תלויה ועומדת.

(ג) כדי להבטיח מתן סיוע לרשות חוץ, יהיו חוקר, מפקח או עובד מדינה שהוסמך לכך לפי סעיף 33, רשאים להשתמש בסמכויות לפי סעיפים 34 עד 37, שהוסמכו לבצען, לפי העניין, ובסמכויות לפי סעיף 43 לפקודת מעצר וחיפוש וסעיף 3 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007 (בסעיף זה – חוק נתוני תקשורת) בשינויים המחויבים ובלבד שנושא בקשת הסיוע עשוי להיות נתון לחקירה כעבירה פלילית לפי חוק זה, ואם הנושא של הבקשה לסיוע הוא פיקוח – תיעשה הפעלת הסמכויות לפי סעיף 34 בלבד.

(ד) קבע ראש הרשות להגנת הפרטיות כי על הבקשה לסיוע יחולו הוראות סעיף זה, ומידע אישי או מסמך שמבוקשים בבקשה לסיוע מצויים בידי הרשות להגנת הפרטיות, רשאי מי שראש הרשות להגנת הפרטיות הסמיכו לכך בכתב להעביר לרשות החוץ את המידע האישי או המסמך או העתק מאושר או העתק צילומי מאושר שלו.

(ה) לא יועבר מידע אישי או מסמך בהתאם לסעיף קטן (ד) לעיל אלא אם שוכנע ראש הרשות להגנת הפרטיות כי הוא ישמש אך ורק למטרה שלשמה נמסר.

(ו) הועבר מידע אישי או מסמך לפי סעיף קטן (ד) לעיל, רשאי ראש הרשות להגנת הפרטיות לאשר לרשות חוץ להעביר מידע אישי או מסמך לשם ביצוע ואכיפה של דיני הגנת הפרטיות ופיקוח על ביצועם, לרשות ממשלתית אחרת או לרשות שהוקמה מכוח הסכם בין מדינות ורשאי הוא להתנות העברת מידע אישי או מסמך כאמור בתנאים.

(ז) ראש הרשות להגנת הפרטיות רשאי להורות שפעולה לפי סעיף זה לא תיעשה לפי בקשת רשות חוץ, אשר מנועה או נמנעה מביצוע פעולה דומה לבקשת הרשות להגנת הפרטיות.

(ח) על אף האמור בכל דין, מידע אישי, ידיעה או מסמך שנמסרו לרשות על ידי רשות חוץ או שהתקבלו, שנאספו או שנוצרו בעקבות בקשה לסיוע או בקשה לקבלת מידע אישי, ידיעה או מסמך שהוגשה לרשות להגנת הפרטיות על ידי רשות חוץ, לרבות הבקשה עצמה, רשאית הרשות להגנת הפרטיות שלא להעבירם לצד שלישי; אין בהוראה זו כדי למנוע גילוי לפי דרישת היועץ המשפטי לממשלה לצורך משפט פלילי או לפי דרישת בית המשפט.

דברי הסבר

סעיף 31: פגיעה בזכות לפרטיות, בעיקר פרטיות במידע, יכולה להיות חוצת גבולות. כך למשל, בפרשת **קיימברידג' אנליטיקה** נחשף מידע אישי על כ-47 אלף משתמשי פייסבוק מישראל.[45] שיתוף פעולה בין הרשויות להגנת פרטיות ברחבי העולם הוא כורח המציאות על מנת לחקור פגיעה בזכות לפרטיות ולהביא לידי אכיפה יעילה של דיני הגנת הפרטיות.

גם ה-GDPR מכיר בצורך להתיר העברת מידע אישי בין רשויות מדינתיות מנימוקים הקשורים באינטרס של הציבור ולשם ייעול האכיפה של דיני הגנת הפרטיות, למשל בין רשויות מדינתיות להגבלים עסקיים או בין רשויות מדינתיות להגנת הפרטיות מדינתיות.

סעיף 112 להקדמה ל-GDPR:

"Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject."

סעיף 116 להקדמה ל-GDPR:

"When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation."

סעיף 50 ל-GDPR קובע את המסגרת לשיתוף פעולה במידע לצורכי אכיפה:

"Article 50

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

סעיף 50 ל-GDPR - המשך

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries."

הצורך בשיתוף מידע אישי בין רשויות מדינתיות קיבל הכרה בינלאומית. זה היה לקח מן החקירה המשותפת שניהלו רשויות הגנת הפרטיות של קנדה, של אוסטרליה ושל ארצות הברית בעניין חשיפת מידע אישי ומידע רגיש על משתמשי האתר "אשלי מדיסון".[46] בספטמבר 2017 נחתמה החלטה על הצורך לבחון עקרונות חקיקתיים שאימוצם יאפשר שיתוף פעולה בינלאומי במישור החקירתי. ההחלטה הדגישה כי שיתוף פעולה בינלאומי נועד להגביר את הציות לחוקי ההגנה על הפרטיות.[47]

בדין הישראלי שיתוף במידע לצורכי אכיפה וחקירה בין רשויות מקובל בדיני ניירות ערך. סעיף 31 המוצע מאמץ את ההסדר הקבוע לעניין זה בפרק ט'2 לחוק ניירות ערך, התשכ"ח–1968, בשינויים האלה:

(1) הסמכויות הניתנות לחוקר ולמפקח בבקשת סיוע לפי סעיף קטן (ג) זהות לסמכויות הנתונות לו על פי הצעת החוק באשר לאכיפה, פיקוח ובירור מינהלי, כפי שהסמכויות הניתנות לחוקר על פי חוק ניירות ערך בסעיף 54יא4 זהות לסמכויות הניתנות מכוח חוק ניירות ערך.

(2) שיתוף פעולה והעברת מידע בין הרשות להגנת הפרטיות לרשות חוץ אינו מותנה בחתימה על מזכר הבנות. ההצדקה לכך היא שגם ההסדר בחוק ניירות ערך מבהיר בסעיף 54יא9(ב) שקיומו של מזכר הבנה הוא לא תנאי להעברת ידיעות ומסמכים.

חוק ניירות ערך, התשכ"ח–1968:

"54יא1. (א) בפרק זה –

"רשות חוץ" – גוף המופקד על ביצוע ואכיפה של דיני ניירות עירך במדינת חוץ ופיקוח על ביצועם, אשר חתם על מזכר הבנה עם הרשות;

"מזכר הבנה" – הסכם שעניינו שיתוף פעולה בביצוע ואכיפה של דיני ניירות ערך ובפיקוח על ביצועם;

"סיוע לרשות חוץ" – דרישת ידיעה ומסמכים, עריכת חיפוש, תפיסת מסמכים, ניהול חקירה והעברת ידיעות ומסמכים, לשם ביצוע ואכיפה של דיני ניירות ערך במדינת חוץ ופיקוח על ביצועם.

"בקשה לסיוע" – בקשה לסיוע שהוגשה בכתב לרשות על ידי רשות חוץ בהתאם למזכר הבנה;

"דיני ניירות ערך" – דינים בתחום ניירות ערך שהרשות או רשות חוץ מופקדת על ביצועם ואכיפתם.

(ב) משמעותם של מונחים בדיני ניירות ערך במדינת חוץ תהא כמשמעותם בדין שבתחום סמכותה של רשות החוץ.

54יא2. מצא יושב ראש הרשות כי התקיימו כל אלה:

(1) רשות חוץ הגישה לרשות בקשה לסיוע בהתאם לתקנות לפי סעיף 54יא7;

(2) נושא הבקשה עשוי להיות הפרה של דיני ניירות ערך שרשות החוץ שהגישה את הבקשה מופקדת על ביצועם, אכיפתם ופיקוחם;

(3) התקיימו הוראות פרק זה ומזכר ההבנה;

רשאי הוא לקבוע כי על הבקשה לסיוע יחולו הוראות פרק זה.

54יא3. לא תיעשה פעולה מכוח הוראות פרק זה אם היא עלולה, לדעת היועץ המשפטי לממשלה, לפגוע בריבונות מדינת ישראל, בביטחונה, באינטרס החיוני לה, בתקנת הציבור או בחקירה תלויה ועומדת.

54יא4. (א) כדי להבטיח מתן סיוע לרשות חוץ, יהיה מי שיושב ראש הרשות הסמיכו לכך בכתב רשאי להשתמש בסמכויות לפי סעיפים 52מג, 56א, 56א1, ו-56ב עד 56ג1,

סעיף 43 לפקודת מעצר וחיפוש וסעיף 3 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007 (בסעיף זה – חוק נתוני תקשורת) בשינויים המחויבים ואולם הפעלת סמכויות לפי סעיפים 56ב, 56ב1 או 56ג1, סעיף 43 לפקודת מעצר חיפוש או סעיף 3 לחוק נתוני תקשורת תיעשה רק אם הנושא של הבקשה לסיוע עשוי להיות נתון לחקירה כעבירה פלילית לפי דיני ניירות ערך בישראל, ואם הנושא של הבקשה לסיוע הוא פיקוח – תיעשה הפעלת הסמכויות לפי סעיפים 56א, 56א1 או 56ו בלבד.

(ב) על ידיעה או מסמך שהגיעו לידי מי שהוסמך לכך כאמור בסעיף קטן (א) יחולו הוראות סעיף 56ה, בשינויים המחויבים.

(ג) קבע יושב ראש הרשות כי על הבקשה לסיוע יחולו הוראות פרק זה, רשאי הוא להורות למי שהוסמך לכך כאמור בסיף קטן (א) כי גביית הודעה תיעשה לפי סדר הגין שבתחום סמכותה של רשות החוץ, אם ביקשה זאת רשות החוץ בבקשה לסיוע.

54יא5. (א) קבע יושב ראש הרשות כאמור בסעיף 54יא2, וידיעה או מסמך שמבוקשים בבקשה לסיוע מצויים בידי הרשות, רשאי מי שיושב ראש הרשות הסמיכו לכך בכתב להעביר לרשות החוץ את הידיעה או המסמך, או העתק מאושר או העתק צילומי מאושר שלו (בסעיף זה – ידיעה).

(ב) מי שיושב ראש הרשות הסמיכו כאמור בסעיף 54יא4, רשאי להעביר לרשות חוץ ידיעה שהגיעה אליו מכוח הסמכה כאמור.

(ג) לא תועבר ידיעה אלא אם כן שוכנע יושב ראש הרשות כי היא תשמש אך ורק למטרה שלשמה נמסר.

(ג1) יושב ראש הרשות רשאי לאשר לרשות חוץ להעביר ידיעה לשם ביצוע ואכיפה של דיני ניירות ערך ופיקוח על ביצועם, לרשות ממשלתית אחרת או לרשות שהוקמה מכוח הסכם בין מדינות ורשאי הוא להתנות העברת ידיעה כאמור בתנאים.

(ד) על אף הוראות סעיף זה, לא יועבר לרשות חוץ מסמך שאינו פומבי או העתק מאושר או העתק צילומי מאושר שלו, הנוגע לעסקי תאגיד בנקאי או מבטח, אלא באישורו של המפקח על הבנקים או המפקח על עסקי ביטוח, לפי העניין; בסעיף קטן זה –

"תאגיד בנקאי" – כהגדרתו בחוק הבנקאות (רישוי), תשמ"א–1981, למעט חברת שירותים משותפים;

"מבטח" – כהגדרתו בחוק הפיקוח על הביטוח.

54יא6. יושב ראש הרשות רשאי להורות שפעולה לפי פרק זה לא תיעשה לפי בקשת רשות חוץ, אשר מנועה או נמנעה מביצוע פעולה דומה לבקשת הרשות.

54יא7. שר המשפטים רשאי להתקין תקנות –

(1) לשם ביצועו של פרק זה, לרבות לעניין נוהלי הגשת בקשה לסיוע לרשות חוץ והטיפול בה;

(2) לשם ביצוע מזכר הבנה.

54יא8. נקבעו במזכר הבנה הוראות בעניינים המפורטים להלן, והותקנו תקנות לביצוען, יהיה לתקנות תוקף, על אף הוראות חוק זה או כל חוק אחר;

(1) המצאת מסמכים, הוכחתם, אימותם ואישורם בידי רשות חוץ, לבקשת הרשות;

(2) גביית עדות, תפיסת מסמכים או ביצוע כל פעולת אכיפה או פיקוח אחרת בידי רשות חוץ, לבקשת הרשות.

54יא9. (א) על אף האמור בכל דין, ידיעה או מסמך שנמסרו לרשות על ידי רשות חוץ או שהתקבלו, שנאספו או שנוצרו בעקבות בקשה לסיוע או בקשה לקבלת ידיעה או מסמך שהוגשה לרשות על ידי רשות חוץ, לרבות הבקשה עצמה, רשאית הרשות שלא להעבירם לצד שלישי; אין בהוראה זו כדי למנוע גילוי לפי דרישת היועץ המשפטי לממשלה לצורך משפט פלילי או לפי דרישת בית המשפט.

(ב) בסעיף זה, "רשות חוץ" – גוף המופקדת על ביצוע ואכיפה של דיני ניירות ערך במדינת חוץ ופיקוח על ביצועם, גם אם לא חתם על מזכר הבנות עם הרשות."

סעיף 32: הוועדה המייעצת

(א) שר המשפטים ימנה ועדה מייעצת שתפקידה:

(1) לייעץ לראש הרשות להגנת הפרטיות, לפי דרישתו, בכל עניין הנוגע להגנת הפרטיות, וכן לייעץ לו בהכנת הדין וחשבון השנתי כאמור בסעיף 74 ובהכנת תוכנית העבודה של הרשות;

(2) לדון בנושאים נוספים בנוגע ליישום הוראות חוק זה שיש לדעתה חשיבות בעיסוק הרשות להגנת הפרטיות בהם.

(ב) הוועדה המייעצת תהיה בת חמישה חברים והם:

(1) עובד משרד המשפטים בדרגה ____;

(2) עובד משרד הכלכלה והתעשייה בדרגה שאינה פחותה מדרגת סגן מנהל כללי;

(3) חבר הסגל האקדמי של מוסד מוכר להשכלה גבוהה כמשמעותו בחוק המועצה להשכלה גבוהה, התשי"ח–1958;[48]

(4) שני נציגי ציבור מקרב מוסד, מכון או ארגון, אשר אחד מהם לפחות יהיה נציג מתחום תעשיית הטכנולוגיה והשני יעסוק באחד מהתחומים האלה: צרכנות, משפט, כלכלה או מדיניות ציבורית;

(ג) שר המשפטים ימנה את אחד מחברי הוועדה המייעצת להיות יושב ראש הוועדה.

(ד) חברי הוועדה המייעצת ימונו לתקופה של שלוש שנים וניתן לחזור למנותם, ובלבד שלא יכהנו שלוש תקופות רצופות.

דברי הסבר

<u>סעיף 32:</u> המועצה הציבורית להגנת הפרטיות, שהוקמה בשנת 1986, מייעצת לשר המשפטים בנושאי פרטיות ומביעה את עמדתה בהליכי חקיקה ראשית ומשנית גם לפני הכנסת וּועדות הכנסת. עם זאת, ההתייחסות לקיומה של המועצה נמצאת רק בסעיף 10א לחוק הגנת הפרטיות הקיים, המעגן את חובתה הסטטוטורית של המועצה להעיר את הערותיה על דוח רשם מאגרי המידע:

"לא יאוחר מ-1 באפריל בכל שנה תגיש המועצה להגנת הפרטיות לוועדת החוקה חוק ומשפט של הכנסת דין וחשבון שיכון הרשם על פעולות האכיפה והפיקוח בשנה שקדמה להגשת הדו"ח, בצירוף הערותיה של המועצה."

המועצה להגנת הפרטיות מונה כיום 10 חברים, 2 מהם עובדי משרד המשפטים בעבר או בהווה, 2 מהמגזר העסקי, 1 מייצג את המגזר השלישי, וכל השאר אנשי אקדמיה מתחום המשפטים, מדעי המחשב, חינוך, תקשורת וסוציולוגיה.

לעומת ההסדר בחוק הגנת הפרטיות הקיים, חוק הגנת הצרכן, התשמ"ח-1981, מקים בסעיף 22א לחוק ועדה מייעצת שתפקידה לייעץ לממונה על הגנת הצרכן עצמו לפי דרישתו בכל עניין הנוגע להגנת הצרכן ולסחר הוגן וכן בהכנת תוכנית העבודה של הרשות להגנת הצרכן:

"(א) השר, בהסכמת שר האוצר, ימנה ועדה מייעצת שתפקידה לייעץ לממונה, לפי דרישתו, בכל עניין הנוגע להגנת הצרכן ולסחר הוגן, וכן לייעץ לו בהכנת דין וחשבון השנתי כאמור בסעיף 22בב ובהכנת תכנית העבודה של הרשות.

(ב) הוועדה המייעצת תהיה בת שישה חברים והם:

(1) עובד משרד התעשיה המסחר והתעסוקה, בדרגה שאינה פחותה מדרגת סגן מנהל כללי;
(2) עובד משרד האוצר, בדרגה שאינה פחותה מדרגת סגן מנהל כללי;
(3) שני חברי הסגל האקדמי של מוסדות מוכרים להשכלה גבוהה כמשמעותם בחוק המועצה להשכלה גבוהה, התשי"ח–1958;
(4) נציג ארגון צרכנים כהגדרתו בסעיף 31(ג), שיקבע השר;
(5) נציג העוסקים שיקבע השר.
(ג) השר, בהסכמת שר האוצר, ימנה את אחד מחברי הוועדה המייעצת להיות יושב ראש הוועדה.
(ד) חברי הוועדה ימונו לתקופה של שלוש שנים וניתן לחזור למנותן, ובלבד שלא יכהנו שלוש תקופות רצופות."

בסעיף המוצע מעוגנת הקמת הוועדה המייעצת במפורש, ובסעיף קטן (א) מעוגנות סמכויותיה – בדומה לקיים בחוק הגנת הצרכן. בנוסף, הרחבנו את סמכות הוועדה המייעצת לדון גם בנושאים נוספים, נוסף על אלו שיידרשו על ידי ראש הרשות להגנת הפרטיות, אם לדעתה של הוועדה יש חשיבות בדיון ובעיסוק בהם על ידי הרשות להגנת הפרטיות. מטרת הרחבה זו היא למנוע את האפשרות שראש הרשות להגנת הפרטיות ירוקן את תפקיד הוועדה המייעצת מתוכן.

סברנו כי ועדה מייעצת של 5 חברים, כמפורט בסעיף קטן (ב), היא סבירה בגודלה ותאפשר פעולה יעילה של הוועדה המייעצת. בהתחשב בחשיבות של הזכות לפרטיות בצד הערך הכלכלי הרב הניתן למידע אישי בעידן המודרני, חשבנו שיש צורך להבטיח שאחד מנציגי הציבור בוועדה יהיה מתחום תעשיית הטכנולוגיה.

באשר לדרישה למינוי עובד משרד המשפטים לחבר בוועדה המייעצת – יש צורך במינוי בעל תפקיד בדרגה מקבילה לדרגת סגן מנהל כללי, בדומה לדרגה הנדרשת מחבר בוועדה המייעצת ממשרד התעשייה והמסחר לפי סעיף 22א(ב)(1) לחוק הגנת הצרכן.

סעיף 33: הסמכת חוקר או מפקח

(א) ראש הרשות להגנת הפרטיות רשאי להסמיך חוקר או מפקח, מבין עובדי המדינה, לביצוע סמכויות לפי חוק זה, כולן או חלקן, אם התקיימו בו כל אלה:

(1) משטרת ישראל הודיעה, בתוך שלושה חודשים מפנייתו של ראש הרשות להגנת הפרטיות אליה, כי היא אינה מתנגדת להסמכתו מטעמים של ביטחון הציבור, לרבות בשל עברו הפלילי;

(2) הוא קיבל הכשרה מתאימה בתחום הסמכויות שיהיו נתונות לו לפי חוק זה, כפי שהורה שר המשפטים בהסכמת השר לביטחון הפנים, ולעניין הפעלת סמכויות חדירה לחומר מחשב או העתקתו כאמור בסעיפים 35-36 – הוא בעל תפקיד המיומן לביצוע פעולות כאמור;

(3) הוא עומד בתנאי כשירות נוספים, ככל שהורה שר המשפטים בהסכמת השר לביטחון הפנים.

(ב) הסמכתו של מפקח או חוקר לפי סעיף זה תהיה בתעודה החתומה בידי ראש הרשות להגנת הפרטיות, שמעידה על תפקידו כמפקח או כחוקר ועל סמכויותיו לפי חוק זה.

דברי הסבר

<u>סעיף 33:</u> מוצע לקבוע שראש הרשות להגנת הפרטיות יהיה רשאי להסמיך חוקר או מפקח, מקרב עובדי המדינה, לביצוע הסמכויות לפי החוק, כולן או חלקן. כמו כן מוצע לקבוע תנאי הסמכה הולמים למפקח ולחוקר, בדגש על הכשרה ראויה לצורך הפעלת סמכות לחדור לחומרי מחשב, כמקובל בדברי חקיקה דומים אחרים.

סעיף קטן (א) מבוסס על התיקון המוצע לסעיף 10(ה) בהצ"ח תיקון מס' 13, שם הוסבר כי "יש לקבוע תנאי הסמכה הולמים למפקח ולחוקר, תוך מתן דגש על הכשרה ראויה לצורך הפעלת סמכות חדירה לחומר מחשב, כמקובל בהוראות דברי חקיקה דומים אחרים."[49]

סעיף קטן (ב) מבוסס על הוראת סעיף 20א(ג) לחוק הגנת הצרכן. תעודת המפקח נועדה להבטיח שהמפקח ישתמש בסמכויות הנתונות לו לפי הצעת החוק רק בעת מילוי תפקידו ורק כאשר יש ברשותו תעודת מפקח, שאותה יצטרך להציג לפי דרישה. בחוק הגנת הצרכן נקבע כי יש צורך בריענון ההכשרה כמפקח אחת לשלוש שנים. הדרישה לריענון ההכשרה מדי שלוש שנים היא ייחודית לחוק הגנת הצרכן, שכן בחוקים אחרים שיש בהם דרישת הסמכה, ההסמכה תקפה לתמיד מרגע נתינתה וההתמודדות עם עובד מוסמך שסרח נעשית מכוח הכללים החלים על עובדי מדינה.[50] לאחר בחינת הנושא הגיעה קבוצת המומחים למסקנה שאין הצדקה להגביל את תוקף הכשרתו של מפקח ברשות להגנת הפרטיות לשלוש שנים. עם זאת יש להסדיר בתקנות את קיומן של הכשרות עיתיות לשם הבטחת הכשירות של המפקח לביצוע תפקידו, בעיקר לנוכח השינויים הטכנולוגיים התדירים בתחום העיבוד של מידע אישי.

לא מצאנו לנכון לאמץ בהצעת החוק הוראה דומה לסעיף 20ב2 בחוק הגנת הצרכן, התשמ"א–1981, המטיל חובה על מפקח ברשות להגנת הצרכן לענוד תג זיהוי גלוי. הצורך בענידת תג עלה בדיון על תיקון מספר 39 בוועדת הכלכלה של

הכנסת מיום 12 ביוני 2012 בנימוק שמדובר בבעל תפקיד שיש לו סמכויות פיקוח, חקירה ואכיפה ואשר על כן יש צורך באמצעי שיאפשר לאזרח לזהותו. מאחר שהמפקחים אינם לובשים מדים אחידים מזוהים הוחלט שהם יידרשו לענוד תג זיהוי ויציגו תעודת מפקח לפי דרישה.[51] לדעתנו, ולנוכח ההסדר בדברי חקיקה דומים וחדשנותו של ההסדר בחוק הגנת הצרכן, אין מקום לקבוע הוראה דומה בחוק הגנת הפרטיות. יש לאפשר למפקח או לחוקר לעשות חקירה סמויה, וכך תתייעל האכיפה של דיני הגנת הפרטיות.

סימן ב': סמכויות פיקוח

סעיף 34: סמכויות מפקח

(א) לשם פיקוח על ביצוע ההוראות לפי פרקים ב', ד', ו-ו', רשאי ראש הרשות להגנת הפרטיות או מפקח שהוסמך על ידו –

(1) לדרוש מכל אדם למסור לו את שמו ומענו ולהציג לפניו תעודת זהות או תעודה רשמית אחרת המזהה אותו;

(2) לדרוש מכל אדם הנוגע בדבר למסור לו כל ידיעה או מסמך;

(3) לדרוש מכל אדם הנוגע בדבר להציג לפניו או למסור לו עותק מחומר מחשב הכולל נתוני מערכת או מידע אישי מדגמי; מידע אישי מידגמי לפי סעיף זה לא ייאסף בהיקף העולה על הנדרש למימוש תכליות הפיקוח.

(4) להיכנס למקום שיש לו יסוד סביר להניח שנעשה בו עיבוד של מידע אישי, ובלבד שלא ייכנס למקום המשמש למגורים אלא לפי צו של בית משפט.

(ב) הממונה ימחק מידע אישי מדגמי, שנמסר או שנאסף לפי סעיף זה, כאשר אינו נדרש עוד באופן סביר להמשך הליכי הפיקוח, ולכל היותר בתוך שלוש שנים ממועד מסירתו או איסופו, אלא אם כן המידע האישי המידגמי דרוש לצורך הליכים לפי פרק ג', סימנים ג' או ד'.

סימן ג': סמכויות בבירור מינהלי

סעיף 35: צו לחיפוש ולחדירה לחומר מחשב

היה לראש הרשות להגנת הפרטיות או לעובד המדינה שהוא הסמיך לכך בהודעה ברשומות, הכשיר לכהן כשופט של בית משפט מחוזי, יסוד סביר להניח כי בוצעה הפרה של הוראה מההוראות לפי חוק זה כאמור בסעיף 38, רשאי הוא לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב לפי סעיפים 23 עד 24 לפקודת המעצר והחיפוש, ולבצעם בעצמו או באמצעות מפקח.

סעיף 36: אופן ביצוע חדירה לחומר מחשב והעתקתו

על ביצוע חיפוש, תפיסת חפץ וחדירה לחומר מחשב או העתקתו לפי סימן זה, יחולו הוראות סעיפים 23א, 24(א)(1) ו (ב), 26 עד 28, 31 ו-45 וכן הוראות הפרק הרביעי, לפקודת המעצר והחיפוש, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות למפקח והסמכויות הנתונות לקצין יהיו נתונות לראש הרשות להגנת הפרטיות ולעובד המדינה שהוא הסמיך כאמור בסעיף 33.

דברי הסבר

<u>סעיף 34</u>: הסעיף מבוסס על סעיף 10(ה1) לחוק הגנת הפרטיות הקיים ועל סעיף 23י להצ"ח תיקון מס' 13.

<u>סעיפים 35 ו-36</u>: הסעיפים מבוססים על סעיפים 23יא ו-23יב להצ"ח תיקון מס' 13.

סעיף 37: סמכויות אכיפה, חקירה, עיכוב ותפיסה

(א) היה לראש הרשות להגנת הפרטיות או לחוקר יסוד סביר לחשד שנעברה עבירה לפי פרקים ב' או ו', או התעורר חשד כי אגב חקירה בעבירה כאמור, נעברה עבירה לפי סעיפים 242, 244, 245, 246, ו-249 לחוק העונשין, התשל"ז–1977[52] (להלן – חוק העונשין), יהיו נתונות לראש הרשות להגנת הפרטיות ולחוקר כל סמכויות הפיקוח לפי סימן ב', וכן רשאים הם –

(1) לחקור כל אדם הקשור לעבירה כאמור או שעשויות להיות לו ידיעות הנוגעות לעבירה כאמור; על חקירה לפי פסקה זו יחולו הוראות סעיפים 2 ו-3 לפקודת הפרוצדורה הפלילית (עדות),[53] והוראות חוק סדר הדין הפלילי (חקירת חשודים), התשס"ב–2002,[54] בשינויים המחויבים;

(2) לתפוס כל חפץ שיש לו יסוד סביר להניח שהוא חפץ הקשור לעבירה כאמור;

(3) לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב לפי סעיפים 23 עד 24 לפקודת המעצר והחיפוש, ולבצעו.

(ב) על ביצוע חיפוש, תפיסת חפץ וחדירה לחומר מחשב או העתקתו לפי סעיף זה יחולו סעיפים 23א, 24(א)(1) ו-(ב), 26 עד 28, 31 ו-45 וכן הוראות הפרק הרביעי לפקודת המעצר והחיפוש, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין יהיו נתונות לראש הרשות להגנת הפרטיות ולעובד המדינה שהוא הסמיך כאמור בסעיף 33.

(ג) היה לראש הרשות להגנת הפרטיות או לחוקר יסוד סביר לחשד שאדם עבר עבירה לפי פרקים ב' או ו', או התעורר חשד כי אגב חקירה בעבירה כאמור, נעברה עבירה לפי סעיפים 242, 244, 245, 246, ו-249 לחוק העונשין,[55] רשאי הוא לעכבו כדי לברר את זהותו ומענו או כדי לחוקרו במקום הימצאו; היה הזיהוי בלתי מספיק או שלא ניתן לחקור את אותו אדם במקום הימצאו, רשאי ראש הרשות להגנת הפרטיות או החוקר לדרוש מאותו אדם להתלוות אליו למשרדי ראש הרשות להגנת הפרטיות או לזמנו למשרדי הרשות להגנת הפרטיות למועד אחר שיקבע. מי שזומן למשרדי ראש הרשות להגנת הפרטיות יתייצב במועד שזומן אליו; על עיכוב לפי סעיף קטן זה יחולו הוראות סעיפים 66, 67 ו-72 עד 74 לחוק המעצרים, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין הממונה יהיו נתונות לראש הרשות להגנת הפרטיות.

(ד) היה לראש הרשות להגנת הפרטיות או לחוקר יסוד סביר לחשד שנעברה עבירה לפי פרקים ב' או ו', או התעורר חשד כי אגב חקירה בעבירה כאמור, נעברה עבירה לפי סעיפים 242, 244, 245, 246, ו-249 לחוק העונשין, רשאי הוא לעכב אדם שיכול למסור לו מידע הנוגע לאותה עבירה, כדי לברר את זהותו ומענו וכדי לחקור אותו במקום הימצאו; וכן רשאי הוא לזמן אותו למשרדי ראש הרשות להגנת הפרטיות למועד סביר אחר שיקבע לצורך ביצוע אותן פעולות; מי שזומן למשרדי ראש הרשות להגנת הפרטיות, יתייצב

במועד שזומן אליו; על עיכוב לפי סעיף קטן זה יחולו הוראות סעיפים 68 ו-72 עד 74 לחוק המעצרים, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין הממונה יהיו נתונות לראש הרשות להגנת הפרטיות.

(ה) לעניין סעיפים קטנים (ג) ו-(ד) יראו את משרדי ראש הרשות להגנת הפרטיות שראש הרשות הכריז עליהם בהודעה ברשומות, כ"תחנת משטרה" לעניין הוראות חוק המעצרים.

דברי הסבר

סעיף 37: הסעיף מבוסס על סעיף 23יג להצ"ח תיקון מס' 13, אך מרחיב את סמכות האכיפה הנתונה לראש הרשות להגנת הפרטיות או לחוקר לביצוע חקירה גם בעבירות נלוות לעבירות לפי חוק זה (סעיפים 242 (השמדת ראיה), 244 (שיבוש מהלכי משפט), 245 (הדחה בחקירה), 246 (הדחה בעדות), ו-249 (הטרדת עד) לחוק העונשין, התשל"ז-1977).

הרחבת סמכות האכיפה כמוצע בסעיף גם לעבירת נלוות מבוססת על סעיף דומה בחוק ההגבלים העסקיים, התשמ"ח–1988, ובחוק ניירות ערך, התשכ"ח–1968. הרחבה זו של סמכות האכיפה נועדה למנוע מצב שבו לא מנוהלת חקירה במכלול השלם של העבירות בנימוק שהעבירה הנלווית אינה חמורה דייה כדי להצדיק חקירת משטרה נפרדת. ולכן הסעיף המוצע מגדיר את הרשות להגנת הפרטיות כרשות חקירה עצמאית, בדומה לרשות לניירות ערך ולרשות להגבלים עסקיים, וכן מאפשר לחוקריה לחקור חשדות לשיבוש הליכי חקירה מסוגים שונים כאשר מתעורר חשד שנעשו פעולות לשיבושה. כפי שנאמר בדברי ההסבר להצעת חוק ההגבלים העסקיים (תיקון מס' 5), התשנ"ט–1999, "הוראה זו עולה בקנה אחד עם מגמת המחוקק המנסה להקשות על שיבוש הליכי משפט, וסמכויות דוגמתה הוענקו לרשויות שונות בידי השר לביטחון פנים."[56]

בניסוח הסעיף נעזרנו במקורות שלהלן:

סעיף 46 לחוק ההגבלים העסקיים, התשמ"ח–1988:

"(א) התעורר חשד לביצוע עבירה לפי חוק זה, או התעורר חשד כי אגב חקירה בעבירה לפי חוק זה, נעברה עבירה לפי סעיפים 242, 244, 245, 246, ו-249 לחוק העונשין, רשאי הממונה, או מי שהוא הסמיך לכך (להלן – חוקר), לחקור כל אדם הקשור לעבירה מעבירות כאמור, או שעשויות להיות לו ידיעות הנוגעות להן, ולדרוש מכל אדם כאמור להתייצב בפניו לשם חקירה כאמור, ולהתלוות אליו לחקירה ולמסור לו כל פרט, מסמך וידיעה הנוגעים לאותה עבירה; על הוראות החקירה יחולו הוראות סעיפים 2 ו-3 לפקודת הפרוצדורה הפלילית (עדות);"

סעיף 56 לחוק ניירות ערך, התשכ"ח–1968:

"56א.(א) כדי להבטיח את ביצועו של חוק זה, או אם היה יסוד סביר להניח כי בוצעה הפרה או התעורר חשד לביצוע עבירת ניירות ערך, רשאי יושב ראש הרשות או עובד הרשות שהוא הסמיכו לכך בכתב –

(1) לדרוש מכל אדם כל ידיעה ומסמך, הנוגעים לעסקי תאגיד שחוק זה חל עליו, או הנוגעים להפרה או לעבירה כאמור;

(2) להיכנס, לאחר שהזדהה, למקום שיש לו יסוד להניח כי מתקיימת בו פעילות של גורם מפוקח ושאינו משמש בית מגורים בלבד, ולדרוש למסור לו מסמכים כאמור בפסקה (1); ואולם אין לתפוס מסמך כאמור אם ניתן להסתפק בהעתק ממנו."

סעיף 1 לחוק ניירות ערך, התשכ"ח–1968, מגדיר "עבירת ניירות ערך" ככוללת "(1) עבירה לפי חוק זה; (3) עבירה לפי סעיפים 284, 290, 291, 415, 423, 424, 424א, ו-425 לחוק העונשין, שנעברה בקשר לעבירה לפי פסקאות (1) או (6); (4) עבירה לפי סעיפים 3 ו-4 לחוק איסור הלבנת הון, שנעברה בקשר לעבירה לפי פסקאות (1) או (6); (5) עבירה לפי סעיפים 240, 242, 244, 245, ו-246 לחוק העונשין, שנעברה בקר לחקירה או להליך שיפוטי בשל עבירה לפי פסקאות (1), (3), (4) או (6); (6) עבירה לפי על חיקוק אחר ששר המשפטים והשר לביטחון הפנים קבעו בצו, באישור ועדת החוקה חוק ומשפט של הכנסת;".

פרק ד: אמצעי אכיפה מינהליים

<u>סימן א': עיצום כספי</u>

סעיף 38: עיצום כספי

(א) הפר אדם הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי ראש הרשות להגנת הפרטיות להטיל עליו עיצום כספי בסכום של ___, ואם המפר הוא תאגיד – בסכום של ___:

(1) עיבד מידע אישי מבלי שמילא את חובת מתן הודעה, בניגוד להוראות סעיף 9;

(2) הפר את זכותו של נושא מידע לחזור בו מהסכמתו, בניגוד להוראות סעיף 10;

(3) הפר את זכות מזכויות נושא מידע לעיין במידע אישי על אודותיו, לקבל הסבר, לתקן, לנייד או למחוק מידע אישי על אודותיו, בניגוד להוראת סעיפים 11; 12, 13, 14 ו-15 בהתאמה; או בניגוד להוראות שנקבעו לעניין זה לפי סעיף 16;

(4) סירב לבקשת נושא מידע למימוש זכות מזכויות נושא המידע כאמור בסעיפים 11(ה) עד (ח), 13(ד), 14(ו) או 15(ג), ולא הודיע על כך לנושא המידע כנדרש לפי סעיף 16(ד).

(ב) הפר אדם הוראה מההוראות חוק זה, כמפורט להלן, רשאי ראש הרשות להגנת הפרטיות להטיל עליו עיצום כספי בסכום של ___, ואם המפר הוא תאגיד – בסכום של ___:

(1) עיבד מידע אישי שלא למטרה לשמה נמסר, בניגוד להוראות סעיף 7;

(2) לא תיכנן, עיצב או הפעיל את מערכות עיבוד המידע האישי שיבטיחו את התאמתן להוראות חוק זה, בניגוד להוראות סעיף 19;

(3) לא הכין תסקיר השפעה על הפרטיות, בניגוד להוראות סעיף 20;

(4) לא נקט אמצעים סבירים לאבטחת מידע אישי, בניגוד להוראות סעיף 21;

(5) לא תיעד או דיווח על אירועי אבטחה, בניגוד להוראות סעיף 22;

(6) לא מינה ממונה הגנת פרטיות במידע או הסמיכו לבצע את תפקידיו, בניגוד להוראות סעיף 23;

דברי הסבר

<u>סעיף 38:</u> הסעיף מבוסס על הוראת סעיף 23יט להצ"ח תיקון מס' 13 ושואב השראה מהוראות סימן א' בפרק ה1 לחוק הגנת הצרכן, התשמ"א-1981. בחרנו את הוראות חוק הגנת הצרכן כמקור להשראה בשל הדמיון הרב בין אופי ומספר ההפרות והמפרים האפשריים. שני החיקוקים עוסקים במספר רב של הפרות ובמספר רב של מֵפרים קטנים וגדולים. חוק הגנת הצרכן מייצג את המודל העכשווי המעודכן ביותר לעיגונה החקיקתי של סמכות מינהלית להטלת עיצום כספי על פי המתווה של משרד המשפטים.

בחרנו שלא לאמץ את המנגנון המסורבל בעינינו בסעיף 23יט להצ"ח תיקון מס' 13, הקובע שהעיצום הכספי ייקבע לפי סכום בסיס ומכפלותיו בהתאם למספר נושאי המידע במאגר מידע ובהתאם לקיומו של מידע רגיש. במקום זה קבענו מנגנון, הקבוע בחוק הגנת הצרכן, שלפיו סכום העיצום הכספי יפורט כאשר ההפרה נעשית על ידי תאגיד או כאשר ההפרה נעשית בידי אדם שאינו תאגיד. כמו כן אימצנו בסעיף 39 את הוראת סעיף 22ד לחוק הגנת הצרכן לעניין הפרה בנסיבות מחמירות הנותנת את הדעת למספר נושאי המידע הנפגעים בתור שיקול אחד מני מכלול השיקולים.

מנגנון הסכום הבסיסי לפי סעיף 23יט(א) להצ"ח תיקון מס' 13:

"הסכום הבסיסי" – סכום כמפורט להלן, לפי העניין:

(1) לעניין הפרה בקשר למאגר מידע הכולל מידע על מספר אנשים שאינו עולה על 1,000, שיש בו רק מידע רגיל – 5,000 ש"ח; ואם יש בו גם מידע בעל רגישות מיוחדת – 50,000 ש"ח;

(2) לעניין הפרה בקשר למאגר מידע הכולל מידע על מספר אנשים העולה על 10,000 ואינו עולה על 100,000 שיש בו רק מידע רגיל – 20,000 ש"ח; ואם יש בו גם מידע בעל רגישות מיוחדת – 200,000 ש"ח;

(3) לעניין הפרה בקשר למאגר מידע הכולל מידע על מספר אנשים העולה על 100,000 ואינו עולה על 1,000,000, שיש בו רק מידע רגיל – 40,000 ש"ח; ואם יש בו גם מידע בעל רגישות מיוחדת – 400,000 ש"ח;

(4) לעניין הפרה בקשר למאגר מידע שיש בו מידע על מספר אנשים העולה על 1,000,000, שיש בו רק מידע רגיל – 80,000 ש"ח; ואם יש בו גם מידע בעל רגישות מיוחדת – 800,000 ש"ח.

בנוסף, התאמנו את ההפרות שבגינן יוטל עיצום כספי להוראות הדין המהותי בהצעת החוק. לפיכך לא אימצנו את סעיפים 23טז(ב), 23יט(ד)(2), 23יט(ג)(7), ו-יט(ג)(9), (10), (11), (12) להצ"ח תיקון מס' 13, שכן הצעת החוק אינה מאמצת את תפיסת מאגרי המידע ואת חובת רישומם וגם אינה כוללת התייחסות לסוגיית הדיוור הישיר.

סעיף 23יט(ב) להצ"ח תיקון מס' 13:

"(ב) הפר אדם הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי הממונה להטיל עליו עיצום כספי בסכום הבסיסי:

(1) ניהל או החזיק מאגר מידע החייב ברישום שלא בהתאם להוראות סעיף 8(א);

(2) כלל פרטים לא נכונים בבקשה לרישום מאגר מידע שהוגשה לפי סעיף 9;

(3) לא הודיע לממונה על שינוי בפרט מהפרטים המפורטים בסעיף 9(ב) או לפי סעיף 9(ג), בניגוד להוראות סעיף 9(ד);

(4) החזיק ברשותו חמישה מאגרי מידע לפחות, החייבים ברישום לפי סעיף 8, ולא קיים את חובת הדיווח השנתי בהתאם להוראות סעיף 17א(ב);

(5) ניהל או החזיק מאגר מידע המשמש לשירותי דיוור ישיר, בלי שיש בידו רישום המציין את המקור שממנו קיבל כל אוסף נתונים המשמש לצורך מאגר המידע ומועד קבלתו וכן למי מסר כל אוסף נתונים כאמור, בניגוד להוראות סעיף 17ה;

(6) לא פירט על דרישת מידע כי הוא מוסר דרך קבע מידע בהתאם לסעיף 23ג, בניגוד להוראות סעיף 23ד(א);

(7) לא קיים רישום של המידע שמסר בהתאם לסעיף 23ג, בניגוד להוראת סעיף 23ד(ב);

(8) לא הודיע לממונה כי הוא מקבל מידע דרך קבע בהתאם לסעיף 23ג והמידע נאגר במאגר מידעף בניגוד להוראות סעיף 23ד(ג);

(9) מסר פרטים לא נכונים במענה לדרישה של הממונה או מפקח לפי סעיף 23י(א)(1) עד (3)."

סעיף 23יט(ד)(2) להצ"ח תיקון מס' 13:

"השתמש במידע ממאגר מידע בלא הרשאה של בעל מאגר המידע, או תוך חריגה מהרשאה כאמור, בניגוד לסעיף 23מה; לעניין זה, מי שברשותו עותק של מאגר מידע, או חלק מהותי ממנו, יראו אותו כמי שמשתמש במידע ממאגר המידע, אלא אם כן הוכיח אחרת."

הוראת סעיף קטן (א) מבוססת על הוראת סעיף 23טז(ג) להצ"ח תיקון מס' 13, המציגה רשימת הפרות שהעיצום הכספי שאפשר להטיל בגינן הוא כפל הסכום הבסיסי. הוראת סעיף קטן (א)(1) מבוססת, בשינויים הנובעים מחוסר ההתייחסות בהצעת החוק למאגרי מידע, על הוראת סעיף 23טז(ג)(1) להצ"ח תיקון מס' 13, שלשונו:

"(1) פנה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע, בלי שמסר לו הודעה כנדרש בסעיף 11;"

סעיף 23יט(ג)(7) להצ"ח תיקון מס' 13:

"(7) החזיק במאגרי מידע של בעלים שונים בלי שהבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בינו לבין בעליו של אותו מאגר, בניגוד להוראות סעיף 17א(א);"

סעיפים 23יט(ג)(9), (10), (11), (12) להצ"ח תיקון מס' 13:

"(9) ניהל או החזיק מאגר מידע המשמש לישורתי דיוור ישיר, בלא שהמאגר היה רשום במרשם ובלא שאחת ממטרותיו הרשומות של המאגר היא שירותי דיוור ישיר, בניגוד להוראות סעיף 17ד;

(10) פנה לאדם בדיוור ישיר באופן שאינו עומד בהוראות סעיף 17ו(א) לחוק;

(11) לא נענה לדרישתו של אדם בהתאם לסעיף 17ו(ב), שמידע המתייחס אליו יימחק ממאגר מידע המשמש לדיוור ישיר, בניגוד להוראות סעיף 17ו(ד).

(12) לא נענה לדרישתו של אדם בהתאם לסעיף 17ו(ג), כי מידע המתייחס אליו, לא יימסר לאדם, לסוג בני אדם או לאנשים מסוימים, בניגוד להוראות סעיף 17ו(ד);"

הוראת סעיף קטן (א)(3) מבוססת, בשינויים הנובעים מהיעדר ההתייחסות בחוק המוצע למאגרי מידע, על הוראת סעיף 23טז(ג)(2) להצ"ח תיקון מס' 13, שלשונו: "(2) סירב לאפשר לאדם שמידע עליו מוחזק במאגר מידע לעיין במידע שעליו, בניגוד להוראות לפי סעיף 13;" ההוראה הורחבה כדי לתת מענה למקרים שיש מקום להטיל בהם עיצום כספי בגלל הפרת ההוראות, על פי הצעת החוק, בעניין הזכויות החדשות של נושא המידע.

הוראת סעיף קטן (א)(4) מבוססת על הוראת סעיפים 23טז(ג)(3)-(5) להצ"ח תיקון מס' 13.

סעיפים 23טז(ג)(3)-(5) להצ"ח תיקון מס' 13:

"(3) ביצע שינוי במידע שברשותו בלי שהודיע עליו לכל מי שקיבל את המידע בניגוד להוראות לפי סעיף 14(ב);

(4) לא הודיע למבקש על סירוב לתקן מידע המצוי במאגר מידע שבבעלותו או למוחקו, בניגוד להוראות לפי סעיף 14(ג);

(5) לא תיקן מידע המצוי במאגר מידע שבהחזקתו, בניגוד להוראות סעיף 14(ד);"

בדומה להבחנה המוצעת גם היום בהצ"ח תיקון מס' 13, גם אנחנו בחרנו להבחין בין הפרות הקשורות בכיבוד זכויותיו של נושא המידע, המנויות בס"ק (א), לבין הפרות הקשורות לחובות של בעל שליטה במידע ומעבד ולדרך עיבוד המידע האישי, לתנאים המקדימים לעיבודו ולהתוויית אופן עיבוד המידע האישי, המנויים בס"ק (ב).

לדעתנו, החובות לאבטחת מידע אישי ולמינוי ממונה על הגנת הפרטיות במידע צריכות להיכלל תחת קטגוריה זו. משום כך הוראת סעיף 23יט(ג)(6) להצ"ח תיקון מס' 13 – המטילה עיצום כספי בגין הפרה של החובה לאבטחת מידע הקבועה בתיקון המוצע בהצ"ח תיקון מס' 13 לסעיף 17(ב) לחוק הגנת הפרטיות הקיים – הוכנסה על ידינו, בשינויים המחויבים, להוראות סעיפים קטנים (ב)(4), (5) ו-(6), הכוללים

את הדרישות בהצעת החוק בעניין אבטחת מידע אישי.

סעיף 23ביט(ג)(6) להצ"ח תיקון מס' 13:
"הפר הוראה מההוראות שנקבעו לפי סעיף 17(ב);"

סעיף 4 להצ"ח תיקון מס' 13, המציע תיקון לסעיף 17(ב) לחוק הגנת הפרטיות הקיים:
"(ב)(1) השר רשאי לקבוע הוראות לעניין האחריות לאבטחת המידע הקבועה בסעיף קטן (א) ובסעיף 17ב(ב), ובכלל זה היקפה והחובות הכלולות בה, וכן לעניין דרכי אבטחת המידע כאמור, בין השאר בעניינים האלה:
(א) הגנה פיזית ולוגית על המאגר;
(ב) סדרי הניהול וכללי העבודה במאגר המידע ובקשר אליו, לרבות לעניין קביעה של הגבולות על גישה של מועסקים למידע.
(2) בתקנות לפי פסקה (1), יכול שייקבעו הוראות שונות לגבי מאגרים בעלי מאפיינים שונים.
(3) תקנות לפי פסקה (1) שיחולו על גופים המנויים בתוספת הראשונה, השנייה והרביעית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998, יותקנו בהתייעצות עם ראש הממשלה, ואולם תקנות כאמור לעניין גופים המנויים בפרטים 2 ו-3 לתוספת הראשונה של החוק האמור, יתוקנו בהתייעצות עם שר הביטחון."

סעיפים קטנים (ב)(2) ו (3) בהצעת החוק קשורים להוראות הנוגעות לעיצוב לפרטיות ולעריכת תסקיר השפעה על הפרטיות בסעיפים 19 ו-20.

סעיף קטן (ב)(1) מבוסס על הוראת סעיף 23ביט(ד)(1) להצ"ח תיקון מס' 13 ומותאם לדרישת קיום המטרה שבסעיף 7 להצעת החוק.

סעיף 23ביט(ד)(1) להצ"ח תיקון מס' 13:
"השתמש במידע ממאגר המידע שלא למטרה שלשמה נמסר, בניגוד לסעיף 23מד;"

סעיף 39: הפרה בנסיבות מחמירות

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי הפר אדם הוראה מההוראות לפי חוק זה המפורטות בסעיף 38, בנסיבות מחמירות, רשאי ראש הרשות להגנת הפרטיות להטיל עליו עיצום כספי לפי הוראות פרק זה, ששיעורו פי אחד וחצי מסכום העיצום הכספי שניתן להטיל בשל אותה הפרה לפי סעיף 38.

(ב) בסעיף זה, "נסיבות מחמירות" – הפרה הנוגעת ל-100,000 נושאי מידע לפחות, או הפרה הנוגעת למידע רגיש.

דברי הסבר

<u>סעיף 39:</u> מבוסס על סעיף 22ד לחוק הגנת הצרכן. לפי ההסדר שבחוק הגנת הצרכן, בנסיבות מחמירות יהיה מותר להטיל על המפר עיצום כספי בסכום גבוה מן הסכום הקבוע להפרה. נסיבות מחמירות מתקיימות לפי סעיף 22ד לחוק הגנת הצרכן כאשר מדובר במספר גדול של צרכנים או כאשר ההפרה נעשית על ידי עוסק ביותר מסניף אחד או נקודת מכירה אחת.

אימוץ הוראה דומה לסעיף 22ד לחוק הגנת הצרכן בסעיף 39 להצעת החוק מאפשר להקשיח את סנקציית העיצום הכספי כאשר מדובר במספר רב של נושאי מידע שעלולים להיפגע או כאשר מדובר במידע רגיש – כל זה בלי לאמץ את ההסדר המסורבל המוצע בהצ"ח תיקון מס' 13 באשר לסכום הבסיסי ולכפולותיו. לשם השמירה על האחידות בחקיקה קבענו אמת מידה כמותית זהה לזו הקבועה בסעיף 23 – 100,000 נושאי מידע לפחות.

בקבוצת המומחים היו שנרתעו מאימוץ סעיף בנוסח דומה לקבוע בחוק הגנת הצרכן בשל הדרישה להוכחת תשתית עובדתית מחמירה יחסית: "היה לראש הרשות יסוד סביר להניח". ואולם מאחר שזהו הנוסח המקובל בחקיקה היום לעניין הטלת עיצומים כספיים בנסיבות מחמירות, אימצנו את נוסח סעיף 22ד לחוק הגנת הצרכן במלואו.

סעיף 22ד לחוק הגנת הצרכן:

"(א) היה לממונה יסוד סביר להניח כי עוסק הפר הוראה מההוראות לפי חוק זה המפורטות בסעיף 22ג, בנסיבות מחמירות, רשאי הממונה להטיל עליו עיצום כספי לפי הוראות פרק זה, ששיעורו פי אחד וחצי מסכום העיצום הכספי שניתן להטיל בשל אותה הפרה לפי סעיף 22ג.

(ב) בסעיף זה, "נסיבות מחמירות" – הפרה הנוגעת למספר רק במיוחד של צרכנים; לעניין זה, חזקה כי הפרה שנעשתה על ידי עוסק ביותר מסניף אחד או נקות מכירה אחת המופעלים על ידו, היא הפרה הנוגעת למספר רק במיוחד של צרכנים."

סעיף 40: הודעה על כוונת חיוב

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי הפר אדם הוראה מההוראות לפי חוק זה, כאמור בסעיף 38 (בפרק זה – המפר), ובכוונתו להטיל עליו עיצום כספי לפי אותו סעיף או לפי סעיף 39, ימסור למפר הודעה על הכוונה להטיל עליו עיצום כספי (בפרק זה – הודעה על כוונת חיוב).

(ב) בהודעה על כוונת חיוב יציין ראש הרשות להגנת הפרטיות, בין השאר, את אלה:

(1) המעשה או המחדל (בפרק זה – המעשה), המהווה את ההפרה, ומועד ביצועו;

(2) סכום העיצום הכספי והתקופה לתשלומו;

(3) זכותו של המפר לטעון את טענותיו לפני ראש הרשות להגנת הפרטיות לפי הוראות סעיף 41;

(4) שיעור התוספת על העיצום הכספי בהפרה נמשכת או בהפרה חוזרת לפי הוראות סעיף 43.

סעיף 41: זכות טיעון

(א) מפר שנמסרה לו הודעה על כוונת חיוב לפי הוראות סעיף 40 רשאי לטעון את טענותיו, בכתב או בעל פה, לעניין הכוונה להטיל עליו עיצום כספי ולעניין סכומו, בתוך 45 ימים ממועד מסירת ההודעה.

(ב) ראש הרשות להגנת הפרטיות רשאי, לבקשת המפר, להאריך את התקופה האמורה בסעיף קטן (א) בתקופה נוספת שלא תעלה על 45 ימים.

סעיף 42: החלטת ראש הרשות להגנת הפרטיות ודרישת תשלום

(א) ראש הרשות להגנת הפרטיות יחליט, לאחר ששקל את הטענות שנטענו לפי סעיף 41, אם להטיל על המפר עיצום כספי, ורשאי הוא להפחית את סכום העיצום הכספי לפי הוראות סעיף 44.

(ב) החליט ראש הרשות לפי סעיף קטן (א) –

(1) להטיל על המפר עיצום כספי – ימסור לו דרישה, בכתב, לשלם את העיצום הכספי (בפרק זה – דרישת תשלום), שבה יציין, בין השאר, את סכום העיצום הכספי המעודכן ואת התקופה לתשלומו כאמור בסעיף 46;

(2) שלא להטיל על המפר עיצום כספי – ימסור לו הודעה על כך, בכתב.

(ג) בדרישת התשלום או בהודעה, לפי סעיף קטן (ב), יפרט ראש הרשות להגנת הפרטות את נימוקי החלטתו.

(ד) לא טען המפר את טענותיו לפי הוראות סעיף 41 בתוך התקופה האמורה באותו סעיף, יראו את ההודעה על כוונת חיוב, בתום אותה תקופה, כדרישת תשלום שנמסרה למפר במועד האמור.

סעיף 43: הפרה נמשכת והפרה חוזרת

(א) בהפרה נמשכת, יווסף על העיצום הכספי הקבוע לאותה הפרה, החלק החמישים שלו לכל יום שבו נמשכת ההפרה; לעניין זה, "הפרה נמשכת" – הפרת הוראה מההוראות לפי חוק זה, כאמור בסעיף 38, לאחר שנמסרה למפר דרישת תשלום בשל הפרת אותה הוראה או לאחר שנמסרה למפר התראה מינהלית כמשמעותה בסעיף 49, בשל הפרת אותה הוראה וההתראה לא בוטלה כאמור בסעיף 50.

(ב) בהפרה חוזרת יווסף על העיצום הכספי הקבוע לאותה הפרה, סכום השווה לעיצום הכספי כאמור; לעניין זה, "הפרה חוזרת" – הפרת הוראה מההוראות לפי חוק זה, כאמור בסעיף 38(א), בתוך שנתיים מהפרה קודמת של אותה הוראה שבשלה הוטל על המפר עיצום כספי או שבשלה הורשע, ולעניין הפרות לפי סעיף 38(ב) – בתוך תשעה חודשים מהפרה קודמת של הוראות אלה.

סעיף 44: סכומים מופחתים

(א) ראש הרשות להגנת הפרטיות אינו רשאי להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים בסימן זה, אלא לפי הוראות סעיף קטן (ב).

(ב) שר המשפטים רשאי לקבוע מקרים, נסיבות ושיקולים שבשלהם יהיה ניתן להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים בסימן זה, ובשיעורים שיקבע.

סעיף 45: סכום מעודכן של הפיצוי הכספי

העיצום הכספי יהיה לפי סכומו המעודכן לפי סעיף 78 ביום מסירת דרישת התשלום, ולגבי מפר שלא טען את טענותיו לפני ראש הרשות להגנת הפרטיות כאמור בסעיף 42(ד) – ביום מסירת ההודעה על כוונת החיוב; הוגשה עתירה לבית המשפט לעניינים מינהליים או הוגש ערעור על החלטה בעתירה כאמור ועוכב תשלומו של העיצום הכספי בידי ראש הרשות להגנת הפרטיות או בית המשפט – יהיה העיצום הכספי לפי סכומו המעודכן ביום ההחלטה בעתירה או בערעור, לפי העניין.

סעיף 46: המועד לתשלום העיצום הכספי

המפר ישלם את העיצום הכספי בתוך 45 ימים מיום מסירת דרישת התשלום כאמור בסעיף 42.

סעיף 47: הפרשי ריבית והצמדה

לא שילם המפר עיצום כספי במועד, ייווספו על העיצום הכספי לתקופת הפיגור, הפרשי הצמדה וריבית כהגדרתם בחוק פסיקת ריבית והצמדה, התשכ"א–1961[57] (בפרק זה – הפרשי הצמדה וריבית), עד לתשלומו.

סעיף 48: גבייה

עיצום כספי ייגבה לאוצר המדינה, ועל גבייתו יחול חוק המרכז לגביית קנסות, אגרות והוצאות, התשנ"ה-1995.[58]

דברי הסבר

<u>סעיפים 40-48:</u> מבוססים על הוראות סעיפים 23כ-23כח להצ"ח תיקון מס' 13 והתאמתם להוראות סימן א' בפרק ה'1 לחוק הגנת הצרכן, התשמ"א-1981, שמציג מתווה מעודכן יותר להטלת עיצום כספי על ידי רשות מינהלית.

סימן ב': התראה מינהלית

סעיף 49: התראה מינהלית

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 38, והתקיימו נסיבות שקבע ראש הרשות להגנת הפרטיות בנהלים, רשאי הוא, במקום להמציא לו הודעה על כוונת חיוב ולהטיל עליו עיצום כספי, לפי הוראות סימן א', להמציא לו התראה מינהלית לפי הוראות סימן זה.

(ב) בהתראה מינהלית יציין ראש הרשות להגנת הפרטיות מהו המעשה המהווה את ההפרה, יודיע למפר כי עליו להפסיק את ההפרה וכי אם ימשיך בהפרה או יחזור עליה יהיה צפוי לעיצום כספי בשל הפרה נמשכת או הפרה חוזרת, לפי העניין, כאמור בסעיף 43, וכן יציין את זכותו של המפר לבקש את ביטול ההתראה לפי הוראות סעיף 50.

סעיף 50: בקשה לביטול התראה מינהלית

(א) נמסרה למפר התראה מינהלית כאמור בסעיף 49 רשאי הוא לפנות לראש הרשות להגנת הפרטיות, בכתב או בעל פה, בתוך 45 ימים, בבקשה לבטל את ההתראה בשל כל אחד מטעמים אלה:

(1) המפר לא ביצע את ההפרה;

(2) המעשה שביצע המפר, המפורט בהתראה, אינו מהווה הפרה.

(ב) קיבל ראש הרשות להגנת הפרטיות בקשה לביטול התראה מינהלית, לפי הוראות סעיף קטן (א), רשאי הוא לבטל את ההתראה או לדחות את הבקשה ולהותיר את ההתראה על כנה; החלטת ראש הרשות להגנת הפרטיות תינתן בכתב ותימסר למפר בצירוף נימוקים.

סעיף 51: הפרה נמשכת והפרה חוזרת לאחר התראה

(א) נמסרה למפר התראה מינהלית לפי הוראות סימן זה והמפר המשיך להפר את ההוראה שבשלה נמסרה לו ההתראה, ימסור לו ראש הרשות להגנת הפרטיות דרישת תשלום בשל הפרה נמשכת כאמור בסעיף 43(א); דרישת תשלום אינה גורעת מזכותו של המפר לטעון כאמור בסעיף 41 לעניין סכום העיצום הכספי ולעניין הימשכות ההפרה, וייחולו הוראות סעיפים 41 ו-42, בשינויים המחויבים.

(ב) נמסרה למפר התראה מינהלית לפי הוראות סימן זה והמפר חזר והפר את ההוראה שבשלה נמסרה לו ההתראה, בתוך שנתיים מיום מסירת ההתראה, יראו את ההפרה הנוספת כאמור כהפרה חוזרת לעניין סעיף 43(ב), וראש הרשות להגנת הפרטיות ימסור למפר הודעה על כוונת חיוב לפי הוראות סעיף 40 בשל ההפרה החוזרת.

דברי הסבר

סעיף 49: הסעיף מבוסס על הוראת סעיף 23כט להצ"ח תיקון מס' 13, אם כי בחרנו לאמץ את ההסדר הקבוע בסעיף 22יג לחוק הגנת הצרכן, המפנה לסעיף סל בעניין אישור הנהלים שייקבעו על ידי הממונה על הגנת הצרכן ובאישור היועץ המשפטי לממשלה.

סעיף 23כט להצ"ח תיקון מס' 13:

"(א) היה לממונה יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 23יט, והתקיימו נסיבות שקבע הממונה, בנהלים, באישור היועץ המשפט לממשלה, רשאי הוא, במקום להמציא לו הודעה על כוונת חיוב ולהטיל

עליו עיצום כספי, לפי הוראות סימן א', להמציא לו התראה מינהלית לפי הוראות סימן זה; בסעיף קטן זה, "היועץ המשפטי לממשלה" – לרבות משנה ליועץ המשפטי לממשלה שהיועץ המשפטי לממשלה הסמיכו לעניין זה.

(ב) בהתראה מינהלית יציין הממונה מהו המעשה המהווה את ההפרה, יודיע למפר כי עליו להפסיק את ההפרה וכי אם ימשיך בהפרה או יחזור עליה יהיה צפוי לעיצום כספי בשל הפרה נמשכת או הפרה חוזרת, לפי העניין, כאמור בסעיף 23לא, וכן יציין את זכותו של המפר לבקש את ביטול ההתראה לפי הוראות סעיף 23ל."

<u>סעיפים 50-51:</u> הסעיפים מבוססים על סעיפים 23ל ו-23לא להצ"ח תיקון מס' 13 ועל סעיפים 22יד ו-22טו לחוק הגנת הצרכן.

סימן ג': התחייבות להימנע מהפרה

סעיף 52: התחייבות להימנע מהפרה והפקדת עירבון

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 38, והתקיימו נסיבות המנויות בנהלים שקבע ראש הרשות להגנת הפרטיות, רשאי הוא להציע למפר, בהודעה בכתב, להגיש לו כתב התחייבות ועירבון מסוג שייקבע בנהלים, לפי הוראות סימן זה, במקום שיוטל עליו עיצום כספי לפי הוראות סימן א'.

(ב) בכתב ההתחייבות יתחייב המפר להפסיק את הפרת ההוראה כאמור בסעיף קטן (א), ולהימנע מהפרה נוספת של אותה הוראה בתוך תקופה שיקבע ראש הרשות להגנת הפרטיות, שתחילתה ביום מסירת ההודעה כאמור באותו סעיף קטן, ובלבד שהתקופה האמורה לא תעלה על שנתיים (בסימן זה – תקופת ההתחייבות).

(ג) ראש הרשות להגנת הפרטיות רשאי לדרוש כי המפר יכלול בכתב ההתחייבות תנאים נוספים שעליו לעמוד בהם בתקופת ההתחייבות לשם הקטנת הנזק שנגרם מההפרה או מניעת הישנותה.

(ד) נוסף על כתב ההתחייבות יפקיד המפר בידי ראש הרשות להגנת הפרטיות עירבון בסכום העיצום הכספי שראש הרשות להגנת הפרטיות היה רשאי להטיל על המפר בשל אותה הפרה, בהתחשב בקיומן של מקרים, נסיבות ושיקולים שנקבעו לפי סעיף 44.

סעיף 53: תוצאות הגשת כתב התחייבות ועירבון או אי הגשתם

(א) הגיש המפר לראש הרשות להגנת הפרטיות כתב התחייבות ועירבון לפי סימן זה, בתוך 45 ימים מיום מסירת ההודעה כאמור בסעיף 52, לא יוטל עליו עיצום כספי בשל אותה הפרה.

(ב) לא הגיש המפר לראש הרשות להגנת הפרטיות כתב התחייבות ועירבון בתוך 45 ימים מיום מסירת ההודעה כאמור בסעיף 52, ימציא לו ראש הרשות להגנת הפרטיות הודעה על כוונת חיוב בשל אותה הפרה, לפי סעיף 40.

סעיף 54: הפרת התחייבות

(א) הגיש המפר כתב התחייבות ועירבון לפי סימן זה והפר תנאי מתנאי ההתחייבות, כמפורט להלן, יחולו הוראות אלה, לפי העניין:

(1) המשיך המפר, במהלך תקופת ההתחייבות, להפר את ההוראה שבשל הפרתה נתן את כתב ההתחייבות – יחלט ראש הרשות להגנת הפרטיות את העירבון וימציא למפר דרישת תשלום בשל ההפרה הנמשכת כאמור בסעיף 43(א);

(2) חזר המפר והפר, במהלך תקופת ההתחייבות, את ההוראה שבשל הפרתה נתן את כתב ההתחייבות – יחלט ראש הרשות להגנת הפרטיות את העירבון ויראו את ההפרה הנוספת כאמור כהפרה חוזרת לעניין סעיף 43(ב); ראש הרשות להגנת הפרטיות ימציא למפר הודעה על כוונת חיוב בשל ההפרה החוזרת;

(3) הפר המפר תנאי מהתנאים הנוספים שנקבעו בכתב ההתחייבות כאמור בסעיף 52 – יודיע ראש הרשות להגנת הפרטיות למפר על כוונתו לחלט את העירבון; המפר רשאי לטעון את טענותיו לעניין זה, בכתב או בעל פה, כפי שיורה

ראש הרשות להגנת הפרטיות, בתוך 45 ימים מיום הודעת ראש הרשות להגנת הפרטיות, וראש הרשות להגנת הפרטיות רשאי, לבקשת המפר, להאריך תקופה זו בתקופה נוספת שלא תעלה על 45 ימים.

(ב) לעניין פרק זה, יראו בחילוט העירבון לפי הוראות סעיף זה, כהטלת עיצום כספי על המפר בשל ההפרה שלגביה ניתן העירבון.

(ג) הופר תנאי מתנאי ההתחייבות כאמור בסעיף זה, והפר המפר פעם נוספת את ההוראה שבשל הפרתה נתן את כתב ההתחייבות, לא יאפשר לו ראש הרשות להגנת הפרטיות להגיש כתב התחייבות נוסף לפי הוראות סימן זה, בשל אותה הפרה.

סעיף 55: השבת העירבון

עמד המפר בתנאי כתב ההתחייבות שמסר לפי סימן זה, יוחזר לו, בתום תקופת ההתחייבות, העירבון שהפקיד; העירבון, למעט אם היה ערבות בנקאית, יוחזר בתוספת הפרשי הצמדה וריבית מיום הפקדתו עד יום החזרתו.

<u>סימן ד': הוראות כלליות</u>

סעיף 56: עיצום כספי בשל הפרה לפי חוק זה ולפי חוק אחר

על מעשה אחד המהווה הפרה של הוראה מהוראות לפי חוק זה המנויות בסעיף 38 ושל הוראה מההוראות לפי חוק אחר, לא יוטל יותר מעיצום כספי אחד.

דברי הסבר

<u>סעיף 52:</u> מבוסס על סעיפים 23לב ו-23לג להצ"ח תיקון מס' 13 ועל סעיפים 22טז ו-22יז לחוק הגנת הצרכן.

<u>סעיפים 53-56:</u> זהים לסעיפים 23לד-23לז בהצ"ח תיקון מס' 13 ולסעיפים 22יז-22יט ו-22כג לחוק הגנת הצרכן.

לא מצאנו לנכון לאמץ את הוראת סעיף 23לח להצ"ח תיקון מס' 13, העוסקת בעיכוב ביצוע ההחלטה של ראש הרשות להגנת הפרטיות לעניין הטלת עיצום כספי והחזר עיצום כספי ששולם או עירבון שהופקד במקרה של ערעור על החלטת ראש הרשות להגנת הפרטיות להפעיל את סמכותו המינהלית לפי פרק זה. כמו כן לא אימצנו הוראה דומה בסעיף 22כ לחוק הגנת הצרכן, העוסקת בערעור על החלטת הממונה להפעיל את סמכותו המינהלית. אנו סבורים כי הנושא צריך להיות מטופל במסגרת הדינים הכלליים, ובמקרה שלנו – בחוק בתי המשפט לעניינים מינהלים, התש"ס–2000. לדעתנו, אין צורך לתת בהצעת החוק מענה לסוגיות אלה.

סעיף 23לח להצ"ח תיקון מס' 13:

"(א) אין בהגשת עתירה לבית המשפט לעניינים מינהליים על החלטת הממונה לפי פרק זה, כדי לעכב את ביצוע ההחלטה, אלא אם כן הסכים לכך הממונה או שבית המשפט הורה על כך.

(ב) החליט בית המשפט לאחר ששולם העיצום הכספי או הופקד העירבון, לקבל עתירה כאמור בסעיף קטן (א), או ערעור על החלטה בעתירה כאמור, והורה על החזרת סכום העיצום הכספי ששולם או על הפחתת העיצום הכספי או החזרת העירבון, יוחזר הסכום ששולם או על חלק ממנו אשר הופחת או יוחזר העירבון,

לפי העניין; בתוספת הפרשי הצמדה וריבית מיום תשלומו או הפקדתו עד יום החזרתו."

סעיף 22כ לחוק הגנת הצרכן, התשמ"א–1981:

"(א) על דרישת תשלום ועל התראה מינהלית ניתן לערער לבית משפט השלום שבו יושב נשיא בית משפט השלום; ערעור כאמור יוגש בתוך 45 ימים מיום שנמסרה דרישת התשלום או מיום שנמסרה החלטת הממונה בבקשה לביטול ההתראה המינהלית.

(ב) אין בהגשת ערעור על דרישת תשלום כדי לעכב את תשלום העיצום הכספי אלא אם כן הסכים לכך הממונה או שבית המשפט הורה על כך.

(ג) החליט בית המשפט לקבל ערעור על דרישת תשלום והורה על החזרת סכום העיצום הכספי ששולם או על הפחתת סכום העיצום הכספי, לאחר ששולם העיצום הכספי לפי הוראות פרק זה, יוחזר סכום העיצום הכספי ששולם או כל חלק ממנו שהופחת, בתוספת הפרה הצמדה וריבית מיום תשלומו עד יום חזרתו."

סעיף 57: פרסום לעניין הטלת עיצום כספי

(א) הטיל ראש הרשות להגנת הפרטיות עיצום כספי לפי פרק זה, יפרסם באתר האינטרנט של הרשות להגנת הפרטיות את הפרטים שלהלן, באופן שיבטיח שקיפות לגבי הפעלת שיקול דעתו בקבלת ההחלטה להטיל עיצום כספי:

(1) דבר הטלת העיצום הכספי;

(2) מהות ההפרה שבשלה הוטל העיצום הכספי ונסיבות ההפרה, לרבות מספר נושאי המידע שמידע אישי על אודותיהם נחשף או עלול להיחשף עקב ההפרה;

(3) סכום העיצום הכספי שהוטל;

(4) אם הופחת העיצום הכספי – הנסיבות שבשלהן הופחת סכום העיצום ושיעורי ההפחתה;

(5) פרטים על אודות המפר, הנוגעים לעניין;

(6) שמו של המפר – ככל שהמפר הוא תאגיד.

(ב) הוגשה עתירה לבית המשפט לעניינים מינהליים או הוגש ערעור על החלטה בעתירה כאמור, יפרסם ראש הרשות להגנת הפרטיות, בפרסום לפי סעיף קטן (א), גם את דבר הגשת העתירה או הערעור ואת תוצאותיהם.

(ג) על אף הוראות סעיף קטן (א)(6), רשאי ראש הרשות להגנת הפרטיות לפרסם את שמו של מפר שהוא יחיד, אם סבר שהדבר נחוץ לצורך אזהרת הציבור.

(ד) פרסום לפי סעיף זה בעניין עיצום כספי שהוטל על תאגיד יהיה לתקופה של ארבע שנים, ובעניין עיצום כספי שהוטל על יחיד – לתקופה של שנתיים.

דברי הסבר

<u>סעיף 57:</u> מבוסס על סעיף 23לט להצ"ח תיקון מס' 13 ועל סעיף 22כא לחוק הגנת הצרכן. במקרים שלהלן אימצנו את המתווה שבחוק הגנת הצרכן:

בסעיף קטן (א) בחרנו לקבוע שהפרסום ייעשה באתר האינטרנט של הרשות להגנת הפרטיות ולא יפורסם באתר האינטרנט של משרד המשפטים או בדרך אחרת על פי ההחלטה של ראש הרשות להגנת הפרטיות.

סעיף 23לט(א) להצ"ח תיקון מס' 13:
"הטיל הממונה עיצום כספי לפי פרק זה, יפרסם באתר האינטרנט של משרד המשפטים את הפרטים שלהלן, בדרך שתבטיח שקיפות לגבי הפעלת שיקול דעתו בקבלת ההחלטה להטיל עיצום כספי:"

בסעיף קטן (א)(2) הוספנו הבהרה שעל ראש הרשות להגנת הפרטיות לציין גם את מספר נושאי המידע שנפגעו או עלולים להיפגע מההפרה כחלק מנסיבות ההפרה. לדעתנו, מספר נושאי המידע שמידע אישי עליהם נחשף או עלול להיחשף בעקבות ההפרה הוא מידע שרלוונטי לבחינת שיקול הדעת של ראש הרשות בהטלת העיצום הכספי.

בחרנו שלא לאמץ את הוראת סעיף 23לט(ו) להצ"ח תיקון מס' 13, שלשונה: "שר המשפטים רשאי לקבוע דרכים נוספות לפרסום הפרטים האמורים בסעיף"; ולא את הוראת סעיף 22כא(ו) לחוק הגנת הצרכן, שלשונו: "שר המשפטים, בהתייעצות עם השר ובאישור ועדת הכלכלה של הכנסת, יקבע הוראות

לעניין אופן הפרסום באינטרנט לפי סעיף זה, כדי למנוע, ככל הניתן, את העיון בפרטים שפורסמו לפי סעיף קטן (א) או (ג), בתום תקופת הפרסום כאמור בסעיף קטן (ה); לא הותקנו תקנות כאמור, יפרסם הממונה באינטרנט את הפרטים המנויים בסעיפים קטנים (א) או (ג), לפי העניין, באופן שימנע ככל הניתן את זיהויו של המפר." אנו סבורים כי יש בהוראה זו משום התערבות יתר ופגיעה בגמישות של סמכויות העזר הנתונות בידי השר האחראי או ראש הרשות להגנת הפרטיות. בחוק ההגבלים העסקיים ובחוק ניירות ערך, למשל, אין הוראה דומה בעניין דרכי פרסום נוספות של דבר הטלת עיצום כספי.

בסעיף קטן (ד) הגבלנו את פרסום דבר הטלת עיצום כספי לתקופה של 4 שנים כאשר העיצום הכספי מוטל על תאגיד, ולשנתיים כאשר העיצום הכספי מוטל על אדם יחיד. הגבלת תקופת הפרסום משמעה, בפועל, הטלת חובה על ראש הרשות להגנת הפרטיות למחוק את הפרסום מאתר האינטרנט שדבר הטלת העיצום פורסם בו.

סעיף 58: שמירת אחריות פלילית

(א) תשלום עיצום כספי, המצאת התראה מינהלית או מתן כתב התחייבות ועירבון, לפי פרק זה, לא יגרעו מאחריותו הפלילית של אדם בשל הפרת הוראה מההוראות לפי חוק זה המפורטות בסעיף 38, שהיא עבירה על חוק זה.

(ב) על אף האמור בסעיף קטן (א), נמסרה למפר הודעה על כוונת חיוב, או התראה מינהלית או הגיש המפר כתב התחייבות ועירבון, בשל הפרה כאמור באותו סעיף קטן, לא יוגש נגדו כתב אישום בשל אותו מעשה, אלא אם כן התגלו עובדות או ראיות חדשות, המצדיקות זאת.

(ג) שילם המפר עיצום כספי או הפקיד עירבון והוגש נגדו כתב אישום בנסיבות האמורות בסעיף קטן (ב), יוחזר לו הסכום ששילם או העירבון; הסכום ששילם המפר כאמור או עירבון, למעט ערבות בנקאית, יוחזר בתוספת הפרשי הצמדה וריבית מיום תשלומו או הפקדתו עד יום החזרתו.

(ד) הוגש נגד אדם כתב אישום בשל הפרה המהווה עבירה כאמור בסעיף קטן (א), לא ינקוט נגדו ראש הרשות להגנת הפרטיות הליכים לפי פרק זה בשל אותה הפרה.

סעיף 59: אישור נהלים ופרסומם

נהלי ראש הרשות להגנת הפרטיות לפי סעיפים 49 ו-52 טעונים אישור היועץ המשפטי לממשלה או משנה ליועץ המשפטי שהוא הסמיך לכך, והם יפורסמו באתר האינטרנט של הרשות להגנת הפרטיות.

סעיף 60: אצילת סמכויות

ראש הרשות להגנת הפרטיות רשאי לאצול את סמכויותיו לפי פרק זה, למעט קביעת נהלים לפי סעיפים 49(א) ו-52(א), לסגנו או לעובד הרשות להגנת הפרטיות האחראי לנושא העיצומים הכספיים.

דברי הסבר

<u>סעיף 58:</u> מבוסס על שילוב של הוראות סעיף 23מ להצ"ח תיקון מס' 13 וסעיף 22כב לחוק הגנת הצרכן. במקרים של אי-התאמה הועדף הנוסח הקבוע בחוק הגנת הצרכן בהנחה שהוא העדכני ביותר.

קבוצת המומחים עסקה בחשש מפני חוסר הוודאות שסעיף שמירת האחריות הפלילית עשוי ליצור. בחינת ההיסטוריה החקיקתית של סעיף שמירת האחריות הפלילית בחוק הגנת הצרכן ובחוק ההגבלים העסקיים מראה כי חשש זה התעורר גם שם.

בדיון בוועדת הכלכלה של הכנסת על ניסוח סעיף 22כב לחוק הגנת הצרכן ביקשו נציגי העוסקים להבחין בחוק במפורש בין העבירות שייאכפו רק מינהלית לבין העבירות שאכיפתן תהיה במישור הפלילי. הוצע גם להגביל את העבירות הפליליות רק לעבירות בנסיבות מחמירות. ההצעות נדחו בנימוק שקשה לרשות להגנת הצרכן לדעת מראש מהן העבירות שיהיה צריך להגיש בגינן כתב אישום במקום להסתפק באכיפה המינהלית. נימוק נוסף היה שפעמים רבות מפרים מעדיפים לשאת בקנס המינהלי מפני שהדבר משתלם להם כלכלית ושבלי השוט של האחריות פלילית, לא יושג שינוי בהתנהגות. הוחלט, על כן, להותיר את שיקול הדעת אם להגיש כתב אישום או לפעול במישור המינהלי בידי הממוּנֶה על הגנת הצרכן,

שהצהירה בדיון בוועדת הכלכלה של הכנסת כי ייקבעו נהלים פנימיים להפעלת שיקול הדעת.[59]

בחוק ההגבלים העסקיים לשון סעיף שמירת האחריות הפלילית מעט אחר:

"50טו. (א) תשלום עיצום כספי לא יגרע מאחריותו הפלילית של אדם בשל הפרת הוראה מההוראות לפי חוק זה, המנויות בסעיף 50ד, המהווה עבירה."

בדיון בוועדת הכלכלה על נוסח סעיף 50טו לחוק ההגבלים העסקיים נטען כי הסעיף יוצר סיכון כפול – המפר גם חשוף לאכיפה מינהלית וגם לא זוכה לסופיות הדיון משום שהוא עדיין חשוף לסנקציה פלילית. הטענה נדחתה והסעיף התקבל כלשונו. הנימוק לדחייה היה שלא מדובר בסיכון כפול מכיוון שכתב אישום יוגש רק אם יתגלו ראיות חדשות המצדיקות את הגשתו.[60] עם זאת, ההבהרה שכתב אישום יוגש רק אם יתגלו עובדות חדשות אינה מופיעה בחוק ההגבלים העסקיים.

בחוק ניירות ערך קובע סעיף 52כח כי "(א) תשלום עיצום כספי לפי הוראות פרק זה, לא יגרע מאחריותו הפלילית של אדם בשל הפרת הוראה לפי חוק זה."

סעיף 52סה לחוק ניירות ערך, התשכ"ח–1968 קובע גם:

52סה. (א) זומן המפר לבירור הפרה לפי סעיף 52מג(א)(2) או נמסרה לו הודעה על פתיחה בהליך מינהלי לפי סעיף 52מו, לא יוגש בשל המעשה המהווה את ההפרה כתב אישום נגד המפר, וכן לא יוטל על המפר בשל המעשה כאמור עיצום כספי לפי פרק ח'3.

(ב)הוזהר אדם בחשד לביצוע עבירת ניירות ערך, עבירה כהגדרתה בסעיף 29 לחוק הייעוץ ועבירה כהגדרתה בסעיף 97א לחוק להשקעות משותפות בנאמנות, לא ייפתח הליך מינהלי בשל המעשים נושא העבירה, אלא אם כן התקיים אחד מאלה:

(1) פרקליט מחוז החליט שלא להעמיד את החשוד לדין;

(2) החשוד הועמד לדין אך יושב ראש הרשות, בהתייעצות עם פרקליט מחוז, שוכנע, בהחלטה מנומקת בכתב, כי מתקיימות נסיבות מיוחדות לפתיחת הליך מינהלי בשל המעשים נושא העבירה או להסדר כאמור בסימן א' בפרק ט'1, ובלבד שאם נפתח הליך מינהלי בנסיבות כאמור, בהחלטת המותב או בהסדר כאמור בסימן א' בפרק ט'1, לא יהיה ניתן להטיל על המפר אלא אמצעי אכיפה כאמור בסעיפים 52נו או 52נז."

בדברי ההסבר לסעיף צוין שהזמנה של מפר לתשאול במסגרת בירור הפרה מן ההפרות של אכיפה מינהלית מונעת הגשת כתב אישום נגדו בשל המעשה או המחדל המהווה הפרה אלא אם יתגלו ראיות להפרות אחרות או חדשות.[61]

מעיון במקורות אלו ובהיסטוריה החקיקתית שלהם עולה לדעתנו הצורך להשאיר את סעיף שמירת הדינים בנוסח המוצע. עם זה כדי ליצור את הוודאות הנדרשת מוצע לקבוע בנהלים קריטריונים ברורים לקבלת ההחלטה אם להחיל אכיפה פלילית או אכיפה מינהלית.

<u>סעיף 59</u>: מבוסס על סעיף 22כד לחוק הגנת הצרכן. מטרתו ליצור סעיף סל לאישור הנהלים שקובע ראש הרשות להגנת הפרטיות. הסעיף הוא חלופה לאזכור החובה לקבל מן היועץ המשפטי לממשלה אישור לנהלים שקובע ראש הרשות בכל סעיף חוק רלוונטי, כפי שנעשה בהצ"ח תיקון מס' 13 בסעיפים 23כט(א) ו-23לב.

<u>סעיף 60</u>: מבוסס על סעיף 22כה לחוק הגנת הצרכן, ואין לו מקבילה בהצ"ח תיקון מס' 13. בחרנו לאמצו על בסיס ההנחה שחוק הגנת הצרכן משקף את המתווה המעודכן ביותר בחוק לעניין סמכויות האכיפה המינהליות.

פרק ה: מסירת מידע אישי או ידיעות מאת גופים ציבוריים

הנושא מצריך מחקר נפרד, שאינו בליבת עבודתנו הנוכחית לגיבוש הצעה לחוק הגנת פרטיות חדש ומעודכן.

פרק ו: עוולה אזרחית ועונשין

סעיף 61: פגיעה בפרטיות – עוולה אזרחית

הפרת הוראה מההוראות לפי סעיפים 4, 9, 11, 13 עד 15, או הוראה שנקבעה לפי סעיף 16 לעניין האופן והתנאים למימוש זכות לפי סעיפים 11, 13, 14 או 15, היא עוולה אזרחית והוראות פקודת הנזיקין [נוסח חדש][62] יחולו עליה בכפוף להוראות חוק זה.

סעיף 62: פגיעה בפרטיות – עבירה

הפוגע בפרטיות זולתו באחת מהדרכים האמורות בסעיף 4, דינו – מאסר 5 שנים; נעברה העבירה או היתה מכוונת כלפי קשישים, חסרי ישע או קטינים, או כלפי ציבור של נושאי מידע הנתונים במצב של חולשה שכלית, נפשית או גופנית– דינו של עובר העבירה מאסר שבע שנים.

דברי הסבר

<u>סעיף 61:</u> הסעיף מבוסס על סעיף 4 לחוק הגנת הפרטיות הקיים, הקובע כי "פגיעה בפרטיות היא עוולה אזרחית, והוראות פקודת הנזיקין [נוסח חדש], יחולו עליה בכפוף להוראות חוק זה." עם זאת, בחרנו לקבוע שלא רק פגיעה בפרטיות לפי סעיף 4 היא עוולה אזרחית, אלא גם פגיעה בזכויות נושא המידע, ולכן בחרנו לפרט את הסעיפים שהפרתם תיחשב עוולה נזיקית. מטרתנו להקל בנטל המוטל על נושא המידע בבואו לתבוע פיצוי נזיקי בגין פגיעה בזכותו לפרטיות על פי חוק זה.

לא מצאנו לנכון לחזור גם על הוראת סעיף 31ב לחוק הגנת הפרטיות הקיים, שכן זו נראית לנו חזרה מיותרת.

סעיף 31ב לחוק הגנת הפרטיות הקיים קובע:

"מעשה או מחדל בניגוד להוראות פרקים ב' או ד' או לתקנות שהותקנו לפי חוק זה יהווה עוולה לפי פקודת הנזיקין [נוסח חדש]."

<u>סעיף 62:</u> מבוסס על סעיף 5 לחוק הגנת הפרטיות הקיים, המונה רק חלק מסעיפי הפגיעה בפרטיות הנמצאים בסעיף 2 לחוק הגנת הפרטיות הקיים. הסעיף המוצע על ידינו אינו מחריג שום פגיעה בפרטיות המפורטת בסעיף 4 להצעת החוק, מפני שכאשר הגדרנו מהי פגיעה בפרטיות עשינו זאת בדיוק גדול יותר מן המפורט בחוק הגנת הפרטיות הקיים. לכן, לתפיסתנו, כל פגיעה שהוגדרה פגיעה בפרטיות לפי סעיף 4 צריכה להוביל לעונש מאסר. בנוסף, הסעיף כולל התייחסות לפגיעה בפרטיות של אוכלוסיות חלשות כגון קטינים, קשישים וחסרי ישע. מצאנו לנכון להרחיב את ההתייחסות לקשישים ולחסרי ישע ולא רק לקטינים כמוצע בהצ"ח פרטיות קטינים, על בסיס ההבנה שאוכלוסיות חלשות אלו עלולות להיתקל בקשיים בשימוש בשירותים מקוונים. באימוץ התייחסות שונה לאוכלוסיות חלשות אלו שאבנו השראה מסעיף 23א לחוק הגנת הצרכן, המונה נסיבות מחמירות שגוררות החמרת הענישה הפלילית. לא אימצנו את כלל הנסיבות המחמירות המנויות בסעיף מאחר שרף הענישה הפלילית הקבוע בחוק הגנת הפרטיות מחמיר יותר מזה הקבוע בחוק הגנת הצרכן. אנו גורסים כי שקלול הנסיבות האחרות המנויות בחוק הגנת הצרכן צריך להיוותר לשיקול דעתו של בית המשפט.

סעיף 5 לחוק הגנת הפרטיות הקיים הקובע:

"הפוגע במזיד בפרטיות זולתו, באחת הדרכים אמורות בסעיף 2(1), (3) עד (7) ו-(9) עד (11), דינו - מאסר 5 שנים."

סעיף 23א לחוק הגנת הצרכן, התשמ"א-1981:

"(א) נעברה עבירה לפי סעיף 23(א)(1) או (2) בנסיבות מחמירות – דינו של עובר העבירה מאסר שלוש שנים או קנס פי עשרים מהקנס כאמור בסעיף 61(א)(4) לחוק העונשין.

(ב) בסעיף זה, "נסיבות מחמירות" – אחת מאלה:

(1) המעשה מתייחס למספר רב במיוחד של צרכנים;

(2) המעשה גרם נזק חמור במיוחד לצרכן או לקבוצת צרכנים;

(3) עובר העבירה הפיק רווחים, או טובות הנאה גדולים במיוחד מהמעשה;

(4) העבירה נעברה או היתה מכוונת כלפי קשישים, חסרי ישע או קטינים, או כלפי ציבור של צרכנים הנתונים במצב של חולשה שכלית, נפשית או גופנית, או כלפי מי שאינם יודעים את השפה שבה נקשרה העסקה במידה מספקת לשם הבנת העסקה;

(5) נעברה עבירה לפי סעיף 23(א)(1) תוך טענת עובדה אשר הטוען אותה יודע שאינה אמת או שאינו מאמין שהיא אמת."

לא אימצנו את הוראת סעיפים 23מא-23מה להצ"ח תיקון 13 מאחר שלדעתנו הן רחבות מדי, מקצתן מכוסות גם כך בהוראת סעיף 62, ומקצתן נוגעות להוראות בדין המהותי שבחרנו להשמיט מהצעת החוק, כמו למשל החובה לרישום מאגר מידע.

סעיף 23מא להצ"ח תיקון מס' 13:

"23מא. המפריע לממונה, או לחוקר או למפקח מטעמו, במילוי תפקידו לפי חוק זה, דינו – מאסר שישה חודשים."

סעיף 23מב להצ"ח תיקון מס' 13:

"23מב. העושה אחד מאלה בכוונה להטעות את הממונה או מפקח מטעמו, דינו מאסר שלוש שנים:

(1) כלל פרטים לא נכונים בבקשה לרישום מאגר מידע שהוגשה לפי סעיף 9;

(2) לא הודיע לממונה על שינוי בפרטים המנויים בסעיף 9(ב) או בפרטים שנקבעו לפי סעיף 9(ג), בניגוד להוראת סעיף 9(ד);

(3) מסר פרטים לא נכונים במענה לדרישה של הממונה או של מפקח לפי סעיף 23י(א)(1) עד (3)".

סעיף 23מג להצ"ח תיקון מס' 13:

"23מג. הפונה לאדם לשם קבלת מידע לשם החזקתו או שימוש בו במאגר מידע, בלי שמסר לו הודעה כנדרש בסעיף 11, בכוונה לקבל את המידע במרמה, דינו – מאסר שלוש שנים; לענין סעיף זה, "מרמה" – טענת עובדה בעניין שבעבר, בהווה או בעתיד, הנטענת בכתב, בעל פה או בהתנהגות, ואשר הטוען אותה יודע שאינה אמת או שאינו מאמין שהיא אמת."

סעיף 23מד להצ"ח תיקון מס' 13:

"23מד. בעל מאגר מידע או מחזיק בו, המשתמש במידע ממאגר המידע שלא למטרה שלשמה נמסר, או המתיר זאת לאחר, דינו כדין הפוגע במזיד בפרטיות זולתו לפי סעיף 5."

סעיף 23מה להצ"ח תיקון מס' 13:

"23מה. (א) לא ישתמש אדם במידע ממאגר מידע בלא הרשאה של בעל מאגר המידע, או בחריגה מהרשאה כאמור; לעניין זה, מי שברשותו עותק של מאגר המידע, או חלק מהותי ממנו - יראו אותו כמי שמשתמש במידע ממאגר המידע, אלא אם כן הוכיח אחרת.

(ב) המשתמש במידע ממאגר המידע בלא הרשאה או בחריגה מהרשאה, כאמור בסעיף קטן (א) – דינו מאסר שלוש שנים."

לא אימצנו את הוראת סעיף 16 לחוק הגנת הפרטיות הקיים מאחר שלדעתנו היא מיותרת, שהרי הפרת חובת הסודיות נחשבת עבירה לפי סעיף 62 המוצע.

סעיף 16 לחוק הגנת הפרטיות הקיים:
"לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך ביצוע עבודתו או לביצוע חוק זה או על פי צו בית משפט בקשר להליך משפטי; אם הוגשה הבקשה לפני תחילת ההליך תידון הבקשה בבית משפט השלום. המפר הוראות סעיף זה, דינו - מאסר 5 שנים."

לא אימצנו את הוראת סעיף 6 לחוק הגנת הפרטיות הקיים הקובעת כי "לא תהיה זכות לתביעה אזרחית או פלילית לפי חוק זה בשל פגיעה שאין בה ממש", שכן לדעתנו הנושא מוסדר לפי העקרונות הכלליים בדיני הנזיקין ובדיני העונשין ואין צורך לחזור על כך בהצעת החוק.

לא אימצנו את סעיף 31א בחוק הגנת הפרטיות הקיים המגדיר מהן עבירות אחריות קפידה. לדעתנו הותרת הוראה בעניין אחריות קפידה מגבירה את הסיכון הכפול שבשמירת האחריות הפלילית לפי סעיף 58. כמו כן אין הוראה דומה בדברי חקיקה אחרים, ששילבו הוראות לאכיפה מינהלית, כמו למשל התיקון משנת 2012 לחוק ההגבלים העסקיים[63] והתיקון משנת 2014 לחוק הגנת הצרכן.[64]

סעיף 31א לחוק הגנת הפרטיות הקיים:
"31א. (א) העושה אחד מאלה, דינו - מאסר שנה: (1) מנהל, מחזיק או משתמש במאגר מידע בניגוד להוראות סעיף 8; (2) מוסר פרטים לא נכונים בבקשה לרישום אגר מידע כנדרש בסעיף 9; (3) אינו מוסר פרטים או מוסר פרטים לא נכונים בהודעה המלווה בקשה לקבלת מידע לפי סעיף 11; (4) אינו מקיים את הוראות סעיפים 13 ו-13א לענין זכות העיון במידע המוחזק במאגר מידע, או אינו מתקן מידע על פי הוראות סעיף 14; (5) מאפשר גישה למאגר מידע בניגוד להוראות סעיף 17א(א) או אינו מוסר לרשם מסמכים או תצהיר בהתאם להוראות סעיף 17א(ב); (6) אינו ממנה ממונה על אבטחת מידע בהתאם להוראות סעיף 17ב; (7) מנהל או מחזיק מאגר המשמש לשירותי דיוור ישיר, בניגוד להוראות סעיפים 17ד עד 17ו; (8) מוסר מידע בניגוד לסעיפים 23ב עד 23ה. (ב) עבירה לפי סעיף זה אינה טעונה הוכחת מחשבה פלילית או רשלנות."

סעיף 63: פיצוי בלא הוכחת נזק

(א) הורשע אדם בעבירה לפי סעיף 62 רשאי בית המשפט לחייבו לשלם לנפגע פיצוי שלא יעלה על 50,000 שקלים חדשים, בלא הוכחת נזק; הורשע אדם בעבירה לפי סעיף 62 לעניין קטין, קשיש, חסר ישע או ציבור של נושאי מידע הנתונים במצב של חולשה שכלית, נפשית או גופנית, רשאי בית המשפט לחייב את הפוגע לשלם לנפגע פיצוי שלא יעלה על כפל הסכום האמור, בלא הוכחת נזק. חיוב בפיצוי לפי סעיף קטן זה הוא כפסק דין של אותו בית משפט שניתן בתובענה אזרחית של הזכאי נגד החייב בו.

(ב)

(1) במשפט בשל עוולה אזרחית לפי סעיף 61 עקב הפרת הוראת סעיף 4(8), רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על 50,000 שקלים חדשים, בלא הוכחת נזק.

(2) במשפט כאמור בפסקה (1) שבו הוכח כי הפגיעה בפרטיות נעשתה בכוונה לפגוע, רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על כפל הסכום כאמור באותה פסקה, בלא הוכחת נזק.

(3) במשפט כאמור בפסקה (1) שבו הוכח כי הפגיעה בפרטיות נעשתה או היתה מכוונת כלפי קשישים, חסרי ישע או קטינים, או כלפי ציבור של נושאי מידע הנתונים במצב של חולשה שכלית, נפשית או גופנית, רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על כפל הסכום כאמור באותה פסקה, בלא הוכחת נזק.

(ג) לא יקבל אדם פיצוי בלא הוכחת נזק לפי סעיף זה, בשל אותה פגיעה בפרטיות, יותר מפעם אחת.

סעיף 64: שיקולים בגזירת הדין או גובה הפיצוי

בבואו לגזור את הדין או לפסוק פיצויים רשאי בית המשפט להתחשב, לטובת הנאשם, הנתבע או הצד להליך מינהלי, גם באלה:

(1) חומרת הפגיעה בפרטיות;

(2) היקף הפגיעה בפרטיות;

(3) משך הזמן שבו בוצעה הפגיעה בפרטיות;

(4) הנזק הממשי שנגרם לנפגע בעבירה או לתובע, לפי העניין, להערכת בית המשפט;

(5) הרווח שצמח לנאשם או לנתבע, לפי העניין, בשל הפגיעה בפרטיות, להערכת בית המשפט;

(6) מאפייני הפעילות של הנאשם או הנתבע, לפי העניין;

(7) טיב היחסים בין הנפגע בעבירה לבין הנאשם, או הנתבע לתובע, לפי העניין;

(8) תום ליבו של הנאשם או הנתבע;

(9) טיב תהליך עיצוב לפרטיות שהתבצע לפי סעיף 19.

דברי הסבר

סעיף 63: מבוסס על סעיף 29א בחוק הגנת הפרטיות הקיים בשילוב התיקונים המוצעים בנוגע להחמרת הענישה כאשר הפגיעה היא בפרטיותם של נושאי מידע מאוכלוסיות חלשות. סעיף קטן (ב) אף מגביל את מתן הפיצויים ללא הוכחת נזק בשל עוולה אזרחית רק להפרת הוראת סעיף 4(8) הנוגעת לעיבוד מידע על פי הוראות הצעת חוק זו – כל זה כדי להגביר את ההרתעה מפני עיבוד מידע אישי בניגוד להוראת הצעת חוק זו.

סעיף 64: בא במקום סעיף 22 לחוק הגנת הפרטיות הקיים, שלדעתנו לא מציג מכניזם ברור דיו לבית המשפט בקובעו את סכום הפיצוי בגין פגיעה בפרטיות. לפיכך אימצנו, כחלופה לסעיף 22 לחוק הגנת הפרטיות הקיים, את המנגנון הקבוע בסעיף 56(ב) לחוק זכויות יוצרים, התשס"ח–2007, בשינויים המחויבים לנוכח העובדה שמדובר בפגיעה בזכות לפרטיות ולא בהפרת זכות יוצרים.

סעיף 22 לחוק הגנת הפרטיות הקיים:

"בבואו לגזור את הדין או לפסוק פיצויים רשאי בית המשפט להתחשב, לטובת הנאשם או הנתבע, גם באלה:

(1) הפגיעה בפרטיות לא היתה אלא חזרה על מה שכבר נאמר, והוא נקב את המקור שעליו הסתמך;

(2) הוא לא התכוון לפגוע;

(3) אם היתה הפגיעה בדרך של פרסום – הוא התנצל על הפרסום ונקט צעדים להפסקת מכירתו או הפצתו של עותק הפרסום המכיל את הפגיעה, ובלבד שההתנצלות פורסמה במקום, במידה ובדרך שבהם פורסמה הפגיעה ולא היתה מסוייגת."

סעיף 56(ב) לחוק זכות יוצרים, התשס"ח-2007:

"... (ב) בקביעת פיצויים לפי הוראות סעיף קטן (א), רשאי בית המשפט לשקול, בין השאר, שיקולים אלה:

(1) היקף ההפרה;

(2) משך הזמן שבו בוצעה ההפרה;

(3) חומרת ההפרה;

(4) הנזק הממשי שנגרם לתובע, להערכת בית המשפט;

(5) הרווח שצמח לנתבע בשל ההפרה, להערכת בית המשפט;

(6) מאפייני פעילותו של הנתבע;

(7) טיב היחסים שבין הנתבע לתובע;

(8) תום לבו של הנתבע."

פרק ז: הגנות

סעיף 65: הגנות מה הן

(א) בכל הליך משפטי או משמעתי לפי חוק זה, תהא זו הגנה טובה אם נתקיימה אחת מאלה:

(1) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי סעיף 13 לחוק איסור לשון הרע, התשכ"ה-1965[65] (בסעיף זה – חוק איסור לשון הרע);

(2) עיבוד של המידע האישי נדרש לשם מילוי חובה על פי דין המוטלת על בעל השליטה במידע או המעבד;

(3) הנתבע, הנאשם או צד להליך מינהלי עשה את הפגיעה בתום לב באחת הנסיבות האלה –

(א) הוא לא ידע ולא היה עליו לדעת על אפשרות הפגיעה בפרטיות;

(ב) הפגיעה נעשתה בנסיבות שבהן היתה מוטלת על הפוגע חובה חוקית או מקצועית לעשותה; לענין פסקה זו, "חובה מקצועית" – חובה לפי עקרונות או כללים של אתיקה מקצועית, החלים עליו מכוח דין או המקובלים על אנשי המקצוע שהוא נמנה עמהם;

(ג) הפגיעה נעשתה לשם הגנה על עניין אישי כשר של הפוגע;

(ד) הפגיעה נעשתה תוך ביצוע עיסוקו של הפוגע כדין ובמהלך עבודתו הרגיל, ובלבד שלא נעשתה דרך פרסום ברבים;

(ה) הפגיעה היתה בדרך של צילום או בדרך של פרסום של תצלום או של תוצר של תיעוד על אודות אדם, שנעשה ברשות הרבים ודמות הנפגע מופיעה בו באקראי;

(ו) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי פסקאות (4) עד (11) לסעיף 15 לחוק איסור לשון הרע;

(ז) הפגיעה היתה נחוצה כדי להגן על חייו, חירותו, בריאותו או שלמות גופו של הנפגע או של אדם אחר;

(4) בפגיעה היה עניין ציבורי המצדיק אותה בנסיבות העניין, ובלבד שאם היתה הפגיעה בדרך של פרסום – הפרסום לא היה כוזב;

(5) הנפגע הוא קשיש, חסר ישע או קטין או שהיה קטין בעת הפגיעה בפרטיותו, והפגיעה נעשתה על ידי הורהו או אפוטרופס שנתמנה לו כדין, לשם הגנה על עניין אישי כשר שלו.

(ב) חזקה על הנאשם, הנתבע או צד להליך מינהלי שעשה את הפגיעה בפרטיות שלא בתום לב אם התקיים אחד מאלה:

(1) הוא פגע ביודעין במידה העולה על הנדרש לצורך עניין מהעניינים שניתנה עליהם הגנה;

(2) נושא המידע שנפגע דרש ממנו לתקן את המידע האישי על אודותיו לפי סעיף 13 והוא סירב שלא כדין לעשות כן.

דברי הסבר

סעיף 65: סעיף קטן (א) המוצע מבוסס על סעיף 18 לחוק הגנת הפרטיות הקיים. ואולם ההגנות אינן מוגבלות, כקבוע בסעיף 18 לחוק הגנת הפרטיות הקיים, ל"משפט פלילי או אזרחי". הסיבה העיקרית לכך היא השאיפה הקיימת כבר היום להרחיב את אפיק האכיפה המינהלית, כפי שעולה מהצ"ח תיקון מס' 13.

סעיף קטן (א)(1) זהה לסעיף 18(1) לחוק הגנת הפרטיות הקיים.

סעיף קטן (א)(2) מבוסס על סעיף 6(1)(c) ל-GDPR. אף שב-GDPR הסעיף מופיע תחת רשימת הבסיסים הלגיטימיים לעיבוד מידע אישי, אנו מציעים לקבוע זאת כהגנה בהצעת החוק כדי שלא להטיל על נושא המידע את הנטל שבהוכחת תנאיו של ס"ק (א)(2).

סעיף 6(1)(c) ל-GDPR:

"Article 6 Lawfulness of processing
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;"

סעיף קטן (א)(3)(א) זהה לסעיף 18(2)(א) לחוק הגנת הפרטיות הקיים, אבל מאחר שהרחבנו את ההגנות לכל הליך משפטי או משמעתי, בחרנו שלא להתייחס רק ל"נתבע או נאשם" אלא גם לצד בהליך המינהלי.

סעיף קטן (א)(3)(ב) מבוסס על סעיף 18(2)(ב) לחוק הגנת הפרטיות הקיים. במשך השנים פורַש סעיף 18(2)(ב) בפסיקה כמספק הגנה בהתקיים אחת מן החובות המאוזכרות בסעיף: חוקית, חברתית, מוסרית או מקצועית.[66] ברם משמעותן והיקפן של החובה החברתית או המוסרית נותרה פתוחה. לעניין החובה החוקית נפסק כי היא כוללת גם את חובת הזהירות הנזיקית;[67] לעניין החובה המקצועית נפסק כי על רופא מוטלת חובה מקצועית להציל את חייו של מטופל גם במחיר של פגיעה בפרטיותו של המטופל (ניתוח בניגוד לרצון המטופל לשם הוצאת סמים מגופו שכן אלו סיכנו את חייו). הוסבר כי לפי דברי הכנסת, המונָחים "חובה חוקית", "חובה מוסרית", "חובה חברתית" ו"חובה מקצועית" נועדו להעניק לעיתונות ולאמצעי התקשורת האחרים הגנה מיוחדת. בדיונים שקדמו לחקיקת הסעיף הוחלט לכתוב במקום "או במילוי חובה עיתונאית" את המילים "חוקית, מוסרית, חברתית ומקצועית" – כדי ליצור מערך חובות ברורות וכדי שלא להכשיל עיתונאי בעת מילוי תפקידו.[68] בהמשך אף נפסק כי על עיתונאים מוטלת החובה לפרסם ידיעות שיש בהן כדי לחשוף פעולות לא כשרות של רשויות וגופים וכי חובה זו נכנסת לגדר חובה מוסרית או חברתית.[69] עוד נפסק כי חובה "מקצועית" היא בעלת אופי כללי ויש ליצוק לתוכה תוכן לפי הנסיבות והאינטרס המוגן. וכך, במקרה של פגיעה בפרטיות מידי חוקרים פרטיים אין די בהתמקדות בחובת האמון בין חוקר ללקוח שלו, ולא כל פעולה של החוקר תיהנה מהגנה. יש לבחון באילו נסיבות חוקר פולש לרשות הפרט, מצלם את יושבי הבית וממלא את חובתו המקצועית על פי החוק ולכן זכאי להגנה.[70]

על מנת להימנע מפסיקות מרחיבות המתירות פגיעה בפרטיות לפי הנסיבות תחת הכסות של חובה מוסרית, חברתית או מקצועית ראינו לנכון לחדד את גבולות ההגנה ולצמצם את ההגנה למקרים של חובה חוקית או מקצועית המבוססת על כללים מוגדרים שנדונו בחקיקה או אומצו על ידי אנשי מקצוע רבים מאותו התחום. משום כך השמטנו את ההגנה של "חובה מוסרית" ו"חובה חברתית" והוספנו קביעה בהירה בנוגע להיקפה של החובה המקצועית לפרסם.

מדובר בחובה מכוח כללי האתיקה המקצועית החלים מכוח דין או המקובלים על אנשי המקצוע מאותו התחום.

סעיף קטן (א)(3)(ג) זהה לסעיף 18(2)(ג) לחוק הגנת הפרטיות הקיים.

סעיף קטן (א)(3)(ד) מבוסס על סעיף 18(2)(ד) בחוק הגנת הפרטיות הקיים.

סעיף קטן (א)(3)(ה) מבוסס על סעיף 18(2)(ה) בחוק הגנת הפרטיות הקיים, ואולם לפעולת ה"צילום" הוספה פעולת "תיעוד", שהגדרתה: "קליטה או שימור של מידע אישי באמצעות אמצעי טכנולוגי". המטרה הייתה להרחיב את ההגנה שניתנת בחוק הגנת הפרטיות הקיים רק לצילום ברשות הרבים שדמותו של הנפגע מופיעה בו באקראי גם לקליטה אקראית של מידע אישי על הנפגע באמצעות חיישנים המוצבים במרחב הציבורי. דוגמה: עיבוד בחיישני קול ומפות חום במרחב הציבורי לצורכי מעקב ומניעת פשיעה. בדרך זו מותאמות ההגנות גם לשינויים שהצענו בסעיף 4 לעניין פגיעה בפרטיות.

סעיף קטן (א)(3)(ו) זהה לסעיף 18(2)(ו) לחוק הגנת הפרטיות הקיים.

סעיף קטן (א)(3)(ז) הוסף כדי לאפשר מצבים שבהם הפגיעה בפרטיות נעשית למטרות הגנה על חייו, חירותו, בריאותו ושלמות גופו של נושא המידע עצמו או של אדם אחר. ההשראה לסעיף באה מסעיפים 6(1)(d), 9(2)(c) ו-9(2)(i) ל-GDPR. בחרנו להגדיר את "האינטרס המהותי" של נושא המידע או של צדדים שלישיים ואת האינטרס של הציבור בתחום הבריאות בהגדרה מצומצמת כהגנה על החיים, החירות, הבריאות או שלמות הגוף. יתרה מזו, בשעה שב-GDPR הסעיפים מופיעים ברשימת העיבודים המותרים במידע אישי ובמידע רגיש (בהתאמה), אנחנו בחרנו לכלול את הוראותיהם תחת ההגנות. הנימוק לבחירתנו: הימנעות מהטלת נטל הוכחה כבד מדי על הנפגע. הכללת הסעיף בהגנות מבטיחה כי הפוגע – בעל השליטה במידע או המעבד – הם שיישאו בנטל ההוכחה.

סעיף קטן (א)(4) זהה לסעיף 18(3) לחוק הגנת הפרטיות הקיים.

סעיף קטן (א)(5) מבוסס על החמרת הענישה כאשר העבירה או הפגיעה היא בנושאי מידע מאוכלוסיות חלשות, כמוצע בסעיף 62 להצעת החוק ו**בסעיף 1א להצ"ח פרטיות קטינים**, הקובע:

"1א. (1) כל קטין זכאי לפרטיות ולהגנה על פרטיותו.
אין פוגעים בפרטיותו של קטין אלא בהתאם להוראות הדין. פגיעה בפרטיותו של קטין על ידי הורהו או אפוטרופסו מותרת רק אם הדבר נעשה לטובתו של הקטין ולשם הגנה על אינטרס כשר שלו."

סעיף 18 לחוק הגנת הפרטיות הקיים קובע:

"במשפט פלילי או אזרחי בשל פגיעה בפרטיות תהא זו הגנה טובה אם נתקיימה אחת מאלה:
(1) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי סעיף 13 לחוק איסור לשון הרע, תשכ"ה–1965;
(2) הנתבע או הנאשם עשה את הפגיעה בתום לב באחת הנסיבות האלה:
(א) הוא לא ידע ולא היה עליו לדעת על אפשרות הפגיעה בפרטיות;
(ב) הפגיעה נעשתה בנסיבות שבהן היתה מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה;
(ג) הפגיעה נעשתה לשם הגנה על ענין אישי כשר של הפוגע;
(ד) הפגיעה נעשתה תוך ביצוע עיסוקו של הפוגע כדין ובמהלך עבודתו הרגיל, ובלבד שלא נעשתה דרך פרסום ברבים;
(ה) הפגיעה היתה בדרך של צילום, או בדרך של פרסום תצלום, שנעשה ברשות הרבים ודמות הנפגע מופיעה בו באקראי;
(ו) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי פסקאות (4) עד (11) לסעיף 15 לחוק איסור לשון הרע, תשכ"ה–1965;
(3) בפגיעה היה ענין ציבורי המצדיק אותה בנסיבות הענין, ובלבד שאם היתה

הפגיעה בדרך של פרסום – הפרסום לא היה כוזב."

סעיף קטן (ב) מעגן את חזקת תום הלב הקבועה בסעיף 20 לחוק הגנת הפרטיות הקיים. הכללת החזקה בסעיף ההגנות נועדה להצביע על שיש לפרשה בצמצום ובהקשר של ההגנות המפורטות בסעיף קטן (א).

סעיף קטן (ב)(1) מבוסס על סעיף 20(ב) לחוק הגנת הפרטיות הקיים.

סעיף 20(ב) לחוק הגנת הפרטיות הקיים קובע:

"חזקה על הנאשם או הנתבע שעשה את הפגיעה בפרטיות שלא בתום לב אם הוא פגע ביודעין במידה גדולה משהיתה נחוצה באופן סביר לצורך הענינים שניתנה להם הגנה בסעיף 18(2)."

סעיף קטן (ב)(2) מבוסס על סעיף 17(א) לחוק איסור לשון הרע, התשכ"ה–1965, העוסק בשלילת הגנת תום הלב. מטרת הסעיף המוצע היא לתת בידי נושא המידע כלי נוסף שיבטיח שבקשתו לתיקון מידע אישי עליו לפי סעיף 13 תישקל באופן מלא וראוי.

סעיף 17(א) לחוק איסור לשון הרע, התשכ"ה–1965:

"פורסמה לשון הרע באמצעי תקשורת לא תעמוד הגנת תום לב לעורכו, למי שהחליט בפועל על הפרסום או לאחראי על אותו אמצעי תקשורת אם הנפגע, או אחד הנפגעים, דרש ממנו לפרסם תיקון או הכחשה מצב הנפגע ולא פרסם את התיקון או ההכחשה בכותרת מתאימה במקום, במידה, בהבלטה ובדרך שבה פורסמה אותה לשון הרע, ותוך זמן סביר מקבלת הדרישה ובלבד שהדרישה היתה חתומה בידי הנפגע, שהתיקון או ההכחשה לא היה בהם משום לשון הרע או תוכן בלתי חוקי אחר וארכם לא חרג מתחום הסביר בנסיבות."

סעיף 66: פטור
לא יישא אדם באחריות לפי חוק זה על מעשה שהוסמך לעשותו על פי דין.

סעיף 67: הפרכה של טענות הגנה
הביא הנאשם, הנתבע או הצד להליך מינהלי ראיה, או העיד בעצמו כדי להוכיח את אחת ההגנות הניתנות בחוק זה, רשאי התובע או הצד שכנגד להביא ראיות סותרות; אין בהוראה זו כדי לגרוע מסמכות בית המשפט לפי כל דין להתיר הבאת ראיות בידי בעלי הדין.

דברי הסבר

סעיף 66: מבוסס על סעיף 19(א) לחוק הגנת הפרטיות הקיים.

מוצע למחוק את הפטור הניתן לרשות ביטחון בסעיף 19(ב) לחוק הגנת הפרטיות הקיים. לנוכח השימוש הגובר בטכנולוגיות למטרות מעקב ומלחמה בפשיעה, גוברת הסכנה לפגיעה חמורה ובהיקף נרחב בזכות לפרטיות על ידי גורמי ביטחון ואכיפת חוק. לפיכך אין לדעתנו להסתפק בסעיף המתיר פגיעה בפרטיות על ידי רשות ביטחון על פי המבחן המוצע בסעיף 19(ב) לחוק הגנת הפרטיות הקיים – מבחן סבירות כל עוד הפגיעה נעשית במסגרת התפקיד ולשם מילויו. זאת ועוד, מאז חקיקת ס' 19(ב) בשנת 1981 התרחשה המהפכה החוקתית והזכות לפרטיות עוגנה כאחת מזכויות היסוד החוקתיות בחוק-יסוד: כבוד האדם וחירותו. אנו סבורים אפוא כי אין להתיר פגיעה בחוק בזכות לפרטיות באופן שאינו עומד בדרישות של פסקת ההגבלה. זאת ועוד, הענקת סמכות מעקב ופגיעה גורפת בפרטיות לרשויות ביטחון עלולה להיות אבן נגף בפני הכרה אירופית (adequacy) שרמת הגנת הפרטיות בדין הישראלי תואמת את זו האירופית.[71] יש צורך לדעתנו לקבוע הסמכה מפורשת ומידתית בחוק ייעודי שתעסוק בשימוש בטכנולוגיות לשם מעקב ומניעת פשיעה.

סעיף 19 לחוק הגנת הפרטיות הקיים:
"(א) לא ישא אדם באחריות לפי חוק זה על מעשה שהוסמך לעשותו על פי דין.
(ב) רשות בטחון, או מי שנמנה עם עובדיה או פועל מטעמה, לא ישאו באחריות לפי חוק זה על פגיעה שנעשתה באופן סביר במסגרת תפקידם ולשם מילויו.
(ג) "רשות בטחון", לענין סעיף זה – כל אחד מאלה:
(1) משטרת ישראל;
(2) אגף המודיעין במטה הכללי והמשטרה הצבאית של צבא-הגנה לישראל;
(3) שירות בטחון כללי;
(4) המוסד למודיעין ולתפקידים מיוחדים;
(5) הרשות להגנה על עדים."

סעיף 67: זהה לסעיף 21 בחוק הגנת הפרטיות הקיים, אם כי לנוכח הרחבת ההגנות לכל הליך משפטי או משמעתי הוספנו גם את המילים "צד להליך מינהלי".

פרק ח: הוראות שונות

סעיף 68: דין המדינה

חוק זה חל על המדינה.

סעיף 69: מות הנפגע

(א) אדם שנפגע בפרטיותו ותוך שישה חודשים לאחר הפגיעה מת בלי שהגיש תובענה או קובלנה בשל אותה פגיעה, רשאים בן זוגו, ילדו או הורהו, ואם לא השאיר בן זוג, ילדים או הורים – אחיו או אחותו, להגיש, תוך שישה חודשים לאחר מותו, תובענה או קובלנה בשל אותה פגיעה.

(ב) אדם שהגיש תובענה או קובלנה בשל פגיעה בפרטיות ומת לפני סיום ההליך, רשאים בן זוגו, ילדו או הורהו, ואם לא השאיר בן זוג, ילדים או הורים – אחיו או אחותו, להודיע לבית המשפט, תוך ששה חודשים לאחר מותו, על רצונם להמשיך בתובענה או בקובלנה, ומשהודיע כאמור יבואו הם במקום התובע או הקובל.

סעיף 70: סייג לפרסום הליכים

במשפט פלילי או אזרחי בשל פגיעה בפרטיות רשאי בית המשפט מיוזמתו או לבקשת בעל דין, לאסור או לעכב זמנית, מנימוקים שירשמו, פרסום ברבים של הליכי בית המשפט – לרבות כתבי טענות, כתבי בי-דין אחרים, כתב אישום ודבר הגשתם של אלה ולרבות פסק דין כל עוד אינו חלוט – במידה שראה צורך בכך לשם הגנה על פרטיותו של אדם הנוגע במשפט; העובר על האיסור לפי סעיף זה, דינו – מאסר ששה חודשים או קנס _____.

סעיף 71: דין שני משפטים

על הליכים משפטיים בשל פגיעה בפרטיות יחולו הוראות סעיף 77 לחוק בתי המשפט [נוסח משולב], התשמ"ד–1984.

סעיף 72: צווים נוספים

הוראת סעיף 29 בחוק הגנת הפרטיות הקיים לא נדונה בקבוצת המומחים.

סעיף 73: חומר פסול לראיה

חומר שהושג תוך פגיעה בפרטיות יהיה פסול לשמש ראיה בבית משפט, ללא הסכמת הנפגע, זולת אם בית המשפט התיר מטעמים שיירשמו להשתמש בחומר, או אם היו לפוגע, שהיה צד להליך, הגנה או פטור לפי חוק זה.

סעיף 74: דו"ח הגנה על הפרטיות

לא יאוחר מ-1 באפריל בכל שנה יגיש ראש הרשות להגנת הפרטיות לוועדת החוקה חוק ומשפט של הכנסת דין וחשבון על פעולותיה של הרשות, ובכלל זה פעולות האכיפה והפיקוח לפי חוק זה בשנה שקדמה להגשת הדוח, לרבות מספר העיצומים הכספיים שהוטלו, סכומם, בשל אילו הפרות הוטלו ומספר ההפרות החוזרות שבוצעו מתוך כלל ההפרות בשנה שקדמה למועד הדיווח.

סעיף 75: תיקון חוק בתי משפט לעניינים מינהליים

בחוק בתי המשפט לעניינים מינהליים, התש"ס–2000,[72] בתוספת הראשונה, במקום פרט 28 יבוא:

"28. החלטה של הרשות להגנת הפרטיות לפי חוק הגנת הפרטיות, התשע"ט–2019".

סעיף 76: שמירת דינים

הוראות חוק זה לא יגרעו מהוראות כל דין אחר שהיה קיים ערב תחילתו של חוק זה.

סעיף 77: ביצוע ותקנות

שר המשפטים ממונה על ביצוע חוק זה והוא רשאי, באישור ועדת החוקה חוק ומשפט של הכנסת, להתקין תקנות, בכל עניין הנוגע לביצועו, ובין השאר –

(1) תנאי החזקת מידע אישי ושמירתו;

(2) תנאים להעברת מידע אישי למחוץ לגבולות המדינה;

(3) תנאי אבטחת מידע אישי;

(4) הוראות לענין ביעור מידע עם הפסקת עיבודו;.

סעיף 78: התאמה למדד

(א) הסכום לתשלום בגין מימוש זכות מזכויות נושא המידע לפי סעיף 16(ב) וסכום הפיצוי בלא הוכחת נזק לפי סעיף 63 יעודכנו ב-16 בכל חודש, בהתאם לשיעורי השינוי במדד החדש לעומת המדד הבסיסי, לעניין זה –
"המדד" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה;
"המדד החדש" – מדד החודש שקדם לחודש העדכון;
"המדד הבסיסי" – מדד חודש דצמבר 2018.

(ב) סכומי העיצום הכספי כאמור בסעיף 38 וסכום הקנס כאמור בסעיף 70 יעודכנו ב-1 בינואר בכל שנה (בסעיף קטן זה – "יום העדכון"), בהתאם לשיעור שינוי המדד הידוע ביום העדכון לעומת המדד שהיה ידוע ב-1 בינואר של השנה הקודמת; הסכום האמור יעוגל לסכום הקרוב שהוא מכפלה של 10 שקלים חדשים; לעניין זה, "מדד" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה. שר המשפטים יפרסם בהודעה ברשומות את סכום הקנס המעודכן לפי סעיף קטן זה. ראש הרשות להגנת הפרטיות יפרסם ברשומות הודעה על סכומי העיצום הכספי המעודכנים לפי סעיף קטן זה.

דברי הסבר

<u>סעיף 68:</u> זהה לסעיף 24 לחוק הגנת הפרטיות הקיים.

<u>סעיף 69:</u> זהה לסעיף 25 לחוק הגנת הפרטיות הקיים.

לא אימצנו את הוראת סעיף 26 בחוק הגנת הפרטיות הקיים, הקובע כי "תקופת ההתיישנות של תביעה אזרחית לפי חוק זה היא שנתיים".

ביולי 2014 ובינואר 2018 הונחו על שולחן מליאת הכנסת לדיון מוקדם שתי הצעות חוק פרטיות, ביוזמת חברי הכנסת עדי קול ועומר בר לב (בהתאמה). הצעות החוק ביקשו לבטל כליל את סעיף 26 כדי "לתקן עוול היסטורי לפיו התיישנות על תביעה אזרחית בהתאם לחוק הגנת הפרטיות היא בת שנתיים בלבד, ואילו חוק ההתיישנות, התשי"ח–1958, קובע שתקופת ההתיישנות בנושאים אזרחיים כגון הפרת חוזה, הסגת גבול, תקיפה, התרשלות ומטרד עומדת על שבע שנים." על פי דברי ההסבר לחוק הגנת הפרטיות הקיים, הסיבה להבדלים בתקופת ההתיישנות הייתה הרצון להאיץ בתובעים להגיש תביעה מייד לאחר הפגיעה

בפרטיותם. ואולם היום יש להשוות את תקופת ההתיישנות לתביעה אזרחית בגין פגיעה בפרטיות מאחר ש"קיום זהויות דיגיטליות מקשה על איתור הפוגע, ויש לאפשר לנפגע פרק זמן להתמודד עם הפגיעה נעשתה כלפיו ולאתר את הפוגע."[73] מסיבות אלו, ולנוכח חשיבותה של הזכות לפרטיות כזכות יסוד חוקתית, אנו סבורים כי יש להשוות את תקופת ההתיישנות הקבועה בהצעת החוק לזו הנהוגה בעוולות אזרחיות אחרות. ככל שמדובר בתקופת התיישנות שאינה חורגת מהקבוע בחוק ההתיישנות, התשי"ח–1958, אין צורך בקביעה מיוחדת בחוק הפרטני, ולכן אין מקום לקביעת הוראה להתיישנות בהצעת החוק.

סעיף 70: הסעיף בא להחליף את סעיף 27 בחוק הגנת הפרטיות הקיים, המפנה לסעיפים 21, 23 ו-24 בחוק איסור לשון הרע, התשכ"ה–1965. סעיף 23 בחוק איסור לשון הרע אינו רלוונטי לעולם הדיגיטלי, ויש להחיל במקומו את דיני הראיות הרגילים.

במקום ההפניה לסעיף 21 לחוק איסור לשון הרע, התשכ"ה–1965, הוספה לתיקון המוצע לשון הסעיף במלואה, למעט ההוראה הקובעת שבית המשפט אינו יכול לעכב או לאסור פרסום דבר פתיחתו של הליך פלילי אם הנפגע התנגד לכך. הוראה זו מתאימה לדיני איסור לשון הרע ואין מקומה בהצעת חוק העוסקת בפגיעה בפרטיות. במקום סעיף 24 לחוק איסור לשון הרע הוספה בסעיף 71 להצעת החוק הפנייה לסעיף 77 לחוק בתי המשפט.

סעיף 27 לחוק הגנת הפרטיות הקיים: "על הליכים משפטיים בשל פגיעה בפרטיות יחולו הוראות סעיפים 21, 23 ו-24 לחוק איסור לשון הרע, תשכ"ה–1965, בשינויים המחוייבים לפי הענין."

סעיף 21 לחוק איסור לשון הרע, התשכ"ה–1965:

"במשפט פלילי או אזרחי בשל לשון הרע רשאי בית המשפט מיזמתו או לבקשת בעל דין, לאסור או לעכב זמנית, מנימוקים שיירשמו, פרסום ברבים של הליכי בית המשפט – לרבות כתבי טענות, כתבי בי-דין אחרים, כתב אישום ודבר הגשתם של אלה ולרבות פסק דין כל עוד אינו חלוט – במידה שראה צורך בכך לשם הגנה על שמו של אדם הנוגע במשפט ואולם לא יאסור בית משפט ולא יעכב זמנית את פרסום דבר פתיחתו של הליך משפטי, או את הפרסום של כתב אישום, תביעה או פסק דין, אם התנגד לכך הנפגע; העובר על האיסור לפי סעיף זה, דינו – מאסר ששה חדשים או קנס 5000 לירות."

סעיף 23 לחוק איסור לשון הרע, התשכ"ה–1965:

"הוגש עותק של עתון או של דבר-דפוס אחר המופץ ברבים שבו נדפסה לשון הרע, ישמש הדבר ראיה לכאורה שאכן נעשה הפרסום באותו עתון או דבר-דפוס."

סעיף 71: מבוסס על סעיף 27 לחוק הגנת הפרטיות הקיים, אבל במקום ההפניה לסעיף 24 לחוק איסור לשון הרע, התשכ"ה–1965, מוצע להפנות להוראת סעיף 77 לחוק בתי המשפט [נוסח משולב], התשמ"ד–1984. בנושא סמכות אזרחית נגררת לפלילים – הוראת סעיף 77 לחוק בתי המשפט היא עדכנית וברורה יותר מהוראת סעיף 24 לחוק איסור לשון הרע.

סעיף 77 לחוק בתי המשפט [נוסח משולב], התשמ"ד–1984:

"(א) הורשע אדם בבית משפט שלום או בבית משפט מחוזי והוגשה נגדו – ונגדו בלבד – תביעה אזרחית בשל העובדות המהוות את העבירה שבה הורשע, מוסמך השופט או המותב שהרשיעו, לאחר שפסק הדין בפלילים הפך לחלוט, לדון בתביעה האזרחית, אם ביקש זאת מגיש התביעה; לענין זה מוסמך בית משפט מחוזי לדון גם אם התביעה לפי שוויה היא בתחום סמכותו של בית משפט שלום.

(ב) שר המשפטים יקבע בתקנות את סדרי הדין בתביעה האזרחית, לרבות הוראות בדבר המועד והדרך להגשת התביעה וההליכים בערעור."

סעיף 24 לחוק איסור לשון הרע, התשכ"ה-1965:

"במשפט אזרחי בשל לשון הרע שנדון לאחר שמשפט פלילי נגד אותו אדם בשל אותה לשון הרע נסתיים, רשאי בית המשפט להסתמך על הממצאים העובדתיים, כולם או מקצתם, שנקבעו במשפט הפלילי על-פי הראיות שנגבו בו, בלי לחזור על גבייתן."

<u>סעיף 73:</u> זהה לסעיף 32 לחוק הגנת הפרטיות הקיים.

<u>סעיף 74:</u> מבוסס על הוראת סעיף 10א בחוק הגנת הפרטיות הקיים ועל סעיף 22כו לחוק הגנת הצרכן לעניין דיווח על אכיפה מינהלית. בדיונים בוועדת הכלכלה של הכנסת בהצעת תיקון מס' 39 לחוק הגנת הצרכן דרשו חברי הכנסת את הכללתו של סעיף 22כו לחוק הגנת הצרכן בנוסח החוק המתוקן. הנימוק לדרישתם היה שיש להכניס אמצעי בקרה של הכנסת על עבודת הממונה על הגנת הצרכן כדי למנוע אכיפת יתר בלתי מידתית שבמסגרתה יטיל הממונה עיצומים כספיים גדולים על עוסקים קטנים בגין עבירות של מה בכך.[74] לדעתנו נימוק זה עומד גם בעניין חוק הגנת הפרטיות. הסרנו מן הסעיף את הדרישה לצרף את הערותיה של המועצה להגנת הפרטיות לדוח. נימוקינו: בהצעת החוק הצענו להקים ועדה מייעצת ולא מועצה ציבורית; ובחוקים אחרים שיש בהם חובת דיווח לכנסת – למשל סעיף 22כו לחוק הגנת הצרכן וס' 14 לחוק ניירות ערך – הדיווח אינו נתון קודם להעברתו לכנסת להערות של גורם נוסף מלבד הרשות עצמה.

סעיף 22כו לחוק הגנת הצרכן, התשמ"א-1981:

"הממונה ידווח לוועדת הכלכלה של הכנסת, אחת לשנה, על מספר העיצומים הכספיים שהוטלו, סכומם, בשל אילו הפרות הוטלו ומספר ההפרות החוזרות שבוצעו מתוך כלל ההפרות בשנה שקדמה למועד הדיווח; דיווח כאמור יימסר במשך חמש שנים מתום שנה מיום תחילתו של חוק הגנת הצרכן (תיקון מס' 39), התשע"ד–2014."

סעיף 14 לחוק ניירות ערך, התשכ"ח-1968:

"הרשות תמסור דו"חות על פעולותיה לשר האוצר ולוועדת הכספים של הכנסת, לפי דרישתם ולפחות אחת לשנה."

<u>סעיף 75:</u> מיועד להבהיר שכל החלטה של הרשות להגנת הפרטיות היא החלטה מינהלית שמותר לעתור בגינה לבית המשפט לעניינים מינהליים.

<u>סעיף 76:</u> מבוסס על שילוב סעיף 35 בחוק הגנת הפרטיות הקיים עם סעיף 10 בחוק-יסוד: כבוד האדם וחירותו – מתוך הבנת חשיבותה ומרכזיותה של הזכות לפרטיות כזכות יסוד חוקתית.

<u>סעיף 77:</u> מבוסס על סעיף 36 לחוק הגנת הפרטיות הקיים מתוך התאמת הנושאים ששר המשפטים מוסמך בהם להתקין תקנות לפי הצעת החוק.

<u>סעיף 78:</u> מבוסס על תקנה 6 לתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי דין בערעור על סירוב לבקשת עיון), התשמ"א–1981, ועל סעיף 23כה(ב) להצ"ח תיקון מס' 13. סעיף 78 הוא סעיף סל שמאגד את כל ההוראות הנוגעות לעדכון סכום כספי לפי הצעת החוק: תשלום בעבור מימוש זכות מזכויות נושא המידע לפי סעיף 16, פיצוי בלא הוכחת נזק לפי סעיף 63, עיצום כספי לפי סעיף 38 וקנס לפי סעיף 70.

1 חוק-יסוד: כבוד האדם וחירותו, ס"ח התשנ"ב 1391.

2 לכתיבה חשובה על תאוריות של פרטיות ראו למשל רות גביזון, "הזכות לפרטיות ולכבוד", **זכויות אדם בישראל: קובץ מאמרים לזכרו של חמן שלח** 61 (רות גביזון עורכת, 1989); Daniel J. Solove, Understanding Privacy (2008); Helen Nissenbaum, Privacy In Context: Technology, Policy and the Integrity of Social Life (2010); מיכאל בירנהק, **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 57-109 (2010).

3 ראו בג"ץ 6650/04 **פלונית נ' בית הדין הרבני האזורי נתניה**, פ"ד סא(1) 581 (2006).

4 ס"ח התשנ"ה 366.

5 ס"ח התשנ"ו 338.

6 הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח–2018 [להלן: "**הצ"ח תיקון מס' 13**"].

7 הצוות לבחינת החקיקה בתחום מאגרי המידע, דין וחשבון (ינואר 2007), עמ' 19-23 [להלן: "**ועדת שופמן**"].

8 ס"ח התש"ע 256.

9 ס"ח התשס"א 62.

10 חוק נתוני אשראי, התשע"ו-2016, ס"ח 2551, עמ' 838.

11 ס"ח התשס"ח 72.

12 משרד הבריאות, "בריאות דיגיטלית: אסטרטגיה", עמ' 27, 56 (אפריל 2017).

13 רחל ארידור-הרשקוביץ ותהילה שוורץ אלטשולר, "אתגר הפרטיות בפרסום יזום של מאגרי מידע ממשלתיים", עמ' 41-47 (המכון הישראלי לדמוקרטיה, הצעה לסדר 14, ספטמבר 2017).

14 דיני מדינת ישראל נוסח חדש 12, עמ' 284.

15 הצעת חוק הגנת הפרטיות (תיקון – הגנה על פרטיות של קטינים), התשע"ז–2017 (להלן: "**הצ"ח פרטיות קטינים**").

16 ועדת שופמן, ה"ש 7 לעיל, עמ' 24.

17 תזכיר חוק הגנת הפרטיות (לצמצום חובת הרישום וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולתיעודם במסמכים), התשע"ב–2012.

18 מניעת הטרדה מאיימת, התשס"ב–2011, ס"ח תשס"ב 1809.

19 ס"ח תשנ"ח 1661.

20 אסף הרדוף, "צילום חכם: האם צילום מחשב ללא רשות ראוי להוות עברה פלילית", **משפטים** על אתר (2018).

21 Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/56/EC*, 844/14/EN WP 217 (2014)

22 ארידור-הרשקוביץ ושוורץ אלטשולר, ה"ש 13 לעיל, עמ' 41-47.

23 סעיף 6 לחוק הכשרות המשפטית והאפוטרופסות, התשכ"ו-1962, קובע: "פעולה משפטית של קטין שדרכם של קטינים בגילו לעשות כמוה, וכן פעולה משפטית בין קטין לבין אדם שלא ידע ולא היה עליו לדעת שהוא קטין ,אינה ניתנת לביטול כאמור בסעיף 5, אף שנעשתה שלא בהסכמת נציגו, אלא אם היה בה משום נזק של ממש לקטין או לרכושו".

24 ועדת שופמן, ה"ש 7 לעיל, עמ' 42-47.

25 ע"א 8954/11 **פלוני נ' פלונית**, סעיף 159-160 (פורסם בנבו, 24.04.2014).

26 סעיף 3(ד)(7) לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007: "פרטי הזיהוי של המנוי או מיתקן הבזק שנתוני התקשורת מתבקשים לגביהם ,אם הם ידועים מראש, לרבות היות המנוי האמור מי שחל לגביו חיסיון מקצועי לפי כל דין (בחוק זה – בעל מקצוע); בפסקה זו, "דין" – לרבות הלכה פסוקה;"

27 Lilian Edwards & Michael Veals, *Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decision"?*, IEEE Security & Privacy (2018)

28 Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, 18 (Adopted on Dec. 13, 2016, as last revised and adopted on April 5, 2017). 16EN WP 242 rev.01

29 Google Spain SL. v. Costeja (May 13, 2014)

30 סעיפים 6(1)(c), 12(b) ו-14(a) ל- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (להלן: "**הדירקטיבה**").

31 Article 29 Data Protection WP, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251rev.01 (Oct. 3, 2017)

32 Michael J. Kelly & Satolam David, *The Right to Be Forgotten*, U. III. L. REV. 1 (2017).

33 AMITAI ETZIONI, HAPPINESS IN THE WRONG METRIC: A LIBERAL COMMUNITARIAN RESPONSE TO POPULISM (2018)

34 Ryan Belbin, *When Google Becomes the Norm: The Case for Privacy and the Right to be Forgotten*, 26 DALHOUSIE J. OF LEGAL STUD. 17 (2018)

35 הצעת חוק פ/3867/20 הגנת הפרטיות (תיקון – הזכות להישכח), התשע"ז–2017, שהגישה חברת הכנסת מירב בן ארי; הצעת חוק פ/3066/20 הצעת חוק הגנת הפרטיות (תיקון – הזכות להישכח), התשע"ו–2016, שהגישו ח"כ עופר שלח וח"כ אורי מקלב.

36 32ND International Conference of Data Protection and Privacy Commissioners, Jerusalem, Oct. 27-29, 2010

37 תקנה 5(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017 קובעת כך:

"5. (ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר סיכוני אבטחת מידע (להלן- סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשרה חודשים לפחות."

38 Privacy Amendment (Notifiable Data Breaches) Act 2017 No. 12, 2017

39 אמיתי זיו, "בעקבות מחדל הסיסמאות: חקירה באיתוראן – הוחרמו ראיות דיגיטליות", **דה מרקר** (6 ביוני 2018).

40 Article 29 Data Protection Working Party, Guidelines on Data Protection Offices ('DPOs'), 16EN WP 243 (Dec. 13, 2016)

41 רע"א 5860/16 **Facebook Inc. נ' בן חמו** (פורסם בנבו, 31.5.2018).

42 ס"ח התשמ"ה 60.

43 ס"ח התשי"א 52.

44 ס"ח התשי"ט 86.

45 שגיא כהן, "פייסבוק: מידע על 47 אלף ישראלים נחשף בפרשת קיימברידג' אנליטיקה", **Ynet** (10 באפריל 2018).

FTC Earns Prestigious International Award for AshleyMadison.com Data Breach Investigation, FTC (Sep. 27, 2017) 46

47 39th International Conference of Data Protection and Privacy Commissioners Hong Kong, Sep. 25-29, 2017, Resolution on exploring future options for International Enforcement Cooperation (2017)

48 ס"ח התשי"ח 191.

49 הצ"ח תיקון מס' 13, דברי ההסבר לסעיף 3.

50 פרוטוקול ישיבה מס' 883 של ועדת הכלכלה של הכנסת ה-18 (12 ביוני 2012).

51 פרוטוקול ישיבה מס' 883 של ועדת הכלכלה של הכנסת ה-18 (12 ביוני 2012).

52 ס"ח התשל"ז 266.

53 חוקי א"י, כרך א', עמ' (ע) 439, (א) 467.

54 ס"ח התשס"ב 468.

55 ס"ח התשל"ז 266.

56 הצעת חוק ההגבלים העסקיים (תיקון מס' 5), התשנ"ט–1989, עמ' 386, דברי ההסבר לסעיף 11.

57 ס"ח התשכ"א 192.

58 ס"ח התשנ"ה 170.

59 פרוטוקול מישיבה מס' 912 של ועדת הכלכלה של הכנסת ה-18, עמ' 64-72 (10 ביולי 2012).

60 פרוטוקול מישיבה מס' 822 של ועדת הכלכלה של הכנסת ה-18, עמ' 25-29 (02 באפריל 2012).

61 הצעת חוק ייעול הליכי האכיפה ברשות ניירות ערך (תיקוני חקיקה), התש"ע–2010, עמ' 440, דברי ההסבר לסעיף 52סא המוצע.

62 דיני מדינת ישראל, נוסח חדש 10, עמ' 266.

63 חוק ההגבלים העסקיים (תיקון מס' 13), התשע"ב–2012.

64 חוק הגנת הצרכן (תיקון מס' 39), התשע"ד–2014.

65 ס"ח התשכ"ה 240.

66 ע"פ 480/85 **קורטאם נ' מדינת ישראל**, פ"ד מ(3) 673.

67 ע"א 9183/09 **The Football Association Premier League Limited נ' פלוני**, פדאור 12(43) 557 (2012)).

68 דנ"א 2121/12 **פלוני נ' ד"ר אילנה דיין אורבך** (פורסם בנבו, 17.04.2013); ע"פ 5026/97 **גלעם נ' מדינת ישראל** (לא פורסם).

69 קביעה זו ניתנה באשר לסעיף 15(2) בחוק איסור לשון הרע, אבל בית המשפט עמד על הזהות שבין סעיף זה לסעיף 18(2)(ב) וקבע שפרשנותן על כן זהה. ראו ע"א 5653/98 **אמיליו פלוס נ' דינה חלוץ**, פ"ד נה(5) 865.

70 ע"פ 5026/97 **גלעם נ' מדינת ישראל** (לא פורסם).

71 סמכות המעקב והפגיעה הגורפת בפרטיות על ידי ה-NSA בארצות הברית, כפי שנתגלה מן המסמכים שחשף סנאודן, הייתה הסיבה העיקרית לביטול ה-harbor safe בארצות הברית (*Maximillian Schrems v Data Commissioner*, Case C–362/14, *Protection* (October 6, 2015, ECLI:EU:C:2015:650). דיונים בעניין ההכרה בתאימות הדין ביפן ובאנגליה ל-GDPR עסקו בסמכות המעקב הניתנת לרשויות הביטחון בכל אחת מהמדינות. ראו Andrew D. Murray, *Data Transfers between the EU and UK Post Brexit?*, 7(3) INTERNATIONAL DATA PRIVACY LAW 149(2017); Claude Moraes, Motion for A Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection of personal data afforded by Japan (2018q2979 (RSP))

72 ס"ח התש"ס 190.

73 הצעת חוק הגנת הפרטיות פ/2706/19 (תיקון – הארכת תקופת התיישנות), התשע"ד–2014; הצעת חוק הגנת הפרטיות פ/5033/20 (תיקון – תקופת ההתיישנות), התשע"ח–2018.

74 פרוטוקול ישיבה מס' 235 של ועדת הכלכלה של הכנסת ה-19, עמ' 74-76 (06 במרץ 2014).

הצעת חוק הגנת הפרטיות, התשע"ט–2019
ודברי הסבר מקוצרים

תוכן העניינים

פרק א: מטרה, פרשנות ועקרונות יסוד 169

סעיף 1: מטרת החוק 169

סעיף 2: הגדרות 169

סעיף 3: איסור פגיעה בפרטיות 175

סעיף 4: פגיעה בפרטיות 175

סעיף 5: פרסום תצלומו של נפטר 175

פרק ב: הגנה על הפרטיות במידע אישי 177

סימן א׳: הוראות כלליות לעניין עיבוד מידע אישי 177

סעיף 6: פגיעה מותרת בפרטיות 177

סעיף 7: דרישת קיום המטרה 179

סעיף 8: הסכמה לעניין פגיעה בפרטיותו של קטין 179

סעיף 9: חובת מתן הודעה 180

סימן ב׳: זכויות נושא המידע 181

סעיף 10: זכות החזרה מהסכמה 181

סעיף 11: זכות עיון במידע אישי 182

סעיף 12: זכות לקבל הסבר 184

סעיף 13: זכות תיקון מידע אישי 185

סעיף 14: הזכות לניוד מידע אישי 186

סעיף 15: זכות המחיקה של מידע אישי 188

סעיף 16: מימוש זכויות נושא המידע 189

סעיף 17: תובענה לבית המשפט 190

סימן ג׳: חובות בעל השליטה במידע והמעבד 190

סעיף 18: מעבד המידע 190

סעיף 19: עיצוב לפרטיות 190

סעיף 20: תסקיר השפעה על הפרטיות 191

סעיף 21: אבטחת מידע אישי 191
סעיף 22: תיעוד ודיווח על אודות אירוע אבטחה 192
סעיף 23: ממונה על הגנת הפרטיות במידע 194

סימן ד': שונות 196

סעיף 24: תחולת הוראות פרק ב' 196
סעיף 25: נציגות בעל שליטה במידע או מעבד בישראל 196

פרק ג: הרשות להגנת הפרטיות וסמכויות פיקוח, אכיפה ובירור מינהלי 197

סימן א': הרשות להגנת הפרטיות 197

סעיף 26: ראש הרשות להגנת הפרטיות 197
סעיף 27: תקציב הרשות 197
סעיף 28: עסקאות הרשות 197
סעיף 29: עובדי הרשות להגנת הפרטיות 197
סעיף 30: תפקידי הרשות להגנת הפרטיות 198
סעיף 31: שיתוף פעולה עם רשות חוץ 199
סעיף 32: הוועדה המייעצת 200
סעיף 33: הסמכת חוקר או מפקח 201

סימן ב': סמכויות פיקוח 202

סעיף 34: סמכויות מפקח 202

סימן ג': סמכויות בבירור מינהלי 202

סעיף 35: צו לחיפוש ולחדירה לחומר מחשב 202
סעיף 36: אופן ביצוע חדירה לחומר מחשב והעתקתו 202
סעיף 37: סמכויות אכיפה, חקירה, עיכוב ותפיסה 203

פרק ד: אמצעי אכיפה מינהליים 204

סימן א': עיצום כספי 204

סעיף 38: עיצום כספי 204
סעיף 39: הפרה בנסיבות מחמירות 205
סעיף 40: הודעה על כוונת חיוב 206

סעיף 41: זכות טיעון 206
סעיף 42: החלטת ראש הרשות להגנת הפרטיות ודרישת תשלום 206
סעיף 43: הפרה נמשכת והפרה חוזרת 207
סעיף 44: סכומים מופחתים 207
סעיף 45: סכום מעודכן של הפיצוי הכספי 207
סעיף 46: המועד לתשלום העיצום הכספי 208
סעיף 47: הפרשי ריבית והצמדה 208
סעיף 48: גבייה 208

סימן ב': התראה מינהלית 208

סעיף 49: התראה מינהלית 208
סעיף 50: בקשה לביטול התראה מינהלית 208
סעיף 51: הפרה נמשכת והפרה חוזרת לאחר התראה 209

סימן ג': התחייבות להימנע מהפרה 209

סעיף 52: התחייבות להימנע מהפרה והפקדת עירבון 209
סעיף 53: תוצאות הגשת כתב התחייבות ועירבון או אי הגשתם 210
סעיף 54: הפרת התחייבות 210
סעיף 55: השבת העירבון 210

סימן ד': הוראות כלליות 211

סעיף 56: עיצום כספי בשל הפרה לפי חוק זה ולפי חוק אחר 211
סעיף 57: פרסום לעניין הטלת עיצום כספי 212
סעיף 58: שמירת אחריות פלילית 213
סעיף 59: אישור נהלים ופרסומם 213
סעיף 60: אצילת סמכויות 213

פרק ה: מסירת מידע אישי או ידיעות מאת גופיים ציבוריים 214

פרק ו: עוולה אזרחית ועונשין 214

סעיף 61: פגיעה בפרטיות – עוולה אזרחית 214
סעיף 62: פגיעה בפרטיות – עבירה 214
סעיף 63: פיצוי בלא הוכחת נזק 215
סעיף 64: שיקולים בגזירת הדין או גובה הפיצוי 216

פרק ז: הגנות 217

סעיף 65: הגנות מה הן 217

סעיף 66: פטור 219

סעיף 67: הפרכה של טענות הגנה 219

פרק ח: הוראות שונות 219

סעיף 68: דין המדינה 219

סעיף 69: מות הנפגע 219

סעיף 70: סייג לפרסום הליכים 220

סעיף 71: דין שני משפטים 220

סעיף 72: צווים נוספים 220

סעיף 73: חומר פסול לראיה 220

סעיף 74: דו"ח הגנה על הפרטיות 220

סעיף 75: תיקון חוק בתי משפט לענינים מינהליים 220

סעיף 76: שמירת דינים 221

סעיף 77: ביצוע ותקנות 221

סעיף 78: התאמה למדד 221

פרק א: מטרה, פרשנות ועקרונות יסוד

סעיף 1: מטרת החוק

חוק זה מטרתו להגן על פרטיותו של אדם, לשם מימוש האוטונומיה של הפרט, ובכלל זה מתן הגנה על המרחב האישי של אדם, צנעת חייו האישיים, סוד שיחו, וזכותו לשלוט במידע אישי על אודותיו ובעיבודו; לשם הבטחת קיומו של הליך דמוקרטי תקין, ולשם מניעת השפעה בלתי הוגנת המבוססת על עיבוד מידע אישי על אודותיו.

סעיף 2: הגדרות

בחוק זה –

"**אבטחת מידע אישי**" – הגנה על נכונות המידע האישי, סודיותו, זמינותו או שלמותו;

"**אדם**" – לעניין סעיף 1, ההגדרות "חסר ישע", "מידע אישי", "מידע רגיש", "נושא מידע", "קטין" ו-"קשיש" שבסעיף 2, וסעיפים 4, 9, 11, 23(ה), 63(ג), 65(א)(3)(ה), 65(א)(3)(ז), 69 ו-70 – למעט תאגיד;

"**אירוע אבטחה**" – אירוע שבו נפגעה אבטחת מידע אישי;

"**בעל שליטה במידע**" – אדם הקובע, לבד או ביחד עם אחר, את המטרות והדרכים לעיבוד מידע אישי;

דברי הסבר

<u>סעיף 1:</u> מטרתו לקדם את ההגנה על פרטיותו של אדם, שהיא זכות אדם חוקתית המעוגנת בחוק-יסוד: כבוד האדם וחירותו.[1] על בסיס ההכרה שהזכות לפרטיות היא זכות רחבה ושלא כל מופעיה מוגדרים במפורש בהצעת החוק, הסעיף מונה רשימה פתוחה של אפשרויות לפגיעה בפרטיות. הרשימה נעה על ציר שבין מניעת פגיעה בבחירה חופשית והבטחת הליך דמוקרטי תקין לבין הגנה על מרחב שבתוכו אדם זכאי להיות עם עצמו וזכותו לשלוט במידע אישי עליו ובעיבודו.[2] ככל זכות אדם אחרת גם הזכות לפרטיות היא יחסית ולא מוחלטת, ועל כן פגיעה בה תיתכן רק לפי דרישות פסקת ההגבלה שבסעיף 8 לחוק-יסוד: כבוד האדם וחירותו ובהתאם להצעת החוק.

<u>סעיף 2:</u> הגדרת "**אבטחת מידע אישי**" מבוססת על הגדרת המונח בסעיף 7 לחוק הגנת הפרטיות הקיים ועל מודל אבטחת המידע המקובל בעולם ובתעשייה, המבוסס על המשולש CIA (Confidentiality, Integrity, Availability): סודיות המידע האישי, נכונותו וזמינותו, כתנאים הדרושים להבטחה שהגישה אל המידע האישי תוגבל רק למי שמורשה לכך.

הגדרת "**אדם**" תואמת את ההגדרה בסעיף 3 לחוק הגנת הפרטיות הקיים, שבדומה להבחנה ב-GDPR, כמוסבר בסעיף 14 להקדמה ל-GDPR, מבחינה בין אדם (natural person) לבין כל ישות משפטית (legal person) ובכלל זה תאגיד.

הגדרת "**אירוע אבטחה**" מבוססת על הגדרת המונח "**אבטחת מידע אישי**" ונועדה להדגיש שאירוע אבטחה הוא כל פגיעה במודל של ה-CIA לאבטחת מידע. ההגדרה מותירה מקום לתוספת של מדרג אירועי אבטחה, בדומה לקבוע בתקנות אבטחת מידע.

הגדרת "**בעל שליטה במידע**" מחליפה את הגדרת "מנהל מאגר מידע" בסעיף 7 לחוק הגנת הפרטיות הקיים ומבוססת על סעיף 4(7) ל-GDPR. מטרתה להגביר את תאימות הצעת החוק ל-GDPR.

"**בקשה לסיוע**" – בקשה לסיוע לרשות חוץ שהוגשה בכתב לרשות להגנת הפרטיות על ידי רשות חוץ;

"**גוף ציבורי**" –

(1) משרדי הממשלה ומוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין;

(2) גוף אחר ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, ובלבד שבצו ייקבעו סוגי המידע האישי והידיעות שהגוף יהיה רשאי למסור ולקבל;

"**דיני הגנת הפרטיות**" – דינים בתחום הגנת הפרטיות ופרטיות במידע שהרשות להגנת הפרטיות או רשות חוץ מופקדת על ביצועם ואכיפתם, ולעניין זה, משמעותם של מונחים בדיני הגנת הפרטיות במדינת חוץ תהא כמשמעותם בדין שבתחום סמכותה של רשות החוץ;

"**הסכמה**" – הסכמה מדעת ומרצון חופשי, במפורש או מכללא;

"**חוק המחשבים**" – חוק המחשבים, התשנ"ה–1995;[3]

"**חוק המעצרים**" – חוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו–1996;[4]

"**חוקר**" ו"**מפקח**" – מי שהוסמך לכך לפי סעיף 33;

"**חומר מחשב**" ו"**מחשב**" – כהגדרתם בחוק המחשבים;

"**חסר ישע**" – אדם שמחמת מחלתו, ליקויו הרוחני, מעצרו או כל סיבה אחרת אינו יכול לספק לעצמו את צרכי חייו;

"**חפץ**" – כהגדרתו בפקודת המעצר והחיפוש;

דברי הסבר

הגדרת "**בקשה לסיוע**" מבוססת על הגדרת המונח בסעיף 54יא1 לחוק ניירות ערך, התשכ"ח–1968. היא אינה מתייחסת ל"מזכר הבנה" שכן שיתוף המידע האישי בין הרשות להגנת הפרטיות לבין רשות חוץ אינו מותנה, לפי סעיף 31 להצעת החוק, בחתימה על מזכר הבנות.

הגדרת "**גוף ציבורי**" זהה להגדרה בסעיף 23 לחוק הגנת הפרטיות הקיים.

הגדרת "**דיני הגנת הפרטיות**" מבוססת על סעיף 54יא1 לחוק ניירות ערך, התשכ"ח–1968, ועל התאמתה להצעת החוק.

הגדרת "**הסכמה**" מבוססת על הגדרת המונח בסעיף 3 לחוק הגנת הפרטיות הקיים, בתוספת דרישת ה"רצון החופשי" כתנאי לתקפות ההסכמה. המטרה היא לחזק את דרישת ההסכמה כדרישה אפקטיבית, לצמצם את השימוש הגובר בהסכמה כדרישה צורנית בלבד וליצור את ההבנה שהסכמה אינה חזות הכול. הסכמה תיחשב לניתנת מ"רצון חופשי" כאשר מוכח שהיא ניתנה לאחר שנושא המידע ידע והבין, או סביר שידע והבין, את מטרת הפגיעה בפרטיותו ואת מידת הפגיעה, הסיכונים הכרוכים בה והאפשרויות העומדות לפניו ונתן את הסכמתו מרצונו החופשי. פרשנות זו עולה בקנה אחד עם תנאיה של דרישת ההסכמה ב-GDPR. עם זאת, ההגדרה מאפשרת לבית המשפט מרחב תמרון באמצעות המונחים "מדעת" וההכרה גם בהסכמה מכללא.

ההגדרות "**חוק המחשבים**", "**חומר מחשב**", ו"**חפץ**" זהות להגדרות בסעיף 23ט להצ"ח תיקון מס' 13.[5]

הגדרת "**חסר ישע**" מבוססת על סעיף 322 לחוק העונשין, התשל"ז–1977.

"מידע אישי" – נתונים על אודות אדם מזוהה, לרבות נתונים המאפשרים במאמץ סביר את זיהויו של אדם;

"מידע אישי מדגמי" – מידע אישי אקראי שבעל שליטה במידע ביצע או מבצע בו פעולות עיבוד.

"מידע רגיש" – מידע אישי שיש בו כדי לזהות אחד מאלה:

(1) נתונים על אישיותו של אדם וצנעת חייו האישיים;

(2) נתונים על עברו הפלילי של אדם;

(3) נתונים על דעותיו הפוליטיות ואמונתו הדתית של אדם;

(4) נתונים על מצבו הבריאותי של אדם;

(5) נתוני זיהוי ביומטריים, כהגדרתם בחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע–2009;[6]

(6) מידע גנטי, כהגדרתו בחוק מידע גנטי, התשס"א–2000;[7]

(7) נתונים על מצבו הכלכלי של אדם, לרבות נתוני אשראי כהגדרתם בחוק נתוני אשראי, התשע"ו–2016;[8]

(8) מידע אישי שנקבעה לגביו חובת סודיות בדין;

(9) נתוני תעבורה ונתוני מיקום, כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007,[9] שיש בהם כדי ללמד על אחד מסוגי המידע המנויים בסעיפים קטנים (1)-(8);

(10) מידע אישי ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש.

דברי הסבר

הגדרת **"מידע אישי"** מחליפה את הגדרת "מידע" בסעיף 7 לחוק הגנת הפרטיות הקיים ומתייחסת לנתונים בלי קשר לפורמט שהם מוצגים בו. ההגדרה מאמצת את מסקנות ועדת שופמן[10] ואת הגדרת "מידע מזוהה" בחוק נתוני אשראי, התשע"ו-2016, ומיועדת ליצור תאימות עם חקיקה השוואתית כגון סעיף 4(1) ל-GDPR, סעיף 2(1) לחוק הפרטיות הקנדי (PIPEDA) וסעיף 6(1) לחוק הפרטיות האוסטרלי.

הגדרת **"מידע אישי מדגמי"** לקוחה מסעיף 23י להצ"ח תיקון מס' 13.

הגדרת **"מידע רגיש"** משקפת את ההבנה שמידע רגיש הוא מידע אישי שיש בו כדי לזהות מידע רגיש. ההגדרה שואבת השראה מסעיפים 7 לחוק הגנת הפרטיות הקיים, 23יט(א) להצ"ח תיקון מס' 13 ו-9 ל-GDPR. ס"ק (3) להגדרת "מידע רגיש" מצומצם לאמונתו הדתית של אדם ואינו מתייחס לכל אמונה של אדם כ"מידע רגיש"; ס"ק (8) מבהיר שמידע אישי המוגדר סודי, במסגרת החסיונות המקצועיים שהתפתחו בדין, הוא מידע רגיש, ועל כן העיבוד שלו כפוף להוראות הצעת החוק בנוגע למידע רגיש; ס"ק (9) מפנה לנתוני תעבורה ולנתוני מיקום כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007, שיש בהם כדי להיות מידע רגיש רק אם הם עלולים ללמד על סוגי מידע המנויים בס"ק (1)–(8) להגדרת "מידע רגיש".

"מסמך" – לרבות פלט כהגדרתו בחוק המחשבים;

"מעבד" – אדם המורשה על ידי בעל שליטה במידע, לפעול מטעמו בעיבוד של מידע אישי;

"נושא מידע" – אדם שנעשה עיבוד של מידע אישי על אודותיו;

"סיוע לרשות חוץ" – דרישת מידע אישי ומסמכים, עריכת חיפוש, תפיסת מסמכים, ניהול חקירה והעברת מידע אישי ומסמכים, לשם ביצוע ואכיפה של דיני הגנת הפרטיות במדינות חוץ ופיקוח על ביצועם;

"עיבוד" – אחת מהפעולות האלה:

(1) איסוף או תיעוד של מידע אישי בכל דרך, לרבות צילום, הקלטה, העתקה או השגת גישה אליו;

(2) ארגון, החזקה או אחסון של מידע אישי, לרבות הבנייה, שינוי, אחזור, ניתוח, איגום או הצלבה;

(3) גילוי או פרסום של מידע אישי, לרבות העברה, מכירה או העמדה לרשות הציבור;

"פקודת המעצר והחיפוש" – פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט–1969;[11]

דברי הסבר

הגדרת **"מסמך"** זהה להגדרה בסעיף 23ט בהצ"ח תיקון מס' 13.

הגדרת **"מעבד"** מחליפה את הגדרת "מחזיק, לעניין מאגרי מידע" בסעיף 3 לחוק הגנת הפרטיות הקיים ומבוססת על הגדרת "מעבד" בסעיף 4(8) ל-GDPR.

הנחת היסוד של הצעת החוק היא שאין עוד הצדקה לחובה לרישום מאגרי מידע הקיימת בחוק הגנת הפרטיות הקיים, ולכן גם הגדרת "מאגר מידע" ו"מחזיק" מיותרות.

הגדרת **"נושא מידע"** שואבת השראה מההתייחסות ל-"data subject" בסעיף 4(1) ב-GDPR כאל אדם שהמידע בעניינו מזהה או ניתן לזיהוי.

הגדרת **"סיוע לרשות חוץ"** מבוססת על הגדרת המונח בסעיף 54יא1 לחוק ניירות ערך, התשכ"ח–1968.

הגדרת **"עיבוד"** מחליפה את הגדרת "שימוש" בסעיף 3 לחוק הגנת הפרטיות הקיים, שאינה מתאימה למכלול הפעולות אשר ניתן לעשות במידע אישי בעולם דיגיטלי. בחרנו במונח "עיבוד" על פני המונח "שימוש" כדי לחדד את ההבחנה בין המונח השגור לפעולות המבוצעות על ידי משתמשי קצה (end-users) לבין הפעולות הנעשות במידע אישי. ההגדרה המוצעת כוללת רשימה סגורה של שלושה סוגי פעולות במידע אישי: איסוף, ניתוח והפצה; ההגדרה מאפשרת בכך הבנה ברורה יותר של סוגי השימושים ומדגישה שמדובר בטיפוסי פעולות שונים. בנוסף, מאחר שהליבה של תפיסת הפרטיות – שליטתו של האדם במידע אישי עליו, זהות ידועה של מבצע העיבוד והאם מדובר באדם או במכונה – אינה רלוונטית. ההגדרה נמצאת בהלימה עם סעיף 4(2) ל-GDPR.

הגדרת **"פקודת המעצר והחיפוש"** זהה להגדרה בסעיף 23ט בהצ"ח תיקון מס' 13.

"פרסום", לעניין מידע אישי – הבאת מידע אישי לידיעת הציבור בכל דרך;

"קטין" – אדם שטרם מלאו לו שמונה עשרה שנים;

"קשיש" – אדם שמלאו לו 65 שנים.

"ראש הרשות להגנת הפרטיות" – מי שהממשלה מינתה אותו, בהודעה ברשומות, לעמוד בראש הרשות להגנת הפרטיות;

"הרשות" או "הרשות להגנת הפרטיות" – הגוף הציבורי המפקח, האוכף והמסדיר את ההגנה על הזכות לפרטיות בהתאם להוראות חוק זה;

"רשות חוץ" – גוף המופקד על ביצוע ואכיפה של דיני הגנת הפרטיות במדינת חוץ ופיקוח על ביצועם;

"שלמות מידע" – שמירה על מהימנות ודיוק המידע האישי במהלך עיבודו, בלא ששונה או הושמד, שלא לפי להוראות חוק זה;

"תיעוד" – לעניין פסקה (1) שבהגדרת "עיבוד" ולעניין סעיפים 4(5) ו-65(א)(3)(ה) – לרבות קליטה או שימור של מידע אישי באמצעות חיישני מיקום, חיישני חום או כל אמצעי טכנולוגי אחר;

דברי הסבר

הגדרת **"פרסום"** מתייחסת לפרסום מידע אישי, שלא כמו השימוש במונח "פרסום" בהקשרים אחרים בהצעת החוק, ושואבת השראה מהגדרת המונח "פרסום" בסעיף 3 לחוק הגנת הפרטיות הקיים, שמפנה להגדרת המונח בסעיף 2 לחוק איסור לשון הרע, התשכ"ה–1965, ומדגישה ש"פרסום" אינו מוגבל לטכנולוגיה או למדיום מסוים. ההגדרה שואבת השראה גם מהגדרת המונחים "פרסום" ו"מפרסם" בחוק העונשין, התשל"ז–1977, שמדגישה את החשיבות שבחשיפת המידע לציבור, כולו או חלקו, כתנאי ל"פרסום".

הגדרת **"קטין"** זהה להגדרה המוצעת בסעיף 3 להצ"ח פרטיות קטינים, שמטרתה לשפר את הגנת הפרטיות על קטינים מצד הורי הקטין ומצד המדינה ולהתאימה למשפט ההשוואתי.[12]

הגדרת **"קשיש"** מבוססת על ההגדרה המקובלת בארץ ובעולם.

הגדרת **"ראש הרשות להגנת הפרטיות"** מחליפה את הגדרת ה"רשם" בסעיף 7 לחוק הגנת הפרטיות הקיים. ועדת שופמן (בשנת 2007[13]) ומשרד המשפטים (בתזכיר הצעת החוק לצמצום החובה לרישום מאגרי המידע משנת 2012[14]) המליצו לצמצם את החובה לרישום מאגרי מידע ולהמירה בחלופה טובה יותר – שתביא להפנמה אמיתית של חובות הגנת הפרטיות לפי החוק, כגון חובת הניהול התקין. ההמלצות התבססו על ההבנה שהתועלת בחובת הרישום קטנה, שהיא אינה מבטיחה בכלל ציות להוראות החוק ושהעיסוק של הרשות להגנת הפרטיות באכיפה של חובת הרישום גורם לבזבוז משאבים חשובים. לדעתנו, ביטול חובת הרישום עדיף על פני צמצומה, ולכן אנו מציעים לבטל לחלוטין את חובת הרישום. בעולם דיגיטלי שבו מידע אישי נאגם ונשמר כעניין שבשגרה, חובת רישום מטילה נטל רגולטורי בלתי סביר על כל אדם כמעט שמחזיק ברשותו רשימת שמות של לקוחות, צרכנים או משתמשים בשירות שהוא נותן. יתרה מזו, בעידן של היום תחימת החובות של הגנת הפרטיות לקיומו או להגדרתו של מקבץ הנתונים כמאגר מידע פוגעת בהיקף הגנת הפרטיות ובעוצמתה. לדעתנו, מערך הכלים החלופי להגנת הפרטיות במידע אישי המוצע בהצעת

החוק נותן מענה מקיף ומדויק יותר להגנה על הפרטיות משנותנת החובה לרישום מאגרי מידע.

עם ביטול ההתייחסות בהצעת החוק למאגרי מידע ולחובת רישום אין הצדקה להתייחסות לתפקיד ספציפי של רישום מאגרי מידע. תנאי הכשירות לתפקיד ראש הרשות להגנת הפרטיות מפורטים בסעיף 26 להצעת החוק.

הגדרת **"רשות חוץ"** מבוססת על הגדרת המונח בסעיף 54יא1(א) לחוק ניירות ערך, התשכ"ח–1968, ועל התאמתה להצעת החוק.

הגדרת **"שלמות המידע"** מבוססת על סעיף 7 לחוק הגנת הפרטיות הקיים ומותאמת לניסוח חקיקה מודרני. ההגדרה המוצעת משקפת את החשיבות שבשמירה על מהימנות ודיוק המידע האישי במהלך עיבודו ומתירה את שינויו לפי הצעת חוק זו, ולא על פי כל דין כפי שמתירה הגדרת המונח בחוק הקיים.

הגדרת **"תיעוד"** משקפת התאמה למציאות טכנולוגית מתפתחת שיש בכוחה לאפשר עיבוד מידע אישי בדרכים נוספות על צילום, הקבוע בחוק הגנת הפרטיות הקיים, למשל באמצעות חיישנים שונים. ההגדרה אינה מתייחסת ל"תיעוד" בסעיפים 22 ו-38(ב)(5) להצעת החוק העוסקים בתיעוד אירועי אבטחה.

סעיף 3: איסור פגיעה בפרטיות

לא יפגע אדם בפרטיות של זולתו אלא לפי הוראות חוק זה.

סעיף 4: פגיעה בפרטיות

פגיעה בפרטיות היא אחת מאלה:

(1) בילוש או התחקות אחרי אדם, העלולים להטרידו;

(2) האזנה האסורה על פי חוק;

(3) צפייה או עיון במידע אישי, לרבות קריאה או האזנה;

(4) צילום אדם כשהוא ברשות היחיד שלא לפי הוראות חוק זה;

(5) פרסום תצלומו של אדם או תוצר של תיעוד אודות אדם בנוגע למצבו או להתנהגותו ברשות הרבים, שלא לפי הוראות חוק זה, בנסיבות שבהן עלול הפרסום להשפילו או לבזותו, ובכלל זה לאחר אירוע פתאומי שבו נגרמה לאותו אדם פגיעה גופנית או נפשית, למעט פרסום תצלום או תוצר של תיעוד בלא השהיות בין רגע הצילום או התיעוד לרגע השידור בפועל שאינו חורג מהסביר באותן נסיבות;

(6) שימוש בשם אדם, בכינויו, בתמונתו או בקולו שלא לפי הוראות חוק זה;

(7) הפרה של חובת סודיות שנקבעה בדין או בהסכם לגבי ענייניו הפרטיים של אדם;

(8) עיבוד של מידע אישי על אודות אדם שלא לפי הוראות חוק זה.

סעיף 5: פרסום תצלומו של נפטר

שאלת קיומה של זכות לפרטיות לאחר המוות דורשת מחקר נפרד, שאינו בליבת עבודתנו הנוכחית לגיבוש הצעה לחוק הגנת פרטיות חדש ומעודכן.

דברי הסבר

סעיף 3: מבוסס על סעיף 1 לחוק הגנת הפרטיות הקיים. ואולם כחלק מהשינוי בתפיסת ההסכמה בהצעת החוק, הסכמה אינה הכלי היחיד להכשרת פגיעה בפרטיות. פגיעה בפרטיות תיעשה לפי הצעת חוק זו אך ורק בכפוף לסעיף 76 העוסק בשמירת הדינים.

סעיף 4: מבוסס על סעיף 2 לחוק הגנת הפרטיות הקיים ומציג רשימה סגורה של פגיעות אפשריות בפרטיות.

ס"ק (1) מבוסס על סעיף 2(1) בחוק הגנת הפרטיות הקיים, אגב מחיקת המילים "או הטרדה אחרת". מובהר שכל הטרדה, אף אם אינה מאיימת, למשל מעקב באמצעות מכשיר GPS סמוי שהנעקב אינו יודע בכלל על קיומו, עדיין עלולה לפגוע בפרטיותו של אדם.

ס"ק (2) וס"ק (4) זהים לסעיף 2(2) ו-2(3) לחוק הגנת הפרטיות הקיים (בהתאמה). האזנה שאינה אסורה על פי חוק האזנת סתר או צילום יכולה להיחשב פגיעה בפרטיות גם לפי ס"ק (8).

ס"ק (3) קובע שצפייה או עיון במידע אישי הם פגיעה בפרטיות, אף אם המידע אינו מפורסם וגם אם אין נעשות בו פעולות עיבוד אחרות.[15]

ס"ק (5) מחליף את הפגיעות המתוארות בסעיפים 2(4), 2(4א), ו-2(10) בחוק הגנת

הפרטיות הקיים ומוסיף פגיעה בפרטיות בעקבות "פרסום תוצר של תיעוד" (למשל, פרסום איכון הטלפון הסלולרי במועדון חשפנות) כשיש בפרסום כדי להשפיל או לבזות את נושא המידע.

ס"ק (6) מבוסס על סעיף 2(6) בחוק הגנת הפרטיות הקיים, אגב השמטת ההתייחסות ל"לשם ריווח", שאינה רלוונטית לשאלת הפגיעה בפרטיות

ס"ק (7) מאחד את הוראת סעיפים 2(7) ו-2(8) בחוק הגנת הפרטיות הקיים, אגב השמטת ההבהרה שההסכם יכול להיות במפורש או במשתמע, שאינה רלוונטית.

ס"ק (8) מחליף את סעיפים 2(9)-(11) לחוק הגנת הפרטיות הקיים ומסדיר אירועי פגיעה בפרטיות במידע עקב עיבוד מידע אישי בניגוד להוראות הצעת החוק. בכך מובהר שהסכמה אינה הכלי היחיד להכשרת פגיעה בפרטיות עקב עיבוד מידע אישי, בדומה להוראות ה-GDPR.

סעיף 2(5) לחוק הגנת הפרטיות הקיים לא נכלל בהצעת החוק המוצעת כאן, משום שהפגיעה בפרטיות המפורטת בו נכללת בס"ק (4), (6) ו-(7) המוצעים.

עקרון צמידות המטרה שבסעיף 2(9) לחוק הגנת הפרטיות הקיים מעוגן בסעיף 7 להצעת החוק.

פרק ב: הגנה על הפרטיות במידע אישי

סימן א׳: הוראות כלליות לעניין עיבוד מידע אישי

סעיף 6: פגיעה מותרת בפרטיות

(א) פגיעה בפרטיות מותרת בהתקיים אחד מאלה:

(1) היא נדרשת לשם מילוי התחייבויות הקבועות בהסכם שנושא המידע הוא צד לו, או לשם נקיטת צעדים המבוקשים על ידי נושא המידע לפני ההתקשרות בהסכם כאמור;

(2) היא נדרשת כדי להגן על אינטרס מהותי של בעל השליטה במידע או צד שלישי שאליו הועבר מידע אישי ובלבד שהיא אינה מבוצעת על ידי גוף ציבורי במסגרת ביצוע משימותיו על פי דין ושנושא המידע היה יכול לצפות באופן סביר בהתחשב בזמן ובנסיבות שתתרחש פגיעה כאמור.

(3) נושא המידע הסכים לפגיעה בפרטיות.

(ב) פגיעה בפרטיות בדרך של עיבוד מידע רגיש מותרת בהתקיים אחד מאלה:

(1) עיבוד המידע הרגיש נחוץ לצורך מימוש זכויותיו של נושא המידע, או לצורך מימוש זכויותיו או מילוי חובותיו של בעל שליטה במידע, במסגרת יחסי העבודה בין בעל שליטה במידע לנושא המידע ובהתאם לחוק המתיר עיבוד מידע רגיש לצורך מטרות אלו.

(2) עיבוד המידע הרגיש מידתי בהיקפו לצורך ביצוע מחקר סטטיסטי, מדעי או היסטורי שיש אינטרס ציבורי בביצועו.

(3) עיבוד המידע הרגיש נדרש כדי להגן על אינטרס מהותי של בעל השליטה במידע או צד שלישי שאליו הועבר המידע הרגיש ובלבד שעיבוד המידע הרגיש אינו מבוצע על ידי גוף ציבורי במסגרת ביצוע משימותיו על פי דין ושנושא המידע הסכים במפורש לעיבוד המידע הרגיש על אודותיו; היה העיבוד לפי פסקה (3) להגדרת עיבוד בסעיף 2 לחוק – נושא המידע הסכים במפורש קודם לביצוע עיבוד כאמור.

דברי הסבר

<u>סעיף 6:</u> מגדיר, בדומה לסעיפים 6 ו-9 ל-GDPR, את הבסיסים הלגיטימיים לפגיעה בפרטיות, לרבות בדרך של עיבוד מידע אישי או מידע רגיש.

התממה (אנונימיזציה) כשלעצמה אינה יכולה לשמש בסיס משפטי להתרת עיבוד מידע אישי,[16] כפי שעולה גם מסעיף 26 להקדמה ל-GDPR. הקביעה אם המידע המותמם אינו מאפשר זיהויו של נושא המידע תיעשה מתוך בחינת כל האמצעים שסביר שיעשה בהם שימוש לשם זיהוי חוזר של מידע לאחר התממתו. סבירות השימוש באמצעים תיקבע לפי מדדים אובייקטיביים, כגון עלות הזיהוי החוזר, פרק הזמן שיש להשקיע בביצוע זיהוי חוזר, הטכנולוגיה הזמינה בזמן עיבוד המידע המותמם והתפתחויות טכנולוגיות צפויות באותה עת.

ס״ק (א)(1) מבוסס על סעיף 6(1)(b) ל-GDPR ומתיר פגיעה בפרטיות כאשר היא נדרשת לשם מילוי מחויבות בהסכם

שנושא המידע הוא צד לו או כניסה להסכם כאמור.

ס"ק (א)(2) מבוסס על סעיף 6(1)(f) ל-GDPR וקובע שפגיעה בפרטיות מותרת כאשר היא נחוצה למימוש אינטרס מהותי של בעל השליטה במידע או של צד שלישי שאליו הועבר מידע אישי, ובלבד שסביר שנושא המידע צפה, בהתחשב בזמן ובנסיבות, שתתרחש פגיעה כאמור. למשל, כאשר הפגיעה בפרטיות היא בדרך של עיבוד מידע אישי שנחוץ לשם העברתו בין חברות קשורות או לשם אבטחת מידע אישי. הסעיף אינו חל על גוף ציבורי המחויב לפעול בהתאם להסמכה בדין ולא על פי מבחן סבירות ומימוש אינטרס מהותי שלו.

ס"ק (א)(3) מבוסס על סעיף 6(1)(a) ל-GDPR ומתיר פגיעה בפרטיות בהסכמת נושא המידע. הסעיף נמצא בסוף רשימת הבסיסים הלגיטימיים כדי לחדד את שינוי התפיסה שבעקבותיו ייטיב בעל שליטה במידע לבדוק אם עומדים לרשותו בסיסים לגיטימיים אחרים לפגיעה בפרטיות קודם שיפנה להכשרת הפגיעה בפרטיות של נושא המידע על ידי קבלת הסכמה.

ס"ק (ב)(1) מבוסס על סעיף 9(2)(b) ל-GDPR ומתיר פגיעה בפרטיות בדרך של עיבוד מידע רגיש, למשל נתונים ביומטריים, לצורך מימוש זכויותיהם של בעל שליטה במידע או של נושא מידע או לצורך מילוי חובותיו של בעל שליטה במידע במסגרת יחסי העבודה בין בעל שליטה במידע לנושא המידע.

ס"ק (ב)(2) שואב השראה מסעיף 9(2)(j) ל-GDPR ומתיר פגיעה בפרטיות בדרך של עיבוד מידע רגיש במידה הדרושה לצורך מחקר מדעי, סטטיסטי או היסטורי שיש אינטרס ציבורי בביצועו.

ס"ק (ב)(3) מתיר פגיעה בפרטיות בדרך של עיבוד מידע רגיש לפי האיזון שבין האינטרס המהותי של בעל שליטה במידע לאינטרס המהותי של נושא המידע, בדומה לס"ק (א)(2). הסעיף אינו מסתפק במבחן הציפייה הסבירה אלא מחייב קבלת הסכמה מפורשת של נושא המידע. רק כאשר מדובר בגילוי או בפרסום של מידע רגיש, כלומר עיבוד לפי פסקה (3) להגדרת המונח "עיבוד" בסעיף 2 להצעת החוק, נדרשת הסכמתו המפורשת של נושא המידע קודם לביצוע הגילוי או הפרסום – כדי להגביר את שליטתו של נושא המידע במידע רגיש עליו וכדי לוודא שהוא מודע למכלול פעולות העיבוד האפשריות במידע הרגיש עליו.

סעיף 7: דרישת קיום המטרה

לא יעבד בעל שליטה במידע מידע אישי אלא למטרה שלשמה נאסף או נמסר המידע האישי כמפורט בהודעה לפי סעיף 9 או למטרה הדומה למטרה שלשמה נאסף או נמסר מידע אישי; בבואו לבחון את קיומה של מטרה דומה כאמור, ישקול בעל שליטה במידע, בין השאר, את אלה:

(1) הקשר בין המטרה לשמה נאסף או נמסר מידע אישי לבין מטרת העיבוד שהוא מבקש לבצע;

(2) הנסיבות שבהן נאסף מידע אישי, קיומה של מערכת יחסים בין נושא המידע לבין בעל השליטה במידע ואת ציפייתו הסבירה של נושא המידע בנוגע לעיבוד נוסף של מידע אישי, מעבר למטרה לשמה נאסף או נמסר;

(3) האם המידע האישי כולל מידע רגיש;

(4) השלכות אפשריות של העיבוד הנוסף שהוא מבקש לבצע.

סעיף 8: הסכמה לעניין פגיעה בפרטיותו של קטין

(א) פגיעה בפרטיותו של קטין מתחת לגיל 13 לפי סעיף 6(א)(3) תיעשה אך ורק בהסכמת אחד מהוריו או אפוטרופוס שנתמנה לו כדין, או לפי הסמכה מפורשת בדין.

(ב) לא יעבד בעל שליטה מידע רגיש לפי סעיף 6(ב)(3) על אודות קטין מתחת לגיל 16 אלא בהסכמת אחד מהוריו או אפוטרופוס שנתמנה לו כדין, או לפי הסמכה מפורשת בדין.

(ג) ראש הרשות להגנת הפרטיות יקבע הנחיות בדבר הדרכים לאימות גילו של קטין ולווידוא קבלת הסכמת הוריו או האפוטרופוס שלו, כאמור בסעיפים קטנים (א) ו-(ב).

דברי הסבר

<u>סעיף 7:</u> מבוסס על סעיף 2(9) לחוק הגנת הפרטיות הקיים ושואב השראה מסעיפים 5(1) ו-6(4) ל-GDPR. הסעיף מעגן את דרישת קיום המטרה כתנאי להתרת פגיעה בפרטיות בדרך של עיבוד מידע אישי או מידע רגיש לפי סעיף 6 ומכיר בצורך בגמישות ובדינמיות בעיבוד של מידע אישי על ידי קביעת מנגנון להכרה בקיומן של מטרות דומות.

<u>סעיף 8:</u> שואב השראה מסעיפים 11ב להצ"ח פרטיות קטינים, 312.5 ל-COPPA האמריקני ו-8 ל-GDPR ומאזן בין הגנה על ילדים לבין ההכרה ביכולתם של ילדים מעל גיל 13 לקבל החלטות עבור עצמם בעניינים שתוצאותיהם אינן גורליות. מטרתו לתמרץ את חברות הטכנולוגיה ליישם טכנולוגיות מתאימות ולהבטיח בכך זהירות יתרה בעת פגיעה בפרטיות של קטינים, בין השאר בדרך של עיבוד מידע אישי ומידע רגיש עליהם.

בס"ק (א) קבענו שגיל 13 הוא הגיל הקובע לעניין הסכמה לעיבוד מידע אישי, בדומה ל-COPPA האמריקני – שהוא הדין הוותיק ביותר לעניין פגיעה בפרטיותם של קטינים בדרך של עיבוד מידע אישי עליהם. הגיל הקובע לעניין הסכמה לעיבוד מידע רגיש הוא 16 לפי ס"ק (ב). מגיל 16 ועד גיל 18 יחול ההסדר הקבוע בחוק הכשרות המשפטית והאפוטרופסות, התשכ"ו–1962,[17] הבוחן אם הסכמת הקטין לעיבוד מידע רגיש בנסיבות המקרה היא פעולה שדרכם של קטינים לעשות.

סעיף 9:
חובת מתן הודעה

(א) פניה לאדם לקבלת מידע אישי לשם עיבודו תלווה בהודעה בשפה ברורה בה נאסף המידע האישי, על כוונת בעל שליטה במידע לעבד את המידע האישי, תוך ציון כל אלה:

(1) שמו של בעל שליטה במידע, מענו ודרכי ההתקשרות עימו;

(2) אם חלה על אותו אדם חובה חוקית למסור את המידע האישי, או שמסירת המידע האישי תלויה ברצונו ובהסכמתו, ותוצאות אי הסכמה למסירת המידע האישי;

(3) המטרה אשר לשמה מבוקש העיבוד ונחיצות המידע האישי להגשמתה;

(4) זכות החזרה מהסכמה לעיבוד מידע אישי לפי סעיף 10, זכות העיון במידע האישי לפי סעיף 11, הזכות לקבלת הסבר לפי סעיף 12, זכות תיקון המידע האישי לפי סעיף 13, הזכות לניוד מידע אישי לפי סעיף 14 וזכות המחיקה של מידע אישי לפי סעיף 15, והדרכים למימוש הזכויות כאמור;

(5) למי יימסר המידע האישי ומטרות המסירה.

(ב) שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, יקבע את דרכי ההצגה של ההודעה לפי סעיף קטן (א), לרבות הצגתה במתכונת דיגיטלית, אופן ניסוחה ומידת הבלטתה בהתחשב, בין היתר, בקהלי היעד שלה.

דברי הסבר

<u>סעיף 9:</u> מבוסס על סעיף 11 בחוק הגנת הפרטיות הקיים, על סעיף 11א להצ"ח פרטיות קטינים ועל תיקונים שהציעה ועדת שופמן.[18]

סימן ב': זכויות נושא המידע

סעיף 10: זכות החזרה מהסכמה

(א) נושא המידע רשאי בכל עת לחזור בו מהסכמתו לפגיעה בפרטיותו לפי סעיף 6(א)(3) או 6(ב)(3) לעיל;

(ב) מבלי לגרוע מהוראות סעיף קטן (א) לעיל, קטין מעל גיל 13 רשאי לחזור בו מהסכמה לפי סעיף 6(א)(3) וקטין מעל גיל 16 רשאי לחזור בו מהסכמה לפי סעיף 6(ב)(3), בין שההסכמה ניתנה על ידו ובין שניתנה על ידי הורה או אפוטרופוס. היה הקטין מתחת לגיל הכשרות למתן הסכמה לפי סעיף 8 לעיל, רשאי אחד מהוריו או אפוטרופוס שנתמנה לו כדין, או לפי הסמכה מפורשת בדין לחזור מהסכמה כאמור.

(ג) חזר נושא המידע מהסכמה כאמור בסעיף קטן (א) או (ב), לא תפגע חוקיות עיבוד המידע שנעשה על בסיס הסכמת נושא המידע עד לאותו מועד.

דברי הסבר

סעיף 10: שואב השראה מסעיפים 7(3) ל-GDPR, 4.3.8 לחוק הפרטיות הקנדי (PIPEDA, Schedule 1, §4.3.8) ו-13ב להצ"ח פרטיות קטינים. הסעיף מעגן זכות מוחלטת לחזרה מהסכמה של כל אדם, לרבות קטין, במטרה להביא לשינוי תפיסתי ולהפסקת השימוש בהסכמה ככלי חסר משמעות וכ"מכבסה" להתחמקות מן הדרישות של חוק הגנת הפרטיות. על בעל שליטה במידע המבקש לפגוע בפרטיותו של אדם לבחון תחילה אם אחד מן הבסיסים הלגיטימיים, מלבד הסכמה, המפורטים בסעיף 6 להצעת החוק מתיר לו לבצע את הפגיעה האמורה. רק בהיעדרם של בסיסים לגיטימיים כאלה יבקש בעל שליטה במידע את הסכמתו של נושא המידע לפגיעה בפרטיות. במקרה כזה יהיה עליו להיערך מראש לאפשרות שנושא המידע יחזור בו מהסכמתו.

חזרת נושא המידע בו מהסכמתו לא תפגע בחוקיות של הפגיעה בפרטיות, שנעשתה על בסיס ההסכמה של נושא המידע עד למועד חזרתו מן ההסכמה. הפְסָקה של הפגיעה בפרטיות בגלל חזרה מהסכמה יכולה להתרחש רק כאשר אף אחד מן הבסיסים הלגיטימיים האחרים המפורטים בסעיף 6 להצעת החוק, מלבד הסכמת נושא המידע, אינו מתיר את הפגיעה בפרטיות המבוקשת על ידי בעל שליטה במידע.

סעיף 11: זכות עיון במידע אישי

(א) כל אדם זכאי לקבל בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, מבעל שליטה במידע מענה לשאלה האם הוא עושה פעולת עיבוד במידע אישי על אודותיו.

(ב) כל נושא מידע זכאי לקבל לידיו ולעיין בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, בכל אחד מאלה:

(1) עותק מהמידע האישי על אודותיו שנעשתה בו פעולת עיבוד;

(2) מידע בנושאים הבאים:

(א) מטרת עיבוד המידע האישי על אודותיו;

(ב) זהותם של מקבלי המידע האישי על אודותיו או הסוגים של מקבלי המידע האישי על אודותיו, שאליהם הועבר או יועבר המידע האישי, ובפרט בנוגע למקבלי מידע אישי במדינות חוץ ומקבלי מידע אישי שהם ארגונים בינלאומיים;

(ג) אם המידע האישי על אודותיו לא נאסף מהמבקש עצמו – זהותו של מקור המידע האישי;

(ג) הגיש נושא מידע בקשה לעיין במידע אישי על אודותיו כאמור בסעיף זה, יידע אותו בעל השליטה במידע על זכויותיו לפי סימן זה.

(ד) המידע האישי המבוקש וכן פרטי המידע הנוספים המבוקשים יימסרו לעיון המבקש בשפה שבה נאסף המידע האישי ובתבנית דיגיטלית מקובלת.

(ה) על אף האמור בסעיף זה, בעל שליטה במידע רשאי לסרב לבקשה לעיון, בהתקיים אחד מאלה:

(1) המידע האישי מתייחס למצבו הרפואי או הנפשי של מבקש העיון, ולדעת בעל השליטה במידע, עיון בו עלול לגרום נזק חמור לבריאותו הגופנית או הנפשית של המבקש או לסכן את חייו; במקרה זה ימסור בעל השליטה במידע את המידע האישי לרופא או לפסיכולוג מטעמו של המבקש;

(2) מתן זכות העיון כמבוקש עלול לדעת בעל השליטה במידע לפגוע בחיי אדם;

(3) מתן זכות העיון כמבוקש עלול לדעת בעל השליטה במידע לפגוע במידה העולה על הנדרש בזכויותיו של צד שלישי שאינו בעל השליטה במידע או המעבד;

(ו) אין בהוראות סעיף זה כדי לחייב למסור מידע אישי בניגוד לחיסיון שנקבע לפי כל דין, אלא אם כן המבקש הוא מי שהחיסיון נועד לטובתו; בפסקה זו, "דין" – לרבות הלכה פסוקה;

(ז) אין בהוראות סעיף זה כדי לחייב למסור מידע אישי בניגוד לדין.

(ח) אין בהוראות סעיף זה כדי לחייב למסור מידע אישי ממאגר מידע המוחרג מסיבות ביטחוניות. **הנושא מצריך דיון נפרד, שאינו בליבת עבודתנו הנוכחית לגיבוש הצעה לחוק הגנת פרטיות חדש ומעודכן.**

דברי הסבר

סעיף 11: מבוסס על סעיפים 13(א) לחוק הגנת הפרטיות הקיים ושואב השראה מסעיפים 4.9 ל-PIPEDA בקנדה ו-15 ל-GDPR.

ס"ק (א) מתייחס ל"אדם" ולא ל"נושא מידע", שכן בשלב זה עדיין לא בטוח שבעל שליטה במידע אכן מעבד מידע אישי על הפונה.

ס"ק (ב)(2)(ג) מבוסס על סעיף 15(1)(g) ל-GDPR ומחיל את זכות העיון גם על מקור המידע האישי, כאשר זה לא נאסף מנושא המידע עצמו. על מנת להימנע מפגיעה בעבודה עיתונאית ובחיסיון של מקורות עיתונאיים, ס"ק (ו) – המבוסס על סעיף 13(ג1) לחוק הגנת הפרטיות הקיים ועל סעיף 3(ד)(7) לחוק סדר הדין הפלילי[19] – מחריג מידע אישי שיש בגילויו כדי לפגוע בחיסיון על פי דין, לרבות חיסיון עיתונאי.

גביית תשלום בעבור מימוש זכות העיון תיעשה מכוח הסמכות הכללית לקביעת תשלומים בעבור מימוש זכות מזכויותיו של נושא המידע לפי סעיף 16(ב) להצעת החוק.

ס"ק (ד) מבוסס על סעיף 13(ב) לחוק הגנת הפרטיות הקיים. ואולם כדי להימנע מהטלת עלויות כבדות על בעל השליטה במידע או המעבד הסעיף אינו דורש לספק את המידע האישי באחת משלוש השפות – עברית, ערבית או אנגלית – אלא מסתפק בדרישה שהמידע האישי יימסר לעיון בשפה שבה הוא נאסף מלכתחילה ובתבנית דיגיטלית שמקובלת במשק באותה העת.

ס"ק (ה)(1) מבוסס על סעיף 13(ג) לחוק הגנת הפרטיות הקיים, בשינויים המתחייבים מהסרת ההתייחסות למאגרי מידע בהצעת החוק. הסייגים בס"ק (ה)(1) ו-(ה)(2) שואבים השראה גם מסעיף 13(ד) לחוק זכויות החולה, התשנ"ו–1996, המתיר למטפל להימנע ממסירת מידע רפואי למטופל אם מסירתו עלולה לגרום נזק חמור לבריאותו הגופנית או הנפשית של המטופל.

הסייגים בס"ק (ה)(2) ו-(ה)(3) שואבים השראה מסעיף 15(4) ל-GDPR, אך צמצמנו את החריג כך שהוא אינו מתיר לבעל השליטה במידע לסרב לבקשת העיון בנימוק שהעיון עלול לפגוע בזכויותיו של בעל השליטה עצמו, למשל בזכויות הקניין הרוחני שלו או של המעבד.

מובהר שבנסיבות המפורטות בס"ק (ו) ו-(ז), כאשר חל על המידע האישי חיסיון או כאשר מסירתו היא בניגוד לדין, אין לבעל שליטה במידע שיקול הדעת אם להתיר את העיון אם לאו, בניגוד לשיקול הדעת הנתון לו ביישום החריגים לזכות העיון המפורטים בסעיף קטן (ה).

ס"ק (ח) מבוסס על סעיף 13(ה) לחוק הגנת הפרטיות הקיים. הנושא מצריך דיון נפרד, שאינו בליבת עבודתנו הנוכחית לגיבוש הצעה לחוק הגנת פרטיות חדש ומעודכן.

סעיף 12: זכות לקבל הסבר

קיבל בעל שליטה במידע החלטה שיש לה השלכה משמעותית על זכות או חובה על פי דין של נושא מידע, המבוססת, במלואה או ברובה, על עיבוד מידע אישי על אודותיו באמצעות תהליכים ואמצעים אוטומטיים, יהיה נושא המידע זכאי לקבל מבעל שליטה במידע הסבר בהיקף סביר ובשפה מובנית על אופן קבלת ההחלטה.

דברי הסבר

סעיף 12: שואב השראה מפרשנות שניתנה בסעיף 71 להקדמה ל-GDPR לסעיף 22 ל-GDPR. על פי פרשנות זו – כחלק מזכותו של נושא המידע שלא תתקבל החלטה בעלת השלכות משפטיות או משמעותיות אחרות עליו, אשר מבוססת רק על עיבוד אוטומטי של מידע אישי – נתונה לנושא המידע גם הזכות לקבל מבעל שליטה במידע הסבר שיכלול את פירוט אופן קבלת החלטה המבוססת על ניתוח אוטומטי של המידע האישי עליו.

מאחר שתכליתה של הזכות של נושא המידע להתנגד לקבלת החלטה כאמור היא הזכות לכבוד ולא הזכות לפרטיות, ומשום שזכותו של נושא המידע להתנגד כאמור מטילה נטל לא מוצדק על חברות מסחריות – שיחויבו להותיר מעורבות אנושית בתהליכים שניתן לייעלם ולבצעם על ידי שימוש בטכנולוגיה בלבד – סעיף 12 להצעת החוק מאמץ רק את הזכות של נושא המידע לקבל הסבר מידתי מבחינת היקפו כאשר ההחלטה בעניינו משפיעה משמעותית על זכות או חובה על פי דין של נושא המידע וכאשר היא מבוססת במלואה או ברובה על עיבוד מידע אישי על נושא המידע באמצעות תהליכים אוטומטיים או אמצעים אוטומטיים.

מטרת הזכות לקבל הסבר נועדה למנוע מצב קפקאי שבו מתקבלת החלטה בעניינו של נושא המידע שאינה ברורה לו ואין ביכולתו להבינה ושיש לה השפעה משמעותית על זכות או חובה שלו על פי דין. בדרך זו תחוזק השקיפות בפעולותיהם של בעלי שליטה במידע, והם יחויבו לשקול, ואף להנגיש, את הפרמטרים מתוך המידע האישי שנעשה בהם שימוש בעת קבלת החלטה בעניינו של אדם.

סעיף 13: זכות תיקון מידע אישי

(א) נושא מידע שעיין במידע אישי על אודותיו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל השליטה במידע בבקשה לתקן את המידע האישי.

(ב) הוגשה בקשה כאמור בסעיף קטן (א), על בעל שליטה במידע לנקוט את אחת מהפעולות הבאות, בהתחשב במטרה שלשמה בוצע עיבוד המידע האישי וסוג המידע האישי שבו מדובר:

(1)למחוק את המידע האישי, כולו או חלקו;

(2)לתקן את המידע האישי;

(3)להשלים את המידע האישי שבשליטתו;

(ג) בעל השליטה במידע יודיע על הפעולה שנקט לפי לסעיף זה, בתוך 30 יום ממועד נקיטת הפעולה, לכל מי שקיבל ממנו את המידע האישי במהלך תקופה של שנתיים שקדמו למועד קבלת בקשת התיקון.

(ד) על אף האמור בסעיף זה, מצא בעל שליטה במידע שהמידע האישי שבשליטתו נכון, מעודכן ומלא, רשאי הוא לסרב לבקשה כאמור בסעיף קטן (א) ובלבד שינמק את סירובו בכתב.

(ה) מעבד חייב למחוק, לתקן או להשלים את המידע האישי, אם בעל שליטה במידע הסכים לתיקון המבוקש או שבית המשפט ציווה על התיקון.

דברי הסבר

<u>סעיף 13:</u> מבוסס על סעיף 14 לחוק הגנת הפרטיות הקיים ושואב השראה מסעיפים 16 ל-GDPR ו-13 לחוק הפרטיות האוסטרלי. הסעיף מוגבל, לפי ס"ק (א), לתיקון מידע אישי בלבד. נושא המידע אינו רשאי לבקש את מחיקתו, כלשון סעיף 14(א) לחוק הגנת הפרטיות הקיים. זכות המחיקה מעוגנת בנפרד בסעיף 15. לבעל שליטה במידע מסור שיקול הדעת, לפי ס"ק (ב), אם לתקן, להשלים או למחוק את המידע האישי, הכול בהתאם למטרת העיבוד וסוג המידע האישי.

ס"ק (ג) מבוסס על סעיף 14(ב) לחוק הגנת הפרטיות הקיים, אך קובע פרק זמן של כשנתיים למתן הודעה לצדדים שלישיים שאליהם העביר בעל שליטה במידע את המידע האישי.

בעל שליטה במידע שמצא שהמידע שברשותו מלא, מעודכן ונכון ללא התיקון המבוקש, רשאי לפי ס"ק (ד), שמבוסס על סעיף 14(ג) לחוק הגנת הפרטיות, לסרב לבקשת תיקון מנימוקים שיירשמו.

ס"ק (ה) מבוסס על סעיף 14(ד) לחוק הגנת הפרטיות הקיים ומחייב את המעבד לפעול בהתאם לפעולות שנקט בעל השליטה במידע לפי ס"ק (ב).

סעיף 14: הזכות לניוד מידע אישי

(א) כל נושא מידע זכאי, בהתאם לבקשה שהגיש לבעל שליטה במידע, שבשליטתו המידע האישי על אודותיו, לקבל לידיו מבעל שליטה במידע, את המידע אישי כאמור, בתבנית דיגיטלית מקובלת, ולהעבירו, על פי שיקול דעתו, בעצמו או לפי הוראת סעיף קטן (ד), לכל בעל שליטה במידע אחר (להלן – הזכות לניוד מידע אישי).

(ב) הזכות לניוד מידע אישי חלה על מידע אישי שעובד לפי הוראות סעיף 6 על אודות נושא המידע.

(ג) הזכות לניוד מידע אישי אינה חלה על מידע אישי שבעל שליטה במידע או המעבד הסיקו באמצעות עיבוד שנעשה לפי הוראות סעיף 6.

(ד) הוגשה בקשה לניוד מידע אישי כאמור בסעיף קטן (א), יעביר בעל שליטה במידע את המידע האישי על אודות מבקש הניוד לבעל שליטה במידע המבוקש על ידו, בהתאם לבקשה ובכפוף למגבלות טכנולוגיות. בעל שליטה במידע שאליו ינויד המידע האישי על פי סעיף זה, יהיה כפוף להוראות חוק זה במלואן.

(ה) בעל שליטה במידע שהוגשה לו בקשה לנייד מידע אישי כאמור בסעיף קטן (א), יידע את מבקש הניוד שאין בניוד המידע האישי לפי סעיף זה כדי להביא להפסקת עיבוד מידע אישי על אודותיו, וכי יש באפשרותו של מבקש הניוד לחזור בו מהסכמתו, במידה שניתנה, לפי סעיף 10 לחוק, או לפנות אל בעל השליטה במידע בבקשה למחוק את המידע האישי על אודותיו לפי סעיף 15.

(ו) על אף האמור בסעיף זה, בעל שליטה במידע רשאי לסרב לבקשה לפי סעיף קטן (א), אם לדעתו יש בניוד המידע האישי בהתאם לבקשה כדי לפגוע במידה העולה על הנדרש בזכויותיו של צד שלישי או במילוי חובותיו לפי דין.

(ז) שר המשפטים רשאי לקבוע בתקנות סוגים של בעלי שליטה במידע שהוראות סעיף זה לא יחולו עליהם.

דברי הסבר

<u>סעיף 14:</u> שואב השראה מסעיף 20 ל-GDPR ומעגן את זכותו של נושא המידע לנייד מידע אישי עליו לבעלי שליטה במידע נוספים לפי שיקול דעתו. מטרת זכות הניוד היא לחזק את השליטה של נושא המידע במידע האישי עליו, לשכלל את השוק על ידי עידוד התחרות בין בעלי שליטה שונים במידע, להקטין את תלותם של נושאי מידע בפלטפורמות שירותי מידע אחת או בבעל שליטה אחד במידע ולמנוע את הגבלתם לאותה הפלטפורמה או לאותו בעל שליטה במידע.

לפי ס"ק (א), על בעל שליטה במידע לנייד את המידע האישי שיש ברשותו על מבקש הניוד למבקש הניוד עצמו או לבעל שליטה במידע אחר, על פי בקשת מבקש הניוד. ניוד המידע האישי ייעשה בתבנית דיגיטלית המקובלת במשק באותה העת. כן נדרש בס"ק (ד) שהניוד יהיה אפשרי מבחינה טכנית, כלומר שאפשר להעביר את המידע האישי בדרך מאובטחת ובתנאי שלבעל השליטה במידע המקבל יש היכולות הטכניות לקבל את המידע האישי.

לפי ס"ק (ב), המידע האישי שזכות הניוד חלה עליו הוא כל מידע אישי שעובד לפי ההוראות שבסעיף 6 להצעת החוק. הסעיף מרחיב בכך את זכות הניוד מזו הקבועה בסעיף 20 ל-GDPR, המצומצמת רק למידע אישי שעובד בהסכמת נושא

המידע. ההרחבה נחוצה על מנת להגשים את מטרת זכות הניוד. עם זאת, לפי ס"ק (ג), המבוסס על סעיף 20(1) ל-GDPR, זכות הניוד חלה רק על המידע האישי הגולמי שעובד לפי סעיף 6. זכות הניוד לא חלה על מידע אישי שבעל השליטה במידע או שהמעבד הסיקו אותו באמצעות עיבוד מידע אישי לפי סעיף 6 להצעת החוק.

לפי ס"ק (ה), בעל שליטה במידע שהניוד התבקש ממנו צריך ליידע את נושא המידע מבקש הניוד שאין בניוד המידע האישי כדי להביא להפסקת עיבודו או למחיקתו. המטרה של חובת היידוע היא למנוע היווצרות רושם מוטעה שלפיו המידע האישי אינו נמצא עוד ברשותו של בעל השליטה במידע.

ס"ק (ו) שואב השראה מסעיף 20(4) ל-GDPR ומתיר לבעל שליטה במידע לסרב לבקשת ניוד כאשר זכות הניוד עלולה לפגוע במידה העולה על הנדרש בזכויותיהם של צדדים שלישיים או במילוי חובותיו של בעל השליטה במידע לפי דין.

ס"ק (ז) מסמיך את שר המשפטים לקבוע שבעלי שליטה במידע מסוימים יוחרגו מתחולת הסעיף מסיבות הקשורות בגודלם, במשך הזמן שחלף מרגע היווסדם או בנתח השוק שהם מחזיקים. המטרה היא להתמודד עם החשש שזכות הניוד עלולה לפגוע קשות דווקא בעסקים קטנים ובינוניים, שיתקשו להתמודד עם העברת מידע אישי מהם בשלבי הפעילות הראשונית שלהם, ולהביא בסופו של דבר להיחלשות התחרות ולהתחזקות החברות הגדולות.

סעיף 15: זכות המחיקה של מידע אישי

(א) כל נושא מידע זכאי לדרוש מבעל שליטה במידע למחוק מידע אישי על אודותיו בהתקיים אחד מאלה:

(1) המידע האישי אינו נחוץ עוד למילוי המטרה שלשמה נאסף;

(2) נושא המידע חזר בו מהסכמתו לעיבוד מידע אישי לפי סעיף 10 ולא מתקיים אף אחד מהתנאים לפי סעיף 6(א)(1)-(2) או 6(ב)(1)-(2) המתירים את המשך עיבוד המידע האישי;

(3) עיבוד המידע האישי נעשה בניגוד להוראות חוק זה.

(ב) בעל שליטה במידע שהתבקש למחוק מידע אישי לפי סעיף קטן (א), ינקוט את הצעדים הסבירים בנסיבות העניין ובהתחשב בטכנולוגיה הקיימת באותה עת ובעלותה, על מנת למחוק את המידע האישי שבשליטתו, ואם העביר את המידע האישי - ליידע כל בעל שליטה אחר אליו העביר את המידע האישי שנושא המידע ביקש למחוק את המידע האישי וכל קישור אליו או העתק שלו;

(ג) על אף האמור בסעיף זה, בעל שליטה במידע רשאי לסרב לבקשת מחיקה לפי סעיף קטן (א), בהתקיים אחד מאלה:

(1) מחיקת המידע האישי תפגע במידה העולה על הנדרש בזכות לחופש ביטוי או בזכות הציבור לדעת;

(2) עיבוד המידע האישי דרוש לשם מילוי חובה חוקית;

(3) מחיקת המידע האישי תפגע במידה העולה על הנדרש ביכולתו של בעל השליטה במידע או המעבד להתגונן בתביעות משפטיות, או לבצע משימה המוטלת עליו למטרות אירכוב, מחקר מדעי, מחקר סטטיסטי שיש אינטרס ציבורי בביצועם.

דברי הסבר

סעיף 15: שואב השראה מסעיף 17 ל-GDPR ומעגן את זכות המחיקה, המכונה גם "הזכות להישכח".

ס"ק (א) מעגן את זכות נושא המידע, לרבות קטין, לדרוש למחוק מידע אישי עליו במקרים המנויים בסעיף. בה בעת, ס"ק (ב) מכיר בקושי האפשרי ליישם את זכות המחיקה ובסכנה שזכות זו עלולה להתברר בעתיד כנטל בלתי סביר על חברות הטכנולוגיה. משום כך, מימוש זכות המחיקה על ידי בעל שליטה במידע, כלומר מחיקת המידע האישי ויידוע בעלי שליטה נוספים שאליהם העביר את המידע האישי, תיעשה לפי מבחן הסבירות ולפי נסיבות העניין, הטכנולוגיה הקיימת באותה העת ומחירה.

ס"ק (ג) מונה את הנסיבות שבהן יותר לבעל שליטה במידע לסרב לבקשת מחיקה.

סעיף 16: מימוש זכויות נושא המידע

(א) בעל שליטה במידע ינקוט אמצעים סבירים כדי לוודא שהמבקש לחזור בו מהסכמתו לפי סעיף 10, לעיין במידע אישי לפי סעיף 11, לקבל הסבר לפי סעיף 12, לתקן מידע אישי לפי סעיף 13, לנייד מידע אישי לפי סעיף 14 או למחוק מידע אישי לפי סעיף 15 (להלן – "זכויות נושא המידע"), הוא אכן נושא המידע, בטרם מתן מענה לבקשה.

(ב) על בעל שליטה במידע לאפשר מימוש זכויות נושא המידע בכתב או בפורמט דיגיטלי ובתבנית מקובלת בתוך 14 ימים ממועד קבלת בקשה למימוש זכות מזכויות נושא המידע. בגין מימוש זכות מזכויות נושא המידע רשאי בעל שליטה במידע לגבות סכום שלא יעלה על ____ שקלים חדשים.

(ג) פנה נושא המידע למעבד בבקשה למימוש זכות מזכויות נושא המידע, יעביר לו המעבד בתוך 14 ימים מיום קבלת הבקשה את שם בעל השליטה במידע שבשליטתו מצוי המידע האישי נשוא הפנייה ואת דרכי הפנייה אליו. אין בהוראת סעיף קטן זה כדי לחייב למסור מידע אישי בניגוד לחיסיון שנקבע לפי כל דין, אלא אם כן המבקש הוא מי שהחיסיון נועד לטובתו. בסעיף קטן זה, "דין" – לרבות הלכה פסוקה.

(ד) סירב בעל שליטה במידע לבקשת נושא מידע למימוש זכות מזכויות נושא המידע, כאמור בסעיפים 11(ה)-(ח), 13(ד), 14(ו), או 15(ג), יודיע על כך למבקש בכתב או בפורמט דיגיטלי ובתבנית מקובלת בתוך 14 ימים ממועד קבלת הבקשה למימוש זכות מזכויות נושא המידע, תוך פירוט הנימוקים לסירוב.

דברי הסבר

<u>סעיף 16:</u> ס"ק (א) שואב השראה מחובת הזהירות הקבועה בסעיף 45 לחוק הפרטיות בניו זילנד, שלפיה טרם מתן מענה לזכות העיון והתיקון יש לוודא שהמבקש הוא אכן נושא המידע.

ס"ק (ב) מבוסס על סעיפים 13(ד) ו-29א(ד) לחוק הגנת הפרטיות הקיים ועל תקנה 6 לתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי דין בערעור על סירוב לבקשת עיון), התשמ"א–1981, וקובע פרקי זמן למימוש כל אחת מן הזכויות של נושא המידע ומנגנון לגביית תשלום בגין מימושן.

ס"ק (ג) מבוסס על סעיף 13א(2) לחוק הגנת הפרטיות הקיים, אך תחולתו רחבה יותר וחלה על כלל הזכויות של נושא המידע. עם זאת, הסעיף מאפשר למעבד להימנע ממענה שנדרש על פי הסעיף אם המענה יביא לחשיפת מידע שחל עליו חיסיון, למשל כאשר המעבד הוא חוקר פרטי או עיתונאי עצמאי, עצם ההעברה של פרטי יצירת הקשר עם בעל שליטה במידע יכולה להיחשב הודאה בכך שהמעבד אכן מעבד מידע אישי על נושא המידע.

ס"ק (ד) מחייב את בעל השליטה במידע לתת הודעת סירוב בתגובה לבקשת נושא המידע לממש זכות מזכויות נושא המידע.

סעיף 17: תובענה לבית המשפט

על סירובו של בעל שליטה במידע לבקשת נושא מידע למימוש זכות מזכויות נושא המידע, כאמור בסעיפים 11(ה)-(ח), 13(ד), 14(ו), או 15(ג), רשאי נושא המידע להגיש תובענה לבית המשפט באופן ובדרך שנקבעו בתקנות.

סימן ג': חובות בעל השליטה במידע והמעבד

סעיף 18: מעבד המידע

(א) מעבד יפעל על פי הוראות חוק זה ועל פי הנחיות בעל שליטה במידע.

(ב) על בעל שליטה במידע להבטיח שהמעבד נקט את כל האמצעים הדרושים לעיבוד מידע אישי וכיבוד זכויותיו של נושא המידע לפי חוק זה.

סעיף 19: עיצוב לפרטיות

(א) בעל שליטה במידע יתכנן, יעצב ויפעיל, ככל שניתן, באמצעות הטמעת אמצעים טכנולוגיים וכן כללים פנים-ארגוניים, מערכות לעיבוד של מידע אישי, באופן שיבטיח את התאמתן להוראות חוק זה.

(ב) תכנון, עיצוב והפעלה של מערכות לעיבוד של מידע אישי כאמור בסעיף קטן (א), ייעשו בהתחשב בכל אלה: הטכנולוגיות הזמינות באותה עת ועלותן; אופי העיבוד של המידע האישי, וכן היקפו ומטרתו של העיבוד; והסכנות הצפויות לפגיעה בפרטיותו של נושא המידע עקב עיבוד המידע האישי על אודותיו.

דברי הסבר

סעיף 17: מבוסס על סעיף 15 לחוק הגנת הפרטיות הקיים ומעגן את הזכות לערער לבית המשפט על החלטת בעל שליטה לסרב לכל אחת מזכויות נושא המידע.

סעיף 18: שואב השראה מסעיפים 29 ו-28(1) ל-GDPR ומיועד להבהיר שעל בעל שליטה במידע להבטיח שמעבד מידע אישי שעימו הוא מתקשר נוקט את כל האמצעים הנדרשים, בכלל זה אמצעים טכניים וארגוניים, כדי לכבד את זכויותיו של נושא המידע לפי הצעת החוק ולהבטיח שעיבוד המידע האישי ייעשה בהתאם להוראות הצעת החוק.

סעיף 19: שואב השראה מסעיף 25 ל-GDPR. מטרתו להטיל על בעל שליטה במידע את החובה להבטיח הטמעת אמצעי הגנה על פרטיות במידע אישי באופן יזום מניעתי – החל בשלבי התכנון והפיתוח של המערכות לעיבוד מידע אישי, עבור בהטמעתן וכלה בהפעלתן – כל זה באמצעות אימוץ הדרישות ל"פרטיות כברירת מחדל" ("privacy by default") ול"עיצוב לפרטיות" ("privacy by design").

לדוגמה, על בעל שליטה במידע למזער ככל האפשר את עיבוד המידע האישי, לפעול להתממת מידע אישי, לעבד מידע אישי בשקיפות, לאפשר לנושא המידע לנטר את עיבוד המידע האישי עליו ולשפר בתכיפות גבוהה את אמצעי האבטחה. בעיצוב, בתכנות ובבחירת אפליקציות, שירותים או מוצרים המבוססים על עיבוד מידע אישי, בעל השליטה במידע או המעבד צריכים להתחשב בזכויותיו של נושא המידע ולוודא שהעיצוב, התכנות, האפליקציות, השירותים או כל טכנולוגיה אחרת המשמשת אותם לעיבוד מידע אישי מסייעים או אינם פוגעים במילוי חובותיהם לפי הצעת החוק.

סעיף 20: תסקיר השפעה על הפרטיות

(א) בעל שליטה במידע יכין תסקיר השפעה על הפרטיות (בסעיף זה – תסקיר ההשפעה על הפרטיות) כאשר בכוונתו לעשות אחד מאלה:

(1) לבצע עיבוד מידע אישי, שבהתחשב בהיקפו ומטרתו, סביר שיביא לפגיעה בזכויות צדדים שלישיים;

(2) לבצע עיבוד מידע אישי בהיקף נרחב העשוי להשפיע על מספר רב של נושאי מידע;

(3) לבצע עיבוד מידע אישי באופן אוטומטי או בעיקר אוטומטי לשם הערכת מאפייני האישיות של נושא המידע וקבלת החלטות בעלות השלכות משמעותיות על זכויות או חובות לפי דין של נושא המידע;

(4) לבצע עיבוד מידע רגיש בהיקף נרחב;

(ב) תסקיר ההשפעה על הפרטיות יכלול התייחסות, בין השאר, להיקף המידע האישי הנאסף, לעיצוב לפרטיות לפי סעיף 19 ולאמצעי אבטחת מידע אישי שינקטו על ידי בעל שליטה במידע לפי סעיף 21.

(ג) תסקיר ההשפעה על הפרטיות לפי סעיף קטן (א) יוכן לפני תחילת העיבוד של המידע האישי ולפני האימוץ של טכנולוגיה חדשה לעיבוד המידע אישי, וכן אחת ל-18 חודשים לפחות.

סעיף 21: אבטחת מידע אישי

בעל שליטה במידע או מעבד יהיו אחראים, ביחד ובנפרד, לאבטחת המידע האישי שבשליטתם או ברשותם וינקטו אמצעים סבירים לצורך אבטחתו, בהתאם לתקן מקובל של אבטחת מידע ולעלותו הכספית, ובהתחשב בסוג המידע האישי, מטרת העיבוד, היקפו, הסכנות הצפויות לפגיעה בפרטיות עקב שימוש לרעה בו, אובדן, שינוי, גילוי, גישה בלתי מורשית אליו או מחיקה בלתי חוקית או מקרית שלו.

דברי הסבר

<u>סעיף 20:</u> מעגן חובה כללית על בעל שליטה במידע לערוך סקר סיכונים לפגיעה בפרטיות. חובה דומה נמצאת כיום בתקנה 5 לתקנות אבטחת מידע, אך היא מוגבלת רק למאגרי מידע שנדרשת בעניינם רמת אבטחה גבוהה.[20] בעתיד נפעל להצעת תיקון לתקנות אבטחת מידע על פי המוצע בסעיף זה. ואולם לעת עתה – כדי להציג את התמונה המלאה של מכלול התיקונים המוצעים – בחרנו להציג את הסעיף הזה כחלק מהצעת החוק.

ס"ק (א) שואב השראה מסעיפים 35(1) ו-35(3) ל-GDPR. הסעיף מעגן חובה כללית על בעל שליטה במידע לערוך תסקיר השפעה על הפרטיות בהתאם לפעולות העיבוד שברצונו לעשות, ולפי מבחן סבירות שיתחשב במטרת העיבוד, בהיקפו ובסוג המידע האישי המעובד.

<u>סעיף 21:</u> מבוסס על סעיף 17 לחוק הגנת הפרטיות הקיים ושואב השראה מסעיפים 32 ל-GDPR, 4.7 לנספח 1 לחוק הפרטיות הקנדי, 11.1 לחוק הפרטיות האוסטרלי ו-5 לחוק הפרטיות הניו זילנדי. הסעיף מעגן חובת אבטחת מידע כללית לפי תקן מקובל של אבטחת מידע ולפי מבחן סבירות שיתחשב גם בסוג המידע האישי, במטרת העיבוד והיקפו ובסכנות הצפויות לפגיעה בפרטיות. החובה לאבטחת מידע כוללת גם שמירה על הסודיות של מידע אישי. בעתיד נפעל להצעת תיקון לתקנות אבטחת מידע על פי המוצע בסעיף זה.

סעיף 22: תיעוד ודיווח על אודות אירוע אבטחה

(א) בעל שליטה במידע אחראי לתיעוד כל אירוע אבטחה שאירע בנוגע למידע האישי שבשליטתו; תיעוד כאמור יבוסס, ככל האפשר, על רישום אוטומטי.

(ב) בעל שליטה במידע ידווח לרשות להגנת הפרטיות על אירוע אבטחה תוך זמן סביר מהמועד שנודע לו על התרחשותו, בהתקיים אלה:

(1) אירוע האבטחה הוביל לעיבוד לא מורשה של מידע אישי או לנסיבות שסביר להניח שיגרמו לעיבוד לא מורשה של מידע אישי;

(2) סביר להניח שאירוע האבטחה יגרום נזק חמור לנושא המידע;

(3) בעל השליטה במידע אינו יכול למנוע את הנזק החמור לנושא המידע באמצעות נקיטת פעולה מתקנת;

בסעיף זה, "פעולה מתקנת"– פעולה שעל בעל שליטה במידע לנקוט לבירור הסיבות שהובילו לאירוע האבטחה, למניעת הישנות אירוע האבטחה ולמיזעור השלכות אירוע האבטחה על זכויות של נושא המידע לפי חוק זה.

(ג) לאחר הדיווח לרשות להגנת הפרטיות כאמור בסעיף קטן (ב), יודיע בעל שליטה במידע לנושא המידע, תוך זמן סביר, על אירוע האבטחה, אלא בהתקיים אחד מאלה:

(1) מתן ההודעה עלול להביא לחשיפת מידע אישי שחל לגביו חיסיון לפי כל דין, אלא אם כן נושא המידע הוא מי שהחיסיון נועד לטובתו; בפסקה זו, "דין" – לרבות הלכה פסוקה;

(2) מתן הודעה כאמור לכל נושא מידע העלול להיפגע מאירוע האבטחה מטיל על בעל שליטה במידע נטל בלתי סביר; במקרה זה, יפרסם בעל שליטה במידע הודעה לכלל הציבור על אודות אירוע האבטחה.

(ד) אירע אירוע אבטחה, יודיע על כך המעבד לבעל שליטה במידע באופן מיידי.

(ה) שר המשפטים יקבע תקנות בעניינים הבאים:

(1) סוגי אירועי אבטחה וסוגי בעלי שליטה במידע הפטורים מחובת הדיווח לפי סעיף קטן (ב);

(2) אופן מתן ההודעות לפי סעיפים קטנים (ב) עד (ד) ותוכנן.

(3) מהן הפעולות המתקנות שעל בעל שליטה במידע לנקוט במקרה של אירוע אבטחה.

דברי הסבר

<u>סעיף 22:</u> הסעיף מעגן בחקיקה ראשית את החובה לתעד אירועי אבטחת מידע אישי הקבועה כיום בתקנה 11 לתקנות אבטחת מידע ולתקנה על בסיס סעיפים 33 ו-34 ל-GDPR והתיקון לחוק האוסטרלי להגנת פרטיות במידע.[21] בעתיד נפעל לקדם הצעת תיקון לתקנות אבטחת מידע על פי המוצע בסעיף זה. לעת עתה – כדי להציג את התמונה המלאה של מכלול התיקונים המוצעים – בחרנו להציג את הסעיף הזה כחלק מהצעת החוק.

ההסדר הקבוע בתקנה 11 לתקנות אבטחת מידע מחייב בעל שליטה במידע לדווח לנושא מידע על אירוע אבטחת מידע רק במקרה של אירוע אבטחה חמור ורק כאשר ראש הרשות להגנת הפרטיות, לאחר היוועצות עם ראש מערך הסייבר, הורה על מתן הודעה כאמור. חובת ההיוועצות עם ראש מערך הסייבר עלולה לגרום סרבול בירוקרטי מיותר.

ההסדר המוצע בסעיף 22 מחייב בעל שליטה במידע לדווח לראש הרשות להגנת הפרטיות על אירוע אבטחת מידע רק כאשר האירוע גרם פגיעה בזכות לפרטיות, בהתאם לתנאים המפורטים בס"ק (ב) ובהתבסס על התיקון לחוק הפרטיות האוסטרלי. להסדר המוצע שלוש מטרות: האחת – להימנע מהטלת נטל לא סביר על בעל שליטה במידע לדווח על כל אירוע אבטחה גם אם לא נגרמה בגינו פגיעה בפרטיות (למשל, כאשר עובד לקח הביתה בטעות התקן נייד שנושא מידע אישי אבל לא השתמש בו והחזירו למחרת היום למקום העבודה); השנייה – להימנע מהטלת חובת דיווח פומבית מיידית שיש בכוחה לגרום לחשיפת אירועי סייבר באופן שעלול לפגוע בהתמודדות עם האירוע בזמן אמת; והשלישית – להימנע מהפיכת פעולת הדיווח לפעולה טכנית בעיקרה ומהצפת הרשות להגנת הפרטיות.

ס"ק (ג) מטיל על בעל שליטה במידע את החובה לדווח לנושא מידע על אירוע אבטחה שהביא לפגיעה בפרטיותו בתוך פרק זמן סביר ורק לאחר שמסר דיווח, כנדרש לפי סעיף קטן (ב), לראש הרשות להגנת הפרטיות. לחלופין, חובת הודעה פומבית תחול רק כאשר הודעה לכל נושא מידע שעלול להיפגע מאירוע האבטחה תדרוש מאמץ לא סביר מבעל שליטה במידע.

ס"ק (ד) מבוסס על סעיף 33(2) ל-GDPR ומחייב את המעבד לדווח לבעל שליטה במידע על התרחשותו של אירוע אבטחה.

ס"ק (ה)(1) מסמיך את שר המשפטים להחריג בתקנות אירועי אבטחה בעלי שליטה במידע מסוימים מחובת התיעוד והדיווח. הסעיף מתכתב עם ההבחנה הקיימת בתקנות אבטחת מידע שחובת התיעוד והדיווח חלה רק במקרים של "אירוע אבטחה חמור".

כדי להגביר את הגמישות בהחלת חובת הדיווח לפי הוראת סעיף 22 הותרנו בסעיפים קטנים (ה)(2) ו-(ה)(3) את הקביעה מה יכלול דיווח על אירוע אבטחה ומהי פעולה שתיחשב "פעולה מתקנת" לתקנות. ככלל, דיווח כאמור צריך לכלול פרטים מזהים ופרטי יצירת קשר עם בעל שליטה במידע, תיאור של אירוע האבטחה ונסיבותיו, תיאור המידע האישי שעובד או סביר שיעובד בלי הרשאה כתוצאה מאירוע האבטחה ופירוט הפעולות המתקנות שביצע בעל שליטה במידע עד למועד הדיווח ואלו שהוא עתיד לבצע. בדיווח לנושא המידע יש לכלול גם פרטים על הפעולות שרצוי שנושא המידע יבצע עקב אירוע האבטחה.

סעיף 23: ממונה על הגנת הפרטיות במידע

(א) בעל שליטה במידע ומעבד ימנו, כל אחד מטעמו, ממונה על הגנת פרטיות במידע העומד בתנאי הכשירות שנקבעו לפי סעיף קטן (ו), בהתקיים אחד מאלה:

(1) בעל שליטה במידע או המעבד, לפי העניין, הוא גוף ציבורי;

(2) בעל שליטה במידע או המעבד, לפי העניין, מבצע עיבוד מידע אישי על 200,000 נושאי מידע לפחות;

(3) בעל שליטה במידע או המעבד, לפי העניין, מבצע עיבוד מידע רגיש על 100,000 נושאי מידע לפחות.

(ב) הממונה על הגנת הפרטיות במידע יפעל להבטחת קיום הוראות חוק זה על ידי בעל שליטה במידע או המעבד, לפי העניין, ויהיה אחראי לטיפול בפניות הציבור וכן בפניות של ראש הרשות להגנת הפרטיות, בנוגע לקיום הוראות חוק זה.

(ג) בעל שליטה במידע או המעבד, לפי העניין, יספק לממונה על הגנת הפרטיות במידע את התנאים הדרושים למילוי תפקידו, לרבות עצמאות בביצוע תפקידיו לפי חוק זה.

(ד) לא ימונה כממונה על הגנת הפרטיות במידע מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה.

(ה) פרטי יצירת הקשר עם הממונה על הגנת הפרטיות במידע ימסרו על פי דרישה או יפורסמו בהתאם להחלטת בעל שליטה במידע או המעבד, לפי העניין. לכל אדם הזכות לפנות לממונה על הגנת הפרטיות במידע בכל הקשור לעיבוד מידע אישי על אודותיו ומימוש זכויות נושא המידע לפי חוק זה.

(ו) שר המשפטים יקבע בתקנות את תנאי הכשירות הנדרשים למינוי ממונה על הגנת הפרטיות במידע ואת הפעולות שעליו לבצע למילוי תפקידו לפי חוק זה, וכן רשאי שר המשפטים, בתקנות, לשנות את מספר נושאי המידע הקבועים בפסקאות (2) או (3) של סעיף קטן (א), לפטור סוגים מסוימים של בעלי שליטה או מעבדים מחובת מינוי ממונה על הגנת פרטיות במידע לפי סעיף קטן (א) או לחייבם במינוי כאמור.

דברי הסבר

<u>סעיף 23:</u> משלב בין החובה למנות ממונה אבטחת מידע לפי סעיף 17ב לחוק הגנת הפרטיות הקיים ולפי תקנה 3 לתקנות אבטחת מידע לבין החובה למנות ממונה פרטיות לפי סעיפים 37 ו-39 ל-GDPR, 4.1 לנספח 1 לחוק הפרטיות הקנדי ו-23 לחוק הפרטיות הניו זילנדי. בעתיד נפעל לקדם הצעת תיקון לתקנות אבטחת מידע על פי המוצע בסעיף זה. לעת עתה – כדי להציג את התמונה המלאה של מכלול התיקונים המוצעים – בחרנו להציג את הסעיף הזה כחלק מהצעת החוק.

החובה למנות ממונה על הגנת פרטיות במידע תיקבע לפי ס"ק (א) בהתאם למיהות הגוף המבצע עיבוד (גוף ציבורי) ובהתאם להיקף העיבוד של מידע אישי או מידע רגיש. בדרך זו החובה אינה מצומצמת יתר על המידה, כקבוע כיום בסעיף 17ב לחוק הגנת הפרטיות, אבל גם אינה רחבה מדי, כפי שנעשה למשל בחקיקה הקנדית, ועל כן אינה מטילה נטל לא סביר על גופים קטנים.

ס"ק (א) ו-(ו) קובעים את תנאי הכשירות הנדרשים למינוי, וס"ק (ג) מטיל על בעל

שליטה ועל מעבד את האחריות לתת לממונה על הגנת הפרטיות במידע את תנאי ההעסקה המתאימים, לרבות פניות לביצוע התפקיד מבחינת עומס המשימות שיוטל עליו ועצמאות בביצוע תפקידו – כדי להבטיח שיפעל למילוי הוראות חוק זה בלי לחשוש למעמדו בחברה או להמשך העסקתו.

ס"ק (ב) מפרט מסגרת כללית לתפקידי הממונה על הגנת הפרטיות. ס"ק (ד) מבוסס על סעיף 17ב(ג) לחוק הגנת הפרטיות הקיים. ס"ק (ה) שואב השראה מסעיף 4.1.2 לחוק הפרטיות הקנדי וקובע שפרטי יצירת הקשר עם הממונה על הגנת הפרטיות יימסרו על פי דרישה או יפורסמו בהתאם להחלטת בעל שליטה במידע או מעבד. הסעיף אינו מטיל חובה להעביר לרשות להגנת הפרטיות את פרטי הקשר עם הממונה על הגנת הפרטיות במידע, בדומה לסעיף 37(7) ל-GDPR, שכן חיוב כאמור כמוהו כהחזרת החובה לרישום מאגרי מידע, שהטעמים להסרתה הוסברו בדברי ההסבר להגדרת "ראש הרשות להגנת הפרטיות" בסעיף 2 לעיל.

ס"ק (ו) מסמיך את שר המשפטים לשנות את התנאים לכינונה של החובה למינוי ממונה על הגנת הפרטיות וכן לפרט את הכישורים הנדרשים להתאמתו לתפקיד.

<u>סימן ד': שונות</u>

סעיף 24: תחולת הוראות פרק ב'

הוראות פרק ב' יחולו על אלה:

(1) בעל שליטה במידע או מעבד המאוגדים או פועלים במדינת ישראל, בין אם עיבוד המידע האישי נעשה בתחומי מדינת ישראל ובין אם לאו;

(2) כל פעולת עיבוד של מידע אישי על אודות נושא מידע הנמצא במדינת ישראל, בין אם בעל השליטה במידע או המעבד נמצאים או מאוגדים בישראל ובין אם לאו, ובלבד שמטרת עיבוד המידע האישי היא אחת מאלה:

(א) מתן טובין או שירות לנושא מידע הנמצא בישראל;

(ב) ניטור התנהגות של נושא מידע המתבצעת במדינת ישראל.

סעיף 25: נציגות בעל שליטה במידע או מעבד בישראל

(א) בעל שליטה במידע או מעבד, לפי העניין, המבצע עיבוד מידע רגיש על אודות 500,000 נושאי מידע לפחות, או המבצע עיבוד מידע אישי על אודות 1,000,000 נושאי מידע לפחות, ומתקיימים תנאי סעיף 24(2), חובה עליו למנות בכתב נציג שמקום מושבו במדינת ישראל ואשר ישמש כתובת לפניות הרשות להגנת הפרטיות או נושאי המידע בכל הקשור ליישום הוראות חוק זה.

(ב) חובת מינוי נציג לפי סעיף קטן (א) לעיל לא תחול כאשר בעל שליטה במידע או המעבד, לפי העניין, הוא גוף ציבורי.

דברי הסבר

<u>סעיף 24:</u> שואב השראה מסעיף 3 ל-GDPR. מטרתו לקבוע שבהתקיים אחת החלופות המפורטות בסעיף תהא תחולת הוראות פרק ב' להצעת החוק חוץ-טריטוריאלית. המטרה היא למנוע מבעלי שליטה במידע להתחמק מציות להוראות הצעת החוק על ידי העברת מידע אישי על נושאי מידע ישראלים לחוות שרתים הממוקמות במדינות שאינן מחייבות הגנת פרטיות ברמה דומה לרמה המוגדרת בהצעת החוק.

לצורך החלה חוץ-טריטוריאלית של פרק ב' אין די בכך שאתר האינטרנט או כתובת הדוא"ל של בעל השליטה במידע או המעבד זמינים לקהל בישראל או שעיבוד המידע האישי נעשה בשפה העברית. לעומת זאת, מתן האפשרות ליצור קשר עם בעל השליטה במידע או עם המעבד דרך אתר אינטרנט בשפה העברית; מתן האפשרות להזמין טובין או שירות בשפה העברית או באמצעות תשלום במטבע ישראלי, הצגת פרסומות המדגישות שלבעל שליטה במידע או למעבד יש לקוחות או משתמשים של השירות או הטובין בתחומי מדינת ישראל; תשלום למנוע חיפוש בתמורה לכך שהאתר יוצג במיקום גבוה בתוצאות החיפוש בתגובה לשאילתות חיפוש מישראל – כל אלה מלמדים על כוונתו של בעל שליטה במידע או של מעבד להציע שירות או טובין לנושאי מידע בישראל.

<u>סעיף 25:</u> שואב השראה מסעיף 27 ל-GDPR. מטרתו להקל על אכיפת ההוראות שבהצעת החוק גם על תאגידי ענק בינלאומיים שאין להם נציגות משפטית מקומית ולהימנע מפגיעה בתחרות ומהדרת שחקנים בינלאומיים מתחומי מדינת ישראל.

פרק ג: הרשות להגנת הפרטיות וסמכויות פיקוח, אכיפה ובירור מינהלי

סימן א': הרשות להגנת הפרטיות

סעיף 26: ראש הרשות להגנת הפרטיות

מי שמתקיימים בו תנאי הכשירות להתמנות לשופט של בית משפט מחוזי ומונה על ידי הממשלה, בהודעה ברשומות, לנהל את הרשות להגנת הפרטיות.

סעיף 27: תקציב הרשות

תקציב הרשות להגנת הפרטיות ייקבע בחוק התקציב השנתי, בסעיף תקציב נפרד, כמשמעותם בחוק יסודות התקציב, התשמ"ה-1985;[22] הממונה על סעיף תקציב זה לעניין החוק האמור יהיה ראש הרשות להגנת הפרטיות.

סעיף 28: עסקאות הרשות

לצורך ביצוע הוראות חוק זה, מורשה ראש הרשות להגנת הפרטיות, יחד עם חשב הרשות, לייצג את הממשלה בעסקאות כאמור בסעיפים 4 ו 5 לחוק נכסי המדינה, התשי"א–1951,[23] למעט עסקאות במקרקעין, ולחתום בשם המדינה על מסמכים הנוגעים לעסקאות כאמור.

סעיף 29: עובדי הרשות להגנת הפרטיות

(א) עובדי הרשות להגנת הפרטיות יהיו עובדי המדינה ויחולו עליהם הוראות חוק שירות המדינה (מנויים), התשי"ט-1959,[24] ואולם ראש הרשות מורשה, באישור שר המשפטים, יחד עם חשב הרשות, לייצג את המדינה בעשיית חוזים מיוחדים עם עובדים.

(ב) עובדי הרשות יפעלו לפי הוראות ראש הרשות להגנת הפרטיות ובפיקוחו.

דברי הסבר

<u>**סעיפים 26-29:**</u> סעיפים אלו שואבים השראה מסעיפים 10(ד) לחוק הגנת הפרטיות הקיים, 41, 41א, 41ב לחוק ההגבלים העסקיים, התשמ"ח–1988, ו-19א-19ג לחוק הגנת הצרכן, התשמ"א-1981. מטרתם להקנות לראש הרשות להגנת הפרטיות כלים שיאפשרו לו וליחידתו חופש פעולה מינהלי ותקציבי שיסייעו בביצוע תפקידיו המורכבים. תקציב הרשות ייקבע בחוק התקציב בסעיף נפרד. ראש הרשות להגנת הפרטיות יהיה הממונה על ביצועו של התקציב, וכך תובטח עצמאותם של הרשות ושל ראש הרשות בניהול הרשות ובהפעלת התקציב שיוקצה לפעולותיה. ראש הרשות יוסמך להתקשר בעסקאות כנדרש לפעולת הרשות. לבסוף, ראש הרשות יוסמך לטפל בענייניה המינהליים של הרשות, אך עובדי הרשות יהיו עובדי מדינה. לפיכך עובדי הרשות יחויבו בנורמות המהותיות והאתיות של עובדי המדינה ויהיו כפופים לחוק שירות המדינה (מינויים), התשי"ט–1959. בד בבד תוקנה לרשות להגנת הפרטיות יכולת ניהול אוטונומית מסוימת.

סעיף 30: תפקידי הרשות להגנת הפרטיות

(א) תפקידי הרשות יהיו –

(1) לפקח על ביצוע הוראות חוק זה;

(2) לחקור חשד לביצוע עבירה לפי חוק זה ולהביא את העבריין לדין;

(3) לנקוט הליכי אכיפה מינהלית נגד מפר לפי הוראות חוק זה;

(4) לטפח תודעה ציבורית להגנת הפרטיות באמצעות חינוך, הדרכה והסברה, ככל שתפקיד זה אינו מוטל על רשות ציבורית אחרת הפועלת על פי דין;

(5) לטפל בתלונות שיש בהן ממש על הפרת הוראות חוק זה או על פגיעה אחרת בפרטיות נושא מידע;

(6) לערוך וליזום סקרים ומחקרים בענייני הגנת הפרטיות;

(7) לייעץ לממשלה בכל הקשור ביישום מטרות חוק זה;

(8) לטפל בכל עניין אחר הקשור להגנת הפרטיות ואשר לא הוטל בדין על רשות אחרת.

(ב) הגיעה לראש הרשות להגנת הפרטיות תלונה בעניין שבו לפי חיקוק יש לרשות אחרת סמכות לפיקוח ולנקיטת אמצעים בעקבות בירור תלונה, ייוועץ באותה רשות לפני שיטפל בתלונה, ורשאי הוא אף להעביר את התלונה אליה; העביר ראש הרשות להגנת הפרטיות את התלונה כאמור, תודיע הרשות אליה הועברה התלונה לראש הרשות להגנת הפרטיות על תוצאות הטיפול.

(ג) ראה ראש הרשות להגנת הפרטיות כי מטרות החוק לפי סעיף 1 מושפעות, כרוכות או עלולות להיות מושפעות או כרוכות בהליך פלוני שלפני בית משפט, רשאי הוא, לפי ראות עיניו, להתייצב באותו הליך ולהשמיע דברו, או להסמיך במיוחד את נציגו לעשות זאת מטעמו;

דברי הסבר

<u>סעיף 30</u>: עיקרו של הסעיף מבוסס על סעיף 20 לחוק הגנת הצרכן, התשמ"א–1981, מתוך הבנה שיש דמיון רב בין הרשות להגנת הצרכן וסחר הוגן לבין הרשות להגנת הפרטיות. הדמיון בין שתי הרשויות בא לידי ביטוי בקהלי היעד שכל אחת מן הרשויות פועלת מולם, בסוג ההליכים שהן מוסמכות לנהל ובטיפוסי הזכויות שהן אמורות להגן עליהן. בשונה מחוק הגנת הצרכן, הסעיף מעגן את תפקידי הרשות ולא רק את תפקידי ראש הרשות, בדומה לסעיף 18ח לחוק שוויון הזדמנויות בעבודה, התשמ"ח–1988, ולסעיף 5 לחוק הרשות השניה לטלויזיה ורדיו, התש"ן–1990.

ס"ק (א)(7) שואב השראה מסעיף 8 לחוק לעידוד מחקר, פיתוח וחדשנות טכנולוגית בתעשיה, התשמ"ד–1984. מטרתו להעמיק את המתאם בין מדיניות הממשלה לפעילות של הרשות להגנת הפרטיות, הן ברמה הכללית והן ברמה היישומית הפרטנית, באמצעות הסמכת הרשות להגנת הפרטיות לייעץ לממשלה בכל הקשור ליישום של מטרות החוק. ס"ק (ג) שואב השראה מסעיף 1 לפקודת סדרי הדין (התייצבות היועץ המשפטי לממשלה) [נוסח חדש]. מטרתו להבטיח את הצגת האינטרס הציבורי שבהגנה על הזכות לפרטיות על ידי אנשי מקצוע מומחים בתחום בהליכים משפטיים, בכלל זה הליכים המתנהלים נגד הרשות המחוקקת או המבצעת.

סעיף 31: שיתוף פעולה עם רשות חוץ

(א) מצא ראש הרשות להגנת הפרטיות כי התקיימו כל אלה:

(1) רשות חוץ הגישה לרשות להגנת הפרטיות בקשה לסיוע;

(2) נושא הבקשה לסיוע עשוי להיות הפרה של דיני הגנת הפרטיות שרשות חוץ, שהגישה את הבקשה, מופקדת על ביצועם, אכיפתם ופיקוחם;

רשאי הוא לקבוע כי על הבקשה לסיוע יחולו הוראות סעיף זה.

(ב) לא תיעשה פעולה מכוח הוראות סעיף זה אם היא עלולה, לדעת היועץ המשפטי לממשלה, לפגוע בריבונות מדינת ישראל, בביטחונה, באינטרס החיוני לה, בתקנת הציבור או בחקירה תלויה ועומדת.

(ג) כדי להבטיח מתן סיוע לרשות חוץ, יהיו חוקר, מפקח או עובד מדינה שהוסמך לכך לפי סעיף 33, רשאים להשתמש בסמכויות לפי סעיפים 34 עד 37, שהוסמכו לבצען, לפי העניין, ובסמכויות לפי סעיף 43 לפקודת מעצר וחיפוש וסעיף 3 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007 (בסעיף זה – חוק נתוני תקשורת) בשינויים המחויבים ובלבד שנושא בקשת הסיוע עשוי להיות נתון לחקירה כעבירה פלילית לפי חוק זה, ואם הנושא של הבקשה לסיוע הוא פיקוח – תיעשה הפעלת הסמכויות לפי סעיף 34 בלבד.

(ד) קבע ראש הרשות להגנת הפרטיות כי על הבקשה לסיוע יחולו הוראות סעיף זה, ומידע אישי או מסמך שמבוקשים בבקשה לסיוע מצויים בידי הרשות להגנת הפרטיות, רשאי מי שראש הרשות להגנת הפרטיות הסמיכו לכך בכתב להעביר לרשות החוץ את המידע האישי או המסמך או העתק מאושר או העתק צילומי מאושר שלו.

(ה) לא יועבר מידע אישי או מסמך בהתאם לסעיף קטן (ד) לעיל אלא אם שוכנע ראש הרשות להגנת הפרטיות כי הוא ישמש אך ורק למטרה שלשמה נמסר.

(ו) הועבר מידע אישי או מסמך לפי סעיף קטן (ד) לעיל, רשאי ראש הרשות להגנת הפרטיות לאשר לרשות חוץ להעביר מידע אישי או מסמך לשם ביצוע ואכיפה של דיני הגנת הפרטיות ופיקוח על ביצועם, לרשות ממשלתית אחרת או לרשות שהוקמה מכוח הסכם בין מדינות ורשאי הוא להתנות העברת מידע אישי או מסמך כאמור בתנאים.

(ז) ראש הרשות להגנת הפרטיות רשאי להורות שפעולה לפי סעיף זה לא תיעשה לפי בקשת רשות חוץ, אשר מנועה או נמנעה מביצוע פעולה דומה לבקשת הרשות להגנת הפרטיות.

(ח) על אף האמור בכל דין, מידע אישי, ידיעה או מסמך שנמסרו לרשות על ידי רשות חוץ או שהתקבלו, שנאספו או שנוצרו בעקבות בקשה לסיוע או בקשה לקבלת מידע אישי, ידיעה או מסמך שהוגשה לרשות להגנת הפרטיות על ידי רשות חוץ, לרבות הבקשה עצמה, רשאית הרשות להגנת הפרטיות שלא להעבירם לצד שלישי; אין בהוראה זו כדי למנוע גילוי לפי דרישת היועץ המשפטי לממשלה לצורך משפט פלילי או לפי דרישת בית המשפט.

סעיף 32: הוועדה המייעצת

(א) שר המשפטים ימנה ועדה מייעצת שתפקידה:

(1) לייעץ לראש הרשות להגנת הפרטיות, לפי דרישתו, בכל עניין הנוגע להגנת הפרטיות, וכן לייעץ לו בהכנת הדין וחשבון השנתי כאמור בסעיף 74 ובהכנת תוכנית העבודה של הרשות;

(2) לדון בנושאים נוספים בנוגע ליישום הוראות חוק זה שיש לדעתה חשיבות בעיסוק הרשות להגנת הפרטיות בהם.

(ב) הוועדה המייעצת תהיה בת חמישה חברים והם:

(1) עובד משרד המשפטים בדרגה ____;

(2) עובד משרד הכלכלה והתעשייה בדרגה שאינה פחותה מדרגת סגן מנהל כללי;

(3) חבר הסגל האקדמי של מוסד מוכר להשכלה גבוהה כמשמעותו בחוק המועצה להשכלה גבוהה, התשי"ח–1958;[25]

(4) שני נציגי ציבור מקרב מוסד, מכון או ארגון, אשר אחד מהם לפחות יהיה נציג מתחום תעשיית הטכנולוגיה והשני יעסוק באחד מהתחומים האלה: צרכנות, משפט, כלכלה או מדיניות ציבורית;

(ג) שר המשפטים ימנה את אחד מחברי הוועדה המייעצת להיות יושב ראש הוועדה.

(ד) חברי הוועדה המייעצת ימונו לתקופה של שלוש שנים וניתן לחזור למנותם, ובלבד שלא יכהנו שלוש תקופות רצופות.

דברי הסבר

<u>סעיף 31:</u> שואב השראה מסעיפים 50 ל-GDPR ו-54יא1–54יא9 לחוק ניירות ערך התשכ"ח–1968.

פגיעה בזכות לפרטיות, בעיקר פרטיות במידע, יכולה להיות חוצת גבולות (למשל, בפרשת **קיימברידג' אנליטיקה** נחשף מידע אישי על כ-47 אלף משתמשי פייסבוק מישראל[26]). שיתוף פעולה בין רשויות הגנת פרטיות ברחבי העולם הוא אפוא כורח המציאות – כדי לאפשר אכיפה יעילה של דיני הגנת הפרטיות.

הצורך בשיתוף מידע אישי בין רשויות מדינתיות קיבל הכרה בינלאומית בהחלטה מספטמבר 2017,[27] לְקח מהחקירה המשותפת שניהלו רשויות הגנת הפרטיות של קנדה, של אוסטרליה ושל ארצות הברית בעניין חשיפת מידע אישי ומידע רגיש על משתמשי האתר "אשלי מדיסון".[28]

<u>סעיף 32:</u> הסעיף שואב השראה מסעיף 22א לחוק הגנת הצרכן, התשמ"ח–1981. הוא בא במקום ההתייחסות ה"כחושה" בסעיף 10א לחוק הגנת הפרטיות הקיים, שהתמקד רק בחובתה הסטטוטורית של המועצה הציבורית להגנת הפרטיות להעיר את הערותיה על דוח רשם מאגרי המידע. מטרת הסעיף לעגן בחוק את הקמת הוועדה המייעצת ולקבוע את סמכויותיה במפורש, מתוך הכרה בסמכותה לדון גם בנושאים נוספים על אלו שידרוש ראש הרשות להגנת הפרטיות, אם לדעתה יש חשיבות לדיון ברשות להגנת הפרטיות ולעיסוק שלה בנושאים אלו. המטרה היא למנוע את האפשרות שראש הרשות להגנת הפרטיות ירוקן את תפקידה של הוועדה המייעצת מתוכן.

סעיף 33: הסמכת חוקר או מפקח

(א) ראש הרשות להגנת הפרטיות רשאי להסמיך חוקר או מפקח, מבין עובדי המדינה, לביצוע סמכויות לפי חוק זה, כולן או חלקן, אם התקיימו בו כל אלה:

(1) משטרת ישראל הודיעה, בתוך שלושה חודשים מפנייתו של ראש הרשות להגנת הפרטיות אליה, כי היא אינה מתנגדת להסמכתו מטעמים של ביטחון הציבור, לרבות בשל עברו הפלילי;

(2) הוא קיבל הכשרה מתאימה בתחום הסמכויות שיהיו נתונות לו לפי חוק זה, כפי שהורה שר המשפטים בהסכמת השר לביטחון הפנים, ולעניין הפעלת סמכויות חדירה לחומר מחשב או העתקתו כאמור בסעיפים 36-35 – הוא בעל תפקיד המיומן לביצוע פעולות כאמור;

(3) הוא עומד בתנאי כשירות נוספים, ככל שהורה שר המשפטים בהסכמת השר לביטחון הפנים.

(ב) הסמכתו של מפקח או חוקר לפי סעיף זה תהיה בתעודה החתומה בידי ראש הרשות להגנת הפרטיות, שמעידה על תפקידו כמפקח או כחוקר ועל סמכויותיו לפי חוק זה.

דברי הסבר

<u>סעיף 33:</u> מבוסס על סעיפים 10(ה) להצ"ח תיקון מס' 13 ו-20א(ג) לחוק הגנת הצרכן. מטרת הסעיף לקבוע שראש הרשות להגנת הפרטיות יהיה רשאי להסמיך חוקר או מפקח, מקרב עובדי המדינה, לביצוע סמכויות האכיפה והפיקוח לפי הצעת החוק, וכן לקבוע תנאי הסמכה הולמים למפקח ולחוקר, בדגש על הכשרה ראויה לצורך הפעלת סמכות חדירה לחומר מחשב. הסעיף אינו מגביל את תוקף הכשרתו של חוקר או מפקח, בדומה לסעיף 20א(ג) בחוק הגנת הצרכן, אלא מסתפק בהסכמת שר המשפטים לקבוע בתקנות תנאי כשירות נוספים, למשל הכשרות עיתיות להבטחת הכשירות של המפקח לביצוע תפקידו, בעיקר לנוכח השינויים הטכנולוגיים התדירים בתחום העיבוד של מידע אישי.

סימן ב': סמכויות פיקוח

סעיף 34: סמכויות מפקח

(א) לשם פיקוח על ביצוע ההוראות לפי פרקים ב', ד', ו-ו', רשאי ראש הרשות להגנת הפרטיות או מפקח שהוסמך על ידו –

(1) לדרוש מכל אדם למסור לו את שמו ומענו ולהציג לפניו תעודת זהות או תעודה רשמית אחרת המזהה אותו;

(2) לדרוש מכל אדם הנוגע בדבר למסור לו כל ידיעה או מסמך;

(3) לדרוש מכל אדם הנוגע בדבר להציג לפניו או למסור לו עותק מחומר מחשב הכולל נתוני מערכת או מידע אישי מדגמי; מידע אישי מידגמי לפי סעיף זה לא ייאסף בהיקף העולה על הנדרש למימוש תכליות הפיקוח.

(4) להיכנס למקום שיש לו יסוד סביר להניח שנעשה בו עיבוד של מידע אישי, ובלבד שלא ייכנס למקום המשמש למגורים אלא לפי צו של בית משפט.

(ב) הממונה ימחק מידע אישי מדגמי, שנמסר או שנאסף לפי סעיף זה, כאשר אינו נדרש עוד באופן סביר להמשך הליכי הפיקוח, ולכל היותר בתוך שלוש שנים ממועד מסירתו או איסופו, אלא אם כן המידע האישי המידגמי דרוש לצורך הליכים לפי פרק ג', סימנים ג' או ד'.

סימן ג': סמכויות בבירור מינהלי

סעיף 35: צו לחיפוש ולחדירה לחומר מחשב

היה לראש הרשות להגנת הפרטיות או לעובד המדינה שהוא הסמיך לכך בהודעה ברשומות, הכשיר לכהן כשופט של בית משפט מחוזי, יסוד סביר להניח כי בוצעה הפרה של הוראה מההוראות לפי חוק זה כאמור בסעיף 38, רשאי הוא לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב לפי סעיפים 23 עד 24 לפקודת המעצר והחיפוש, ולבצעם בעצמו או באמצעות מפקח.

סעיף 36: אופן ביצוע חדירה לחומר מחשב והעתקתו

על ביצוע חיפוש, תפיסת חפץ וחדירה לחומר מחשב או העתקתו לפי סימן זה, יחולו הוראות סעיפים 23א, 24(א)(1) ו (ב), 26 עד 28, 31 ו-45 וכן הוראות הפרק הרביעי, לפקודת המעצר והחיפוש, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות למפקח והסמכויות הנתונות לקצין יהיו נתונות לראש הרשות להגנת הפרטיות ולעובד המדינה שהוא הסמיך כאמור בסעיף 33.

דברי הסבר

<u>סעיף 34</u>: מבוסס על סעיפים 10(ה1) לחוק הגנת הפרטיות הקיים ו-23י להצ"ח תיקון מס' 13.

<u>סעיפים 35 ו-36</u>: מבוססים על סעיפים 23יא ו-23יב להצ"ח תיקון מס' 13.

סעיף 37: סמכויות אכיפה, חקירה, עיכוב ותפיסה

(א) היה לראש הרשות להגנת הפרטיות או לחוקר יסוד סביר לחשד שנעברה עבירה לפי פרקים ב' או ו', או התעורר חשד כי אגב חקירה בעבירה כאמור, נעברה עבירה לפי סעיפים 242, 244, 245, 246, ו-249 לחוק העונשין, התשל"ז–1977,[29] (להלן – חוק העונשין) יהיו נתונות לראש הרשות להגנת הפרטיות ולחוקר כל סמכויות הפיקוח לפי סימן ב', וכן רשאים הם –

(1) לחקור כל אדם הקשור לעבירה כאמור או שעשויות להיות לו ידיעות הנוגעות לעבירה כאמור; על חקירה לפי פסקה זו יחולו הוראות סעיפים 2 ו-3 לפקודת הפרוצדורה הפלילית (עדות),[30] והוראות חוק סדר הדין הפלילי (חקירת חשודים), התשס"ב–2002,[31] בשינויים המחויבים;

(2) לתפוס כל חפץ שיש לו יסוד סביר להניח שהוא חפץ הקשור לעבירה כאמור;

(3) לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב לפי סעיפים 23 עד 24 לפקודת המעצר והחיפוש, ולבצעו.

(ב) על ביצוע חיפוש, תפיסת חפץ וחדירה לחומר מחשב או העתקתו לפי סעיף זה יחולו סעיפים 23א, 24(א)(1) ו-(ב), 26 עד 28, 31 ו-45 וכן הוראות הפרק הרביעי לפקודת המעצר והחיפוש, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין יהיו נתונות לראש הרשות להגנת הפרטיות ולעובד המדינה שהוא הסמיך כאמור בסעיף 33.

(ג) היה לראש הרשות להגנת הפרטיות או לחוקר יסוד סביר לחשד שאדם עבר עבירה לפי פרקים ב' או ו', או התעורר חשד כי אגב חקירה בעבירה כאמור, נעברה עבירה לפי סעיפים 242, 244, 245, 246, ו-249 לחוק העונשין,[32] רשאי הוא לעכבו כדי לברר את זהותו ומענו או כדי לחוקרו במקום הימצאו; היה הזיהוי בלתי מספיק או שלא ניתן לחקור את אותו אדם במקום הימצאו, רשאי ראש הרשות להגנת הפרטיות או החוקר לדרוש מאותו אדם להתלוות אליו למשרדי ראש הרשות להגנת הפרטיות או לזמנו למשרדי הרשות להגנת הפרטיות למועד אחר שיקבע. מי שזומן למשרדי ראש הרשות להגנת הפרטיות יתייצב במועד שזומן אליו; על עיכוב לפי סעיף קטן זה יחולו הוראות סעיפים 66, 67 ו-72 עד 74 לחוק המעצרים, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין הממונה יהיו נתונות לראש הרשות להגנת הפרטיות.

(ד) היה לראש הרשות להגנת הפרטיות או לחוקר יסוד סביר לחשד שנעברה עבירה לפי פרקים ב' או ו', או התעורר חשד כי אגב חקירה בעבירה כאמור, נעברה עבירה לפי סעיפים 242, 244, 245, 246, ו-249 לחוק העונשין, רשאי הוא לעכב אדם שיכול למסור לו מידע הנוגע לאותה עבירה, כדי לברר את זהותו ומענו וכדי לחקור אותו במקום הימצאו; וכן רשאי הוא לזמן אותו למשרדי ראש הרשות להגנת הפרטיות למועד סביר אחר שיקבע לצורך ביצוע אותן פעולות; מי שזומן למשרדי ראש הרשות להגנת הפרטיות, יתייצב

במועד שזומן אליו; על עיכוב לפי סעיף קטן זה יחולו הוראות סעיפים 68 ו-72 עד 74 לחוק המעצרים, בשינויים המחויבים, ובשינוים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין הממונה יהיו נתונות לראש הרשות להגנת הפרטיות.

(ה) לעניין סעיפים קטנים (ג) ו-(ד) יראו את משרדי ראש הרשות להגנת הפרטיות שראש הרשות הכריז עליהם בהודעה ברשומות, כ"תחנת משטרה" לעניין הוראות חוק המעצרים.

פרק ד : אמצעי אכיפה מינהליים

סימן א': עיצום כספי

סעיף 38: עיצום כספי

(א) הפר אדם הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי ראש הרשות להגנת הפרטיות להטיל עליו עיצום כספי בסכום של ___, ואם המפר הוא תאגיד – בסכום של ___:

(1) עיבד מידע אישי מבלי שמילא את חובת מתן הודעה, בניגוד להוראות סעיף 9;

(2) הפר את זכותו של נושא מידע לחזור בו מהסכמתו, בניגוד להוראות סעיף 10;

(3) הפר את זכות מזכויות נושא מידע לעיין במידע אישי על אודותיו, לקבל הסבר, לתקן, לנייד או למחוק מידע אישי על אודותיו, בניגוד להוראת סעיפים 11; 12, 13, 14 ו-15 בהתאמה; או בניגוד להוראות שנקבעו לעניין זה לפי סעיף 16;

(4) סירב לבקשת נושא מידע למימוש זכות מזכויות נושא המידע כאמור בסעיפים 11(ה) עד (ח), 13(ד), 14(ו) או 15(ג), ולא הודיע על כך לנושא המידע כנדרש לפי סעיף 16(ד).

(ב) הפר אדם הוראה מההוראות חוק זה, כמפורט להלן, רשאי ראש הרשות להגנת הפרטיות להטיל עליו עיצום כספי בסכום של ___, ואם המפר הוא תאגיד – בסכום של ___:

(1) עיבד מידע אישי שלא למטרה לשמה נמסר, בניגוד להוראות סעיף 7;

(2) לא תיכנן, עיצב או הפעיל את מערכות עיבוד המידע האישי שיבטיחו את התאמתן להוראות חוק זה, בניגוד להוראות סעיף 19;

(3) לא הכין תסקיר השפעה על הפרטיות, בניגוד להוראות סעיף 20;

(4) לא נקט אמצעים סבירים לאבטחת מידע אישי, בניגוד להוראות סעיף 21;

(5) לא תיעד או דיווח על אירועי אבטחה, בניגוד להוראות סעיף 22;

(6) לא מינה ממונה הגנת פרטיות במידע או הסמיכו לבצע את תפקידיו, בניגוד להוראות סעיף 23;

סעיף 39: הפרה בנסיבות מחמירות

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי הפר אדם הוראה מההוראות לפי חוק זה המפורטות בסעיף 38, בנסיבות מחמירות, רשאי ראש הרשות להגנת הפרטיות להטיל עליו עיצום כספי לפי הוראות פרק זה, ששיעורו פי אחד וחצי מסכום העיצום הכספי שניתן להטיל בשל אותה הפרה לפי סעיף 38.

(ב) בסעיף זה, "נסיבות מחמירות" – הפרה הנוגעת ל 100,000 נושאי מידע לפחות, או הפרה הנוגעת למידע רגיש.

דברי הסבר

סעיף 37: מבוסס על סעיף 23יג להצ"ח תיקון מס' 13, אך בהשראת סעיף 46 לחוק ההגבלים העסקיים, התשמ"ח–1988, וסעיף 56 לחוק ניירות ערך, התשכ"ח–1968, סמכות האכיפה הנתונה לפי הסעיף לראש הרשות להגנת הפרטיות או לחוקר הורחבה גם לביצוע חקירה גם בעבירות נלוות לעבירות לפי חוק זה (סעיפים 242 (השמדת ראיה), 244 (שיבוש מהלכי משפט), 245 (הדחה בחקירה), 246 (הדחה בעדות), ו-249 (הטרדת עד) לחוק העונשין התשל"ז-1977). הרחבה זו של סמכות האכיפה נועדה למנוע מצב שלא מנוהלת חקירה במכלול השלם של העבירות בנימוק שהעבירה הנלווית אינה חמורה מספיק ולכן אינה מצדיקה חקירת משטרה נפרדת. הסעיף מגדיר אפוא את הרשות להגנת הפרטיות כרשות חקירה עצמאית, בדומה לרשות לניירות ערך ולרשות להגבלים העסקיים, ואף מאפשר לחוקריה לחקור חשדות לשיבוש הליכי חקירה מסוגים שונים כאשר מתעורר חשד שנעשו פעולות לשיבושה. הוראה זו עולה בקנה אחד עם מגמת המחוקק להקשות על שיבוש הליכי משפט.

סעיף 38: מבוסס על הוראת סעיף 23יט להצ"ח תיקון מס' 13 ושואב השראה מהוראות סימן א בפרק ה1 לחוק הגנת הצרכן, התשמ"א–1981, המעגן את המודל העכשווי העדכני ביותר לסמכות אכיפה מינהלית בהקשרים של הגנת הצרכן שהם בעלי דמיון רב מבחינת אופי ומספר ההפרות האפשריות לפגיעות אפשריות בזכות לפרטיות. מודל זה בא במקום המודל המסורבל המוצע בסעיף 23יט להצ"ח תיקון מס' 13.

הסעיף מונה את ההפרות שבגינן יוטל עיצום כספי על פי הוראות הדין המהותי בהצעת החוק. לפיכך הוא אינו מאמץ את סעיפים 23טז(ב), 23יט(ד)(2), 23יט(ג)(7), ו-יט(ג)(9), (10), (11), (12) להצ"ח תיקון מס' 13 העוסקים בהפרת חובות הנוגעות לרישום מאגרי מידע ולדיוור ישיר.

בדומה להבחנה המוצעת גם היום בהצ"ח תיקון מס' 13, סעיף 38 מבחין בין הפרות הקשורות לכיבוד זכויותיו של נושא המידע, המנויות בס"ק (א), לבין הפרות הקשורות לחובות של בעל שליטה במידע ושל מעבד ולדרך עיבוד המידע האישי, לתנאים המקדימים לעיבודו ולהתוויה של אופן עיבוד המידע האישי, המנויים בס"ק (ב).

סעיף 39: מבוסס על סעיף 22ד לחוק הגנת הצרכן ומאפשר הטלת עיצום כספי בסכום גבוה מן הסכום הקבוע להפרה כאשר מדובר בנסיבות מחמירות. בדרך זו אפשר להקשיח את הענישה המינהלית כאשר מדובר במספר גדול של נושאי מידע שעלולים להיפגע או כאשר מדובר במידע רגיש – בלי לאמץ את ההסדר המסורבל המוצע בהצ"ח תיקון מס' 13 באשר לסכום הבסיסי ולכפולותיו.

סעיף 40: הודעה על כוונת חיוב

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי הפר אדם הוראה מההוראות לפי חוק זה, כאמור בסעיף 38 (בפרק זה – המפר), ובכוונתו להטיל עליו עיצום כספי לפי אותו סעיף או לפי סעיף 39, ימסור למפר הודעה על הכוונה להטיל עליו עיצום כספי (בפרק זה – הודעה על כוונת חיוב).

(ב) בהודעה על כוונת חיוב יציין ראש הרשות להגנת הפרטיות, בין השאר, את אלה:

(1) המעשה או המחדל (בפרק זה – המעשה), המהווה את ההפרה, ומועד ביצועו;

(2) סכום העיצום הכספי והתקופה לתשלומו;

(3) זכותו של המפר לטעון את טענותיו לפני ראש הרשות להגנת הפרטיות לפי הוראות סעיף 41;

(4) שיעור התוספת על העיצום הכספי בהפרה נמשכת או בהפרה חוזרת לפי הוראות סעיף 43.

סעיף 41: זכות טיעון

(א) מפר שנמסרה לו הודעה על כוונת חיוב לפי הוראות סעיף 40 רשאי לטעון את טענותיו, בכתב או בעל פה, לעניין הכוונה להטיל עליו עיצום כספי ולעניין סכומו, בתוך 45 ימים ממועד מסירת ההודעה.

(ב) ראש הרשות להגנת הפרטיות רשאי, לבקשת המפר, להאריך את התקופה האמורה בסעיף קטן (א) בתקופה נוספת שלא תעלה על 45 ימים.

סעיף 42: החלטת ראש הרשות להגנת הפרטיות ודרישת תשלום

(א) ראש הרשות להגנת הפרטיות יחליט, לאחר ששקל את הטענות שנטענו לפי סעיף 41, אם להטיל על המפר עיצום כספי, ורשאי הוא להפחית את סכום העיצום הכספי לפי הוראות סעיף 44.

(ב) החליט ראש הרשות לפי סעיף קטן (א) –

(1) להטיל על המפר עיצום כספי – ימסור לו דרישה, בכתב, לשלם את העיצום הכספי (בפרק זה – דרישת תשלום), שבה יציין, בין השאר, את סכום העיצום הכספי המעודכן ואת התקופה לתשלומו כאמור בסעיף 46;

(2) שלא להטיל על המפר עיצום כספי – ימסור לו הודעה על כך, בכתב.

(ג) בדרישת התשלום או בהודעה, לפי סעיף קטן (ב), יפרט ראש הרשות להגנת הפרטות את נימוקי החלטתו.

(ד) לא טען המפר את טענותיו לפי הוראות סעיף 41 בתוך התקופה האמורה באותו סעיף, יראו את ההודעה על כוונת חיוב, בתום אותה תקופה, כדרישת תשלום שנמסרה למפר במועד האמור.

סעיף 43: הפרה נמשכת והפרה חוזרת

(א) בהפרה נמשכת, יווסף על העיצום הכספי הקבוע לאותה הפרה, החלק החמישים שלו לכל יום שבו נמשכת ההפרה; לעניין זה, "הפרה נמשכת" – הפרת הוראה מההוראות לפי חוק זה, כאמור בסעיף 38, לאחר שנמסרה למפר דרישת תשלום בשל הפרת אותה הוראה או לאחר שנמסרה למפר התראה מינהלית כמשמעותה בסעיף 49, בשל הפרת אותה הוראה וההתראה לא בוטלה כאמור בסעיף 50.

(ב) בהפרה חוזרת יווסף על העיצום הכספי הקבוע לאותה הפרה, סכום השווה לעיצום הכספי כאמור; לעניין זה, "הפרה חוזרת" – הפרת הוראה מההוראות לפי חוק זה, כאמור בסעיף 38(א), בתוך שנתיים מהפרה קודמת של אותה הוראה שבשלה הוטל על המפר עיצום כספי או שבשלה הורשע, ולעניין הפרות לפי סעיף 38(ב) – בתוך תשעה חודשים מהפרה קודמת של הוראות אלה.

סעיף 44: סכומים מופחתים

(א) ראש הרשות להגנת הפרטיות אינו רשאי להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים בסימן זה, אלא לפי הוראות סעיף קטן (ב).

(ב) שר המשפטים רשאי לקבוע מקרים, נסיבות ושיקולים שבשלהם יהיה ניתן להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים בסימן זה, ובשיעורים שיקבע.

סעיף 45: סכום מעודכן של הפיצוי הכספי

העיצום הכספי יהיה לפי סכומו המעודכן לפי סעיף 78 ביום מסירת דרישת התשלום, ולגבי מפר שלא טען את טענותיו לפני ראש הרשות להגנת הפרטיות כאמור בסעיף 42(ד) – ביום מסירת ההודעה על כוונת החיוב; הוגשה עתירה לבית המשפט לעניינים מינהליים או הוגש ערעור על החלטה בעתירה כאמור ועוכב תשלומו של העיצום הכספי בידי ראש הרשות להגנת הפרטיות או בית המשפט – יהיה העיצום הכספי לפי סכומו המעודכן ביום ההחלטה בעתירה או בערעור, לפי העניין.

דברי הסבר

<u>סעיפים 40-46:</u> מבוססים על סעיפים 23כ-23כה להצ"ח תיקון מס' 13 ומותאמים להוראות סימן א בפרק ה'1 לחוק הגנת הצרכן, התשמ"א–1981, שמציג מתווה מעודכן יותר להטלת עיצום כספי על ידי רשות מינהלית.

סעיף 46: המועד לתשלום העיצום הכספי

המפר ישלם את העיצום הכספי בתוך 45 ימים מיום מסירת דרישת התשלום כאמור בסעיף 42.

סעיף 47: הפרשי ריבית והצמדה

לא שילם המפר עיצום כספי במועד, ייווספו על העיצום הכספי לתקופת הפיגור, הפרשי הצמדה וריבית כהגדרתם בחוק פסיקת ריבית והצמדה, התשכ"א–1961[33] (בפרק זה – הפרשי הצמדה וריבית), עד לתשלומו.

סעיף 48: גבייה

עיצום כספי ייגבה לאוצר המדינה, ועל גבייתו יחול חוק המרכז לגביית קנסות, אגרות והוצאות, התשנ"ה–1995.[34]

סימן ב': התראה מינהלית

סעיף 49: התראה מינהלית

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 38, והתקיימו נסיבות שקבע ראש הרשות להגנת הפרטיות בנהלים, רשאי הוא, במקום להמציא לו הודעה על כוונת חיוב ולהטיל עליו עיצום כספי, לפי הוראות סימן א', להמציא לו התראה מינהלית לפי הוראות סימן זה.

(ב) בהתראה מינהלית יציין ראש הרשות להגנת הפרטיות מהו המעשה המהווה את ההפרה, יודיע למפר כי עליו להפסיק את ההפרה וכי אם ימשיך בהפרה או יחזור עליה יהיה צפוי לעיצום כספי בשל הפרה נמשכת או הפרה חוזרת, לפי העניין, כאמור בסעיף 43, וכן יציין את זכותו של המפר לבקש את ביטול ההתראה לפי הוראות סעיף 50.

סעיף 50: בקשה לביטול התראה מינהלית

(א) נמסרה למפר התראה מינהלית כאמור בסעיף 49 רשאי הוא לפנות לראש הרשות להגנת הפרטיות, בכתב או בעל פה, בתוך 45 ימים, בבקשה לבטל את ההתראה בשל כל אחד מטעמים אלה:

(1) המפר לא ביצע את ההפרה;

(2) המעשה שביצע המפר, המפורט בהתראה, אינו מהווה הפרה.

(ב) קיבל ראש הרשות להגנת הפרטיות בקשה לביטול התראה מינהלית, לפי הוראות סעיף קטן (א), רשאי הוא לבטל את ההתראה או לדחות את הבקשה ולהותיר את ההתראה על כנה; החלטת ראש הרשות להגנת הפרטיות תינתן בכתב ותימסר למפר בצירוף נימוקים.

דברי הסבר

<u>סעיפים 46-48:</u> מבוססים על סעיפים 23כו-23כח להצ"ח תיקון מס' 13 ומותאמים להוראות סימן א בפרק ה'1 לחוק הגנת הצרכן, התשמ"א-1981.

<u>סעיף 49:</u> מבוסס על הוראת סעיפים 23כט להצ"ח תיקון מס' 13 ו-22יג לחוק הגנת הצרכן לעניין ההסדר לאישור הנהלים שיקבעו על ידי ראש הרשות להגנת הפרטיות ובאישור היועץ המשפטי לממשלה.

<u>סעיף 50:</u> מבוסס על סעיפים 23ל ו-22יד לחוק הגנת הצרכן.

סעיף 51: הפרה נמשכת והפרה חוזרת לאחר התראה

(א) נמסרה למפר התראה מינהלית לפי הוראות סימן זה והמפר המשיך להפר את ההוראה שבשלה נמסרה לו ההתראה, ימסור לו ראש הרשות להגנת הפרטיות דרישת תשלום בשל הפרה נמשכת כאמור בסעיף 43(א); דרישת תשלום אינה גורעת מזכותו של המפר לטעון כאמור בסעיף 41 לעניין סכום העיצום הכספי ולעניין הימשכות ההפרה, וייחולו הוראות סעיפים 41 ו-42, בשינויים המחויבים.

(ב) נמסרה למפר התראה מינהלית לפי הוראות סימן זה והמפר חזר והפר את ההוראה שבשלה נמסרה לו ההתראה, בתוך שנתיים מיום מסירת ההתראה, יראו את ההפרה הנוספת כאמור כהפרה חוזרת לעניין סעיף 43(ב), וראש הרשות להגנת הפרטיות ימסור למפר הודעה על כוונת חיוב לפי הוראות סעיף 40 בשל ההפרה החוזרת.

<u>סימן ג': התחייבות להימנע מהפרה</u>

סעיף 52: התחייבות להימנע מהפרה והפקדת עירבון

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 38, והתקיימו נסיבות המנויות בנהלים שקבע ראש הרשות להגנת הפרטיות, רשאי הוא להציע למפר, בהודעה בכתב, להגיש לו כתב התחייבות ועירבון מסוג שייקבע בנהלים, לפי הוראות סימן זה, במקום שיוטל עליו עיצום כספי לפי הוראות סימן א'.

(ב) בכתב ההתחייבות יתחייב המפר להפסיק את הפרת ההוראה כאמור בסעיף קטן (א), ולהימנע מהפרה נוספת של אותה הוראה בתוך תקופה שיקבע ראש הרשות להגנת הפרטיות, שתחילתה ביום מסירת ההודעה כאמור באותו סעיף קטן, ובלבד שהתקופה האמורה לא תעלה על שנתיים (בסימן זה – תקופת ההתחייבות).

(ג) ראש הרשות להגנת הפרטיות רשאי לדרוש כי המפר יכלול בכתב ההתחייבות תנאים נוספים שעליו לעמוד בהם בתקופת ההתחייבות לשם הקטנת הנזק שנגרם מההפרה או מניעת הישנותה.

(ד) נוסף על כתב ההתחייבות יפקיד המפר בידי ראש הרשות להגנת הפרטיות עירבון בסכום העיצום הכספי שראש הרשות להגנת הפרטיות היה רשאי להטיל על המפר בשל אותה הפרה, בהתחשב בקיומן של מקרים, נסיבות ושיקולים שנקבעו לפי סעיף 44.

דברי הסבר

<u>סעיף 51:</u> מבוסס על סעיפים 23לא להצ"ח תיקון מס' 13 ו-22טו לחוק הגנת הצרכן.

<u>סעיף 52:</u> מבוסס על סעיפים 23לב ו-23לג להצ"ח תיקון מס' 13 ועל סעיפים 22טז ו-22יז לחוק הגנת הצרכן.

סעיף 53: תוצאות הגשת כתב התחייבות ועירבון או אי הגשתם

(א) הגיש המפר לראש הרשות להגנת הפרטיות כתב התחייבות ועירבון לפי סימן זה, בתוך 45 ימים מיום מסירת ההודעה כאמור בסעיף 52, לא יוטל עליו עיצום כספי בשל אותה הפרה.

(ב) לא הגיש המפר לראש הרשות להגנת הפרטיות כתב התחייבות ועירבון בתוך 45 ימים מיום מסירת ההודעה כאמור בסעיף 52, ימציא לו ראש הרשות להגנת הפרטיות הודעה על כוונת חיוב בשל אותה הפרה, לפי סעיף 40.

סעיף 54: הפרת התחייבות

(א) הגיש המפר כתב התחייבות ועירבון לפי סימן זה והפר תנאי מתנאי ההתחייבות, כמפורט להלן, יחולו הוראות אלה, לפי העניין:

(1) המשיך המפר, במהלך תקופת ההתחייבות, להפר את ההוראה שבשל הפרתה נתן את כתב ההתחייבות – יחלט ראש הרשות להגנת הפרטיות את העירבון וימציא למפר דרישת תשלום בשל ההפרה הנמשכת כאמור בסעיף 43(א);

(2) חזר המפר והפר, במהלך תקופת ההתחייבות, את ההוראה שבשל הפרתה נתן את כתב ההתחייבות – יחלט ראש הרשות להגנת הפרטיות את העירבון ויראו את ההפרה הנוספת כאמור כהפרה חוזרת לעניין סעיף 43(ב); ראש הרשות להגנת הפרטיות ימציא למפר הודעה על כוונת חיוב בשל ההפרה החוזרת;

(3) הפר המפר תנאי מהתנאים הנוספים שנקבעו בכתב ההתחייבות כאמור בסעיף 52 – יודיע ראש הרשות להגנת הפרטיות למפר על כוונתו לחלט את העירבון; המפר רשאי לטעון את טענותיו לעניין זה, בכתב או בעל פה, כפי שיורה ראש הרשות להגנת הפרטיות, בתוך 45 ימים מיום הודעת ראש הרשות להגנת הפרטיות, וראש הרשות להגנת הפרטיות רשאי, לבקשת המפר, להאריך תקופה זו בתקופה נוספת שלא תעלה על 45 ימים.

(ב) לעניין פרק זה, יראו בחילוט העירבון לפי הוראות סעיף זה, כהטלת עיצום כספי על המפר בשל ההפרה שלגביה ניתן העירבון.

(ג) הופר תנאי מתנאי ההתחייבות כאמור בסעיף זה, והפר המפר פעם נוספת את ההוראה שבשל הפרתה נתן את כתב ההתחייבות, לא יאפשר לו ראש הרשות להגנת הפרטיות להגיש כתב התחייבות נוסף לפי הוראות סימן זה, בשל אותה הפרה.

סעיף 55: השבת העירבון

עמד המפר בתנאי כתב ההתחייבות שמסר לפי סימן זה, יוחזר לו, בתום תקופת ההתחייבות, העירבון שהפקיד; העירבון, למעט אם היה ערבות בנקאית, יוחזר בתוספת הפרשי הצמדה וריבית מיום הפקדתו עד יום החזרתו.

סימן ד': הוראות כלליות

סעיף 56: עיצום כספי בשל הפרה לפי חוק זה ולפי חוק אחר

על מעשה אחד המהווה הפרה של הוראה מהוראות לפי חוק זה המנויות בסעיף 38 ושל הוראה מההוראות לפי חוק אחר, לא יוטל יותר מעיצום כספי אחד.

דברי הסבר

סעיפים 56-53: מבוססים על סעיפים 23לד-23לז בהצ"ח תיקון מס' 13 ועל סעיפים 22יז-22יט ו-22כג לחוק הגנת הצרכן.

סעיף 23לח להצ"ח תיקון מס' 13, העוסק בעיכוב הביצוע של החלטת ראש הרשות להגנת הפרטיות לעניין הטלת עיצום כספי והחזר עיצום כספי ששולם או עירבון שהופקד במקרה של ערעור על החלטת ראש הרשות להגנת הפרטיות להפעיל את סמכותו המינהלית לפי פרק זה, לא אומץ בהצעת החוק, שכן הנושא צריך להיות מטופל במסגרת הדינים הכלליים, ובמקרה שלנו – חוק בתי המשפט לעניינים מינהלים, תש"ס–2000.

סעיף 57: פרסום לעניין הטלת עיצום כספי

(א) הטיל ראש הרשות להגנת הפרטיות עיצום כספי לפי פרק זה, יפרסם באתר האינטרנט של הרשות להגנת הפרטיות את הפרטים שלהלן, באופן שיבטיח שקיפות לגבי הפעלת שיקול דעתו בקבלת ההחלטה להטיל עיצום כספי:

(1) דבר הטלת העיצום הכספי;

(2) מהות ההפרה שבשלה הוטל העיצום הכספי ונסיבות ההפרה, לרבות מספר נושאי המידע שמידע אישי על אודותיהם נחשף או עלול להיחשף עקב ההפרה;

(3) סכום העיצום הכספי שהוטל;

(4) אם הופחת העיצום הכספי – הנסיבות שבשלהן הופחת סכום העיצום ושיעורי ההפחתה;

(5) פרטים על אודות המפר, הנוגעים לעניין;

(6) שמו של המפר – ככל שהמפר הוא תאגיד.

(ב) הוגשה עתירה לבית המשפט לעניינים מינהליים או הוגש ערעור על החלטה בעתירה כאמור, יפרסם ראש הרשות להגנת הפרטיות, בפרסום לפי סעיף קטן (א), גם את דבר הגשת העתירה או הערעור ואת תוצאותיהם.

(ג) על אף הוראות סעיף קטן (א)(6), רשאי ראש הרשות להגנת הפרטיות לפרסם את שמו של מפר שהוא יחיד, אם סבר שהדבר נחוץ לצורך אזהרת הציבור.

(ד) פרסום לפי סעיף זה בעניין עיצום כספי שהוטל על תאגיד יהיה לתקופה של ארבע שנים, ובעניין עיצום כספי שהוטל על יחיד – לתקופה של שנתיים.

דברי הסבר

<u>סעיף 57:</u> מבוסס על סעיפים 23לט להצ"ח תיקון מס' 13 ו-22כא לחוק הגנת הצרכן.

בס"ק (א) הועדף ההסדר שבסעיף 22כא לחוק הגנת הצרכן. כמו כן נקבע בו שהפרסום ייעשה באתר האינטרנט של הרשות להגנת הפרטיות ולא יפורסם באתר האינטרנט של משרד המשפטים או בדרך אחרת על פי החלטת ראש הרשות להגנת הפרטיות.

ס"ק (א)(2) מבהיר שמספר נושאי המידע, שמידע אישי עליהם נחשף או עלול להיחשף עקב ההפרה, הוא מידע שרלוונטי לבחינה של שיקול הדעת של ראש הרשות בהטלת העיצום הכספי, ולכן יש לפרסמו כחלק מנסיבות ההפרה.

סעיף 23לט(ו) להצ"ח תיקון מס' 13 לא אומץ בהצעת החוק משום שיש בו משום התערבות יתרה ופגיעה בגמישות של סמכויות העזר הנתונות בידי השר האחראי או בידי ראש הרשות להגנת הפרטיות. בחוק ההגבלים העסקיים ובחוק ניירות ערך, למשל, אין הוראה דומה לדרכי פרסום נוספות של דבר הטלת עיצום כספי.

ס"ק (ד) מגביל את פרסום דבר הטלת עיצום כספי לתקופה של 4 שנים כאשר העיצום הכספי הוטל על תאגיד ולשנתיים כאשר העיצום הכספי הוטל על אדם יחיד. הסעיף מחייב בכך את ראש הרשות להגנת הפרטיות למחוק את הפרסום מאתר האינטרנט בתום התקופה האמורה.

סעיף 58: שמירת אחריות פלילית

(א) תשלום עיצום כספי, המצאת התראה מינהלית או מתן כתב התחייבות ועירבון, לפי פרק זה, לא יגרעו מאחריותו הפלילית של אדם בשל הפרת הוראה מההוראות לפי חוק זה המפורטות בסעיף 38, שהיא עבירה על חוק זה.

(ב) על אף האמור בסעיף קטן (א), נמסרה למפר הודעה על כוונת חיוב, או התראה מינהלית או הגיש המפר כתב התחייבות ועירבון, בשל הפרה כאמור באותו סעיף קטן, לא יוגש נגדו כתב אישום בשל אותו מעשה, אלא אם כן התגלו עובדות או ראיות חדשות, המצדיקות זאת.

(ג) שילם המפר עיצום כספי או הפקיד עירבון והוגש נגדו כתב אישום בנסיבות האמורות בסעיף קטן (ב), יוחזר לו הסכום ששילם או העירבון; הסכום ששילם המפר כאמור או עירבון, למעט ערבות בנקאית, יוחזר בתוספת הפרשי הצמדה וריבית מיום תשלומו או הפקדתו עד יום החזרתו.

(ד) הוגש נגד אדם כתב אישום בשל הפרה המהווה עבירה כאמור בסעיף קטן (א), לא ינקוט נגדו ראש הרשות להגנת הפרטיות הליכים לפי פרק זה בשל אותה הפרה.

סעיף 59: אישור נהלים ופרסומם

נהלי ראש הרשות להגנת הפרטיות לפי סעיפים 49 ו-52 טעונים אישור היועץ המשפטי לממשלה או משנה ליועץ המשפטי שהוא הסמיך לכך, והם יפורסמו באתר האינטרנט של הרשות להגנת הפרטיות.

סעיף 60: אצילת סמכויות

ראש הרשות להגנת הפרטיות רשאי לאצול את סמכויותיו לפי פרק זה, למעט קביעת נהלים לפי סעיפים 49(א) ו-52(א), לסגנו או לעובד הרשות להגנת הפרטיות האחראי לנושא העיצומים הכספיים.

דברי הסבר

<u>סעיף 58:</u> מבוסס על סעיפים 23מ להצ"ח תיקון מס' 13 ו-22כב לחוק הגנת הצרכן. במקרים של אי-התאמה הועדף הנוסח הקבוע בחוק הגנת הצרכן מתוך הנחה שהוא העדכני ביותר. הסעיף משקף את הצורך הממשי באכיפה פלילית לצד זו המינהלית. המטרה היא לצמצם את מספר ההפרות ה"משתלמות כלכלית" באמצעות ה"שוט" של האחריות הפלילית. עם זאת, כדי להפיג את חוסר הוודאות הנלווה לחשש מסיכון כפול, כלומר ממצב שהמפר חשוף לאכיפה מינהלית ואינו זוכה לסופיות הדיון כי הוא עדיין חשוף לסנקציה פלילית, יש לקבוע בנהלים קריטריונים ברורים לאכיפה פלילית ולאכיפה מינהלית.

<u>סעיף 59:</u> מבוסס על סעיף 22כד לחוק הגנת הצרכן. מטרתו ליצור סעיף-סל לאישור הנהלים שקובע ראש הרשות להגנת הפרטיות. הסעיף הוא חלופה לאזכור הצורך באישור בכל סעיף חוק רלוונטי, כפי שנעשה בהצ"ח תיקון מס' 13 בסעיפים 23כט(א) ו-23לב.

<u>סעיף 60:</u> מבוסס על סעיף 22כה לחוק הגנת הצרכן.

פרק ה: מסירת מידע אישי או ידיעות מאת גופים ציבוריים

הנושא מצריך מחקר נפרד, שאינו בליבת עבודתנו הנוכחית לגיבוש הצעה לחוק הגנת פרטיות חדש ומעודכן.

פרק ו: עוולה אזרחית ועונשין

סעיף 61: פגיעה בפרטיות – עוולה אזרחית

הפרת הוראה מההוראות לפי סעיפים 4, 9, 11, 13 עד 15, או הוראה שנקבעה לפי סעיף 16 לעניין האופן והתנאים למימוש זכות לפי סעיפים 11, 13, 14 או 15, היא עוולה אזרחית והוראות פקודת הנזיקין [נוסח חדש][35] יחולו עליה בכפוף להוראות חוק זה.

סעיף 62: פגיעה בפרטיות – עבירה

הפוגע בפרטיות זולתו באחת מהדרכים האמורות בסעיף 4, דינו – מאסר 5 שנים; נעברה העבירה או היתה מכוונת כלפי קשישים, חסרי ישע או קטינים, או כלפי ציבור של נושאי מידע הנתונים במצב של חולשה שכלית, נפשית או גופנית– דינו של עובר העבירה מאסר שבע שנים.

דברי הסבר

סעיף 61: בא במקום סעיף 31ב לחוק הגנת הפרטיות הקיים ומבוסס על סעיף 4 לחוק הגנת הפרטיות הקיים, אך מרחיב אותו לכל פגיעה בפרטיות ולכל פגיעה בזכות מזכויות נושא המידע.

סעיף 62: מבוסס על סעיף 5 לחוק הגנת הפרטיות הקיים ובא במקום סעיף 16 לחוק הגנת הפרטיות הקיים.

הסעיף שואב השראה מסעיף 23א לחוק הגנת הצרכן. הוא מחמיר את הענישה כאשר העבירה נעברה כלפי אוכלוסיות חלשות כגון קטינים, קשישים וחסרי ישע, מתוך הבנה שאוכלוסיות אלו, ולא רק קטינים, כמוצע בהצ"ח פרטיות קטינים, עלולות להיתקל בקשיים בהתמודדות עם השימוש בשירותים מקוונים.

סעיפים 23מא-23מה להצ"ח תיקון מס' 13 לא אומצו בהצעת החוק מאחר שמקצתם מכוסים גם כך בהוראת סעיף 62, מקצתם נוגעים להוראות בדין המהותי שאינן מופיעות בהצעת החוק, למשל חובת רישום מאגר מידע, ומקצתם רחבים מדי.

סעיף 6 לחוק הגנת הפרטיות הקיים לא אומץ בהצעת החוק, שכן הוראתו ש"לא תהיה זכות לתביעה אזרחית או פלילית לפי חוק זה בשל פגיעה שאין בה ממש" מוסדרת בעקרונות הכלליים של דיני הנזיקין ושל דיני העונשין.

סעיף 31א בחוק הגנת הפרטיות הקיים, המגדיר מהן עבירות אחריות קפידה, לא אומץ בהצעת החוק. הותרת הוראה בעניין אחריות קפידה מגבירה את הסיכון הכפול שבשמירת האחריות הפלילית לפי סעיף 58. נוסיף גם כי אין הוראה דומה בדברי חקיקה אחרים, ששילבו הוראות לאכיפה מינהלית, למשל התיקון משנת 2012 לחוק ההגבלים העסקיים[36] והתיקון משנת 2014 לחוק הגנת הצרכן.[37]

סעיף 63: פיצוי בלא הוכחת נזק

(א) הורשע אדם בעבירה לפי סעיף 62 רשאי בית המשפט לחייבו לשלם לנפגע פיצוי שלא יעלה על 50,000 שקלים חדשים, בלא הוכחת נזק; הורשע אדם בעבירה לפי סעיף 62 לעניין קטין, קשיש, חסר ישע או ציבור של נושאי מידע הנתונים במצב של חולשה שכלית, נפשית או גופנית, רשאי בית המשפט לחייב את הפוגע לשלם לנפגע פיצוי שלא יעלה על כפל הסכום האמור, בלא הוכחת נזק. חיוב בפיצוי לפי סעיף קטן זה הוא כפסק דין של אותו בית משפט שניתן בתובענה אזרחית של הזכאי נגד החייב בו.

(ב)

(1) במשפט בשל עוולה אזרחית לפי סעיף 61 עקב הפרת הוראת סעיף 4(8), רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על 50,000 שקלים חדשים, בלא הוכחת נזק.

(2) במשפט כאמור בפסקה (1) שבו הוכח כי הפגיעה בפרטיות נעשתה בכוונה לפגוע, רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על כפל הסכום כאמור באותה פסקה, בלא הוכחת נזק.

(3) במשפט כאמור בפסקה (1) שבו הוכח כי הפגיעה בפרטיות נעשתה או היתה מכוונת כלפי קשישים, חסרי ישע או קטינים, או כלפי ציבור של נושאי מידע הנתונים במצב של חולשה שכלית, נפשית או גופנית, רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על כפל הסכום כאמור באותה פסקה, בלא הוכחת נזק.

(ג) לא יקבל אדם פיצוי בלא הוכחת נזק לפי סעיף זה, בשל אותה פגיעה בפרטיות, יותר מפעם אחת.

דברי הסבר

<u>סעיף 63:</u> מבוסס על סעיף 29א לחוק הגנת הפרטיות הקיים, בשילוב התיקונים המוצעים בעניין החמרת הענישה כאשר הפגיעה היא בפרטיותם של נושאי מידע מאוכלוסיות חלשות.

ס"ק (ב) מגביל את מתן הפיצויים בלא הוכחת נזק בשל עוולה אזרחית רק להפרה של הוראת סעיף 4(8) להצעת החוק הנוגעת לעיבוד מידע אישי. המטרה היא להגביר את ההרתעה מפני עיבוד מידע אישי בניגוד להוראת הצעת חוק זו.

סעיף 64: שיקולים בגזירת הדין או גובה הפיצוי

בבואו לגזור את הדין או לפסוק פיצויים רשאי בית המשפט להתחשב, לטובת הנאשם, הנתבע או הצד להליך מינהלי, גם באלה:

(1) חומרת הפגיעה בפרטיות;

(2) היקף הפגיעה בפרטיות;

(3) משך הזמן שבו בוצעה הפגיעה בפרטיות;

(4) הנזק הממשי שנגרם לנפגע בעבירה או לתובע, לפי העניין, להערכת בית המשפט;

(5) הרווח שצמח לנאשם או לנתבע, לפי העניין, בשל הפגיעה בפרטיות, להערכת בית המשפט;

(6) מאפייני הפעילות של הנאשם או הנתבע, לפי העניין;

(7) טיב היחסים בין הנפגע בעבירה לבין הנאשם, או הנתבע לתובע, לפי העניין;

(8) תום ליבו של הנאשם או הנתבע;

(9) טיב תהליך עיצוב לפרטיות שהתבצע לפי סעיף 19.

דברי הסבר

<u>סעיף 64:</u> מבוסס על סעיף 56(ב) לחוק זכויות יוצרים, התשס"ח-2007, ומחליף את סעיף 22 לחוק הגנת הפרטיות הקיים, שלא מציג מכניזם ברור דיו לבית המשפט בקובעו את סכום הפיצוי בגין פגיעה בפרטיות.

פרק ז: הגנות

סעיף 65: הגנות מה הן

(א) בכל הליך משפטי או משמעתי לפי חוק זה, תהא זו הגנה טובה אם נתקיימה אחת מאלה:

(1) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי סעיף 13 לחוק איסור לשון הרע, התשכ"ה–1965[38] (בסעיף זה – חוק איסור לשון הרע);

(2) עיבוד של המידע האישי נדרש לשם מילוי חובה על פי דין המוטלת על בעל השליטה במידע או המעבד;

(3) הנתבע, הנאשם או צד להליך מינהלי עשה את הפגיעה בתום לב באחת הנסיבות האלה –

(א) הוא לא ידע ולא היה עליו לדעת על אפשרות הפגיעה בפרטיות;

(ב) הפגיעה נעשתה בנסיבות שבהן היתה מוטלת על הפוגע חובה חוקית או מקצועית לעשותה; לענין פסקה זו, "חובה מקצועית" – חובה לפי עקרונות או כללים של אתיקה מקצועית, החלים עליו מכוח דין או המקובלים על אנשי המקצוע שהוא נמנה עמהם;

(ג) הפגיעה נעשתה לשם הגנה על עניין אישי כשר של הפוגע;

(ד) הפגיעה נעשתה תוך ביצוע עיסוקו של הפוגע כדין ובמהלך עבודתו הרגיל, ובלבד שלא נעשתה דרך פרסום ברבים;

(ה) הפגיעה היתה בדרך של צילום או בדרך של פרסום של תצלום או של תוצר של תיעוד על אודות אדם, שנעשה ברשות הרבים ודמות הנפגע מופיעה בו באקראי;

(ו) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי פסקאות (4) עד (11) לסעיף 15 לחוק איסור לשון הרע;

(ז) הפגיעה היתה נחוצה כדי להגן על חייו, חירותו, בריאותו או שלמות גופו של הנפגע או של אדם אחר;

(4) בפגיעה היה עניין ציבורי המצדיק אותה בנסיבות העניין, ובלבד שאם היתה הפגיעה בדרך של פרסום – הפרסום לא היה כוזב;

(5) הנפגע הוא קשיש, חסר ישע או קטין או שהיה קטין בעת הפגיעה בפרטיותו, והפגיעה נעשתה על ידי הורהו או אפוטרופס שנתמנה לו כדין, לשם הגנה על עניין אישי כשר שלו.

(ב) חזקה על הנאשם, הנתבע או צד להליך מינהלי שעשה את הפגיעה בפרטיות שלא בתום לב אם התקיים אחד מאלה:

(1) הוא פגע ביודעין במידה העולה על הנדרש לצורך עניין מהעניינים שניתנה עליהם הגנה;

(2) נושא המידע שנפגע דרש ממנו לתקן את המידע האישי על אודותיו לפי סעיף 13 והוא סירב שלא כדין לעשות כן.

דברי הסבר

סעיף 65: ס"ק (א) מבוסס על סעיף 18 בחוק הגנת הפרטיות הקיים, אך ההגנות הורחבו לכל הליך משפטי או משמעתי כדי שיכלול גם הליכי אכיפה מינהלית וגם הליכים אחרים שאינם פליליים או אזרחיים.

ס"ק (א)(1) זהה לסעיף 18(1) בחוק הגנת הפרטיות הקיים.

ס"ק (א)(2) מבוסס על סעיף 6(1)(c) ל-GDPR, אך הוסף כהגנה ולא כבסיס לגיטימי לעיבוד מידע אישי, כפי שקבוע ב-GDPR. המטרה היא שלא להטיל על נושא המידע את הנטל שבהוכחת תנאיו של ס"ק (א)(2).

ס"ק (א)(3)(א) מבוסס על סעיף 18(2)(א) לחוק הגנת הפרטיות הקיים, אבל מאחר שהרחבנו את ההגנות לכל הליך משפטי או משמעתי, בחרנו שלא להתייחס רק ל"נתבע או נאשם" אלא גם לצד בהליך מינהלי.

ס"ק (א)(3)(ב) מבוסס על סעיף 18(2)(ב) לחוק הגנת הפרטיות הקיים, אך הוא מחדד את ההבנה מהי חובה מקצועית ומסיר את ההתייחסות לחובה חברתית ומוסרית שמשמעותן והיקפן אינן ברורות. המטרה היא להימנע מפסיקות מרחיבות המתירות פגיעה בפרטיות בכסות של חובה מוסרית או חברתית.

ס"ק (א)(3)(ג) זהה לסעיף 18(2)(ג) לחוק הגנת הפרטיות הקיים.

ס"ק (א)(3)(ד) מבוסס על סעיף 18(2)(ד) בחוק הגנת הפרטיות הקיים.

ס"ק (א)(3)(ה) מבוסס על סעיף 18(2)(ה) בחוק הגנת הפרטיות הקיים. עם זה, לפעולת ה"צילום" הוספה פעולת "תיעוד" כדי להרחיב את ההגנה גם לקליטה אקראית של מידע אישי על הנפגע באמצעות חיישנים המוצבים במרחב הציבורי. לדוגמה: עיבוד בחיישני קול ובמפות חום במרחב הציבורי לצורך מעקב ומניעת פשיעה.

ס"ק (א)(3)(ו) זהה לסעיף 18(2)(ו) לחוק הגנת הפרטיות הקיים.

ס"ק (א)(3)(ז) שאב השראה מסעיפים 6(1)(d), 9(2)(c) ו-9(2)(i) ל-GDPR, אך הוסף כהגנה ולא כבסיס לגיטימי לעיבוד של מידע אישי, כפי שקבוע ב-GDPR. המטרה היא שלא להטיל על נושא המידע את הנטל שבהוכחת תנאי הסעיף.

ס"ק (א)(4) זהה לסעיף 18(3) לחוק הגנת הפרטיות הקיים.

ס"ק (א)(5) מבוסס על החמרת הענישה כאשר העבירה או הפגיעה היא בנושאי מידע מאוכלוסיות חלשות, כמוצע בסעיף 62 להצעת החוק ובסעיף 1א להצ"ח פרטיות קטינים.

ס"ק (ב) מבוסס על סעיף 20 לחוק הגנת הפרטיות הקיים. הכללת חזקת תום הלב בסעיף ההגנות נועדה להצביע על כך שיש לְפרשה בצמצום ואך ורק בהקשר של ההגנות המפורטות בסעיף קטן (א).

ס"ק (ב)(1) מבוסס על סעיף 20(ב) לחוק הגנת הפרטיות הקיים.

ס"ק (ב)(2) מבוסס על סעיף 17(א) לחוק איסור לשון הרע, העוסק בשלילת הגנת תום הלב. מטרתו לתת בידי נושא המידע כלי נוסף שיבטיח שבקשתו לתיקון מידע אישי עליו לפי סעיף 13 תישקל במלוא תשומת הלב וכראוי.

סעיף 66: פטור
לא יישא אדם באחריות לפי חוק זה על מעשה שהוסמך לעשותו על פי דין.

סעיף 67: הפרכה של טענות הגנה
הביא הנאשם, הנתבע או הצד להליך מינהלי ראיה, או העיד בעצמו כדי להוכיח את אחת ההגנות הניתנות בחוק זה, רשאי התובע או הצד שכנגד להביא ראיות סותרות; אין בהוראה זו כדי לגרוע מסמכות בית המשפט לפי כל דין להתיר הבאת ראיות בידי בעלי הדין.

פרק ח: הוראות שונות

סעיף 68: דין המדינה
חוק זה חל על המדינה.

סעיף 69: מות הנפגע
(א) אדם שנפגע בפרטיותו ותוך שישה חודשים לאחר הפגיעה מת בלי שהגיש תובענה או קובלנה בשל אותה פגיעה, רשאים בן זוגו, ילדו או הורהו, ואם לא השאיר בן זוג, ילדים או הורים – אחיו או אחותו, להגיש, תוך שישה חודשים לאחר מותו, תובענה או קובלנה בשל אותה פגיעה.

(ב) אדם שהגיש תובענה או קובלנה בשל פגיעה בפרטיות ומת לפני סיום ההליך, רשאים בן זוגו, ילדו או הורהו, ואם לא השאיר בן זוג, ילדים או הורים – אחיו או אחותו, להודיע לבית המשפט, תוך ששה חודשים לאחר מותו, על רצונם להמשיך בתובענה או בקובלנה, ומשהודיע כאמור יבואו הם במקום התובע או הקובל.

דברי הסבר

<u>סעיף 66:</u> מבוסס על סעיף 19(א) לחוק הגנת הפרטיות הקיים.

סעיף 19(ב) לחוק הגנת הפרטיות הקיים לא אומץ בהצעת החוק. מאז חקיקת סעיף 19(ב) בשנת 1981 התרחשה המהפכה החוקתית והזכות לפרטיות עוגנה כאחת מזכויות היסוד החוקתיות בחוק-יסוד: כבוד האדם וחירותו. כתוצאה מכך, אין להתיר היום פגיעה בחוק בזכות לפרטיות באופן שאינו עומד בדרישות פסקת ההגבלה. בנוסף, סמכות מעקב ופגיעה גורפת בפרטיות לרשויות ביטחון יכולה להיות אבן נגף בפני הכרה אירופית (adequacy) שרמת הגנת הפרטיות בדין הישראלי תואמת את זו האירופית.[39] יש צורך לקבוע הסמכה מפורשת ומידתית בחוק ייעודי שתעסוק בשימוש בטכנולוגיות לשם מעקב ומניעת פשיעה.

<u>סעיף 67:</u> זהה לסעיף 21 בחוק הגנת הפרטיות הקיים, אך לאור הרחבת ההגנות לכל הליך משפטי או משמעתי הוספנו גם את המילים "צד להליך מינהלי".

<u>סעיף 68:</u> זהה לסעיף 24 לחוק הגנת הפרטיות הקיים.

<u>סעיף 69:</u> זהה לסעיף 25 לחוק הגנת הפרטיות הקיים.

סעיף 26 לחוק הגנת הפרטיות הקיים, המגביל את תקופת ההתיישנות של תביעה אזרחית לשנתיים, לא אומץ בהצעת החוק. לנוכח חשיבותה של הזכות לפרטיות כזכות יסוד חוקתית מוצע להשוות את תקופת ההתיישנות הקבועה בהצעת החוק לתקופה הנהוגה בעוולות אזרחיות אחרות. ככל שמדובר בתקופת התיישנות שאינה חורגת מן הקבוע בחוק ההתיישנות, התשי"ח–1958, אין צורך בקביעה מיוחדת בחוק הפרטני, ולכן אין הצדקה לקביעת הוראה בנוגע להתיישנות בהצעת החוק.

סעיף 70: סייג לפרסום הליכים

במשפט פלילי או אזרחי בשל פגיעה בפרטיות רשאי בית המשפט מיוזמתו או לבקשת בעל דין, לאסור או לעכב זמנית, מנימוקים שירשמו, פרסום ברבים של הליכי בית המשפט – לרבות כתבי טענות, כתבי בי-דין אחרים, כתב אישום ודבר הגשתם של אלה ולרבות פסק דין כל עוד אינו חלוט – במידה שראה צורך בכך לשם הגנה על פרטיותו של אדם הנוגע במשפט; העובר על האיסור לפי סעיף זה, דינו – מאסר ששה חודשים או קנס _____.

סעיף 71: דין שני משפטים

על הליכים משפטיים בשל פגיעה בפרטיות יחולו הוראות סעיף 77 לחוק בתי המשפט [נוסח משולב], התשמ"ד–1984.

סעיף 72: צווים נוספים

הוראת סעיף 29 בחוק הגנת הפרטיות הקיים לא נדונה בקבוצת המומחים.

סעיף 73: חומר פסול לראיה

חומר שהושג תוך פגיעה בפרטיות יהיה פסול לשמש ראיה בבית משפט, ללא הסכמת הנפגע, זולת אם בית המשפט התיר מטעמים שיירשמו להשתמש בחומר, או אם היו לפוגע, שהיה צד להליך, הגנה או פטור לפי חוק זה.

סעיף 74: דו"ח הגנה על הפרטיות

לא יאוחר מ-1 באפריל בכל שנה יגיש ראש הרשות להגנת הפרטיות לוועדת החוקה חוק ומשפט של הכנסת דין וחשבון על פעולותיה של הרשות, ובכלל זה פעולות האכיפה והפיקוח לפי חוק זה בשנה שקדמה להגשת הדוח, לרבות מספר העיצומים הכספיים שהוטלו, סכומם, בשל אילו הפרות הוטלו ומספר ההפרות החוזרות שבוצעו מתוך כלל ההפרות בשנה שקדמה למועד הדיווח.

סעיף 75: תיקון חוק בתי משפט לענינים מינהליים

בחוק בתי המשפט לענינים מינהליים, התש"ס–2000,[40] בתוספת הראשונה, במקום פרט 28 יבוא:

" 28. החלטה של הרשות להגנת הפרטיות לפי חוק הגנת הפרטיות, התשע"ט–2019".

דברי הסבר

<u>סעיפים 70-71:</u> מחליפים את סעיף 27 בחוק הגנת הפרטיות הקיים, המפנה לסעיפים 21 ו-23-24 בחוק איסור לשון הרע, התשכ"ה–1965. במקום ההפניה לסעיף 21 בחוק איסור לשון הרע, התשכ"ה–1965, הוספה לשון הסעיף במלואה, למעט ההוראה הקובעת שבית המשפט אינו יכול לעכב או לאסור פרסום דבר פתיחתו של הליך פלילי אם הנפגע התנגד לכך. הוראה זו מתאימה לדיני איסור לשון הרע ואין מקומה בהצעת חוק העוסקת בפגיעה בפרטיות. סעיף 23 בחוק איסור לשון הרע אינו רלוונטי בעולם דיגיטלי, ויש להחיל במקומו את דיני הראיות הרגילים. במקום ההפניה לסעיף 24 בחוק איסור לשון הרע הוספה בסעיף 71 להצעת החוק הפניה לסעיף 77 בחוק בתי המשפט [נוסח משולב], התשמ"ד–1984, שהיא עדכנית וברורה יותר.

<u>סעיף 73:</u> זהה לסעיף 32 לחוק הגנת הפרטיות הקיים.

<u>סעיף 74:</u> מבוסס על סעיפים 10א בחוק הגנת הפרטיות הקיים ו-22כו לחוק הגנת הצרכן, לעניין דיווח על אכיפה מינהלית.

<u>סעיף 75:</u> מבהיר שכל החלטה של הרשות להגנת הפרטיות היא החלטה מינהלית שמותר לעתור בגינה לבית המשפט לעניינים מינהליים.

סעיף 76: שמירת דינים

הוראות חוק זה לא יגרעו מהוראות כל דין אחר שהיה קיים ערב תחילתו של חוק זה.

סעיף 77: ביצוע ותקנות

שר המשפטים ממונה על ביצוע חוק זה והוא רשאי, באישור ועדת החוקה חוק ומשפט של הכנסת, להתקין תקנות בכל עניין הנוגע לביצועו, ובין השאר –

(1) תנאי החזקת מידע אישי ושמירתו;

(2) תנאים להעברת מידע אישי למחוץ לגבולות המדינה;

(3) תנאי אבטחת מידע אישי;

(4) הוראות לענין ביעור מידע עם הפסקת עיבודו.

סעיף 78: התאמה למדד

(א) הסכום לתשלום בגין מימוש זכות מזכויות נושא המידע לפי סעיף 16(ב) וסכום הפיצוי בלא הוכחת נזק לפי סעיף 63 יעודכנו ב-16 בכל חודש, בהתאם לשיעורי השינוי במדד החדש לעומת המדד הבסיסי, לעניין זה –
"המדד" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה;
"המדד החדש" – מדד החודש שקדם לחודש העדכון;
"המדד הבסיסי" – מדד חודש דצמבר 2018.

(ב) סכומי העיצום הכספי כאמור בסעיף 38 וסכום הקנס כאמור בסעיף 70 יעודכנו ב-1 בינואר בכל שנה (בסעיף קטן זה – "יום העדכון"), בהתאם לשיעור שינוי המדד הידוע ביום העדכון לעומת המדד שהיה ידוע ב-1 בינואר של השנה הקודמת; הסכום האמור יעוגל לסכום הקרוב שהוא מכפלה של 10 שקלים חדשים; לעניין זה, "מדד" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה. שר המשפטים יפרסם בהודעה ברשומות את סכום הקנס המעודכן לפי סעיף קטן זה. ראש הרשות להגנת הפרטיות יפרסם ברשומות הודעה על סכומי העיצום הכספי המעודכנים לפי סעיף קטן זה.

דברי הסבר

<u>סעיף 76:</u> מבוסס על סעיפים 35 בחוק הגנת הפרטיות הקיים ו-10 בחוק-יסוד: כבוד האדם וחירותו – מתוך הבנת חשיבותה ומרכזיותה של הזכות לפרטיות כזכות יסוד חוקתית.

<u>סעיף 77:</u> מבוסס על סעיף 36 לחוק הגנת הפרטיות הקיים ומותאם לנושאים ששר המשפטים מוסמך להתקין בעניינם תקנות לפי הצעת החוק.

<u>סעיף 78:</u> מבוסס על תקנה 6 לתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי דין בערעור על סירוב לבקשת עיון), התשמ"א–1981, ועל סעיף 23כה(ב) להצ"ח תיקון מס' 13. סעיף 78 הוא סעיף סל שמאגד את כל ההוראות הנוגעות לעדכון סכום כספי לפי הצעת החוק: תשלום בעבור מימוש זכות מזכויות נושא המידע לפי סעיף 16, פיצוי בלא הוכחת נזק לפי סעיף 63, עיצום כספי לפי סעיף 38 וקנס לפי סעיף 70.

1 חוק-יסוד: כבוד האדם וחירות, ס"ח התשנ"ב 1391.

2 ראו בג"ץ 6650/04 **פלונית נ' בית הדין הרבני האזורי נתניה**, פ"ד סא(1) 581 (2006).

3 ס"ח התשנ"ה 366.

4 ס"ח התשנ"ו 338.

5 הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח–2018 [להלן: "**הצ"ח תיקון מס' 13**"].

6 ס"ח התש"ע 256.

7 ס"ח התשס"א 62.

8 חוק נתוני אשראי, התשע"ו-2016, ס"ח 2551, עמ' 838.

9 ס"ח התשס"ח 72.

10 הצוות לבחינת החקיקה בתחום מאגרי המידע, דין וחשבון (ינואר 2007), עמ' 19-23 [להלן: "**ועדת שופמן**"].

11 דיני מדינת ישראל, נוסח חדש 12, עמ' 284.

12 הצעת חוק הגנת הפרטיות (תיקון – הגנה על פרטיות של קטינים), התשע"ז–2017 (להלן: "**הצ"ח פרטיות קטינים**").

13 ועדת שופמן, ה"ש 10 לעיל, עמ' 24.

14 תזכיר חוק הגנת הפרטיות (לצמצום חובת הרישום וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולתיעודם במסמכים), התשע"ב–2012.

15 אסף הרדוף, "צילום חכם: האם צילום מחשב ללא רשות ראוי להוות עברה פלילית", **משפטים** על אתר (2018).

16 Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/56/EC, 844/14/EN WP 217 (2014)

17 סעיף 6 לחוק הכשרות המשפטית והאפוטרופסות, התשכ"ו–1962, קובע: "פעולה משפטית של קטין שדרכם של קטינים בגילו לעשות כמוה, וכן פעולה משפטית בין קטין לבין אדם שלא ידע ולא היה עליו לדעת שהוא קטין, אינה ניתנת לביטול כאמור בסעיף 5, אף שנעשתה שלא בהסכמת נציגו, אלא אם היה בה משום נזק של ממש לקטין או לרכושו".

18 ועדת שופמן, ה"ש 10 לעיל, עמ' 42-47.

19 סעיף 3(ד)(7) לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007: "פרטי הזיהוי של המנוי או מיתקן בזק שנתוני התקשורת מתבקשים לגביהם, אם הם ידועים מראש, לרבות היות המנוי האמור מי שחל לגביו חיסיון מקצועי לפי כל דין (בחוק זה – בעל מקצוע); בפסקה זו, 'דין' – לרבות הלכה פסוקה;"

20 תקנה 5(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017, קובעת כך:

"5. (ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר סיכוני אבטחת מידע (להלן - סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשרה חודשים לפחות."

21 privacy Amendment (Notifiable Data Breaches) Act 2017 No. 12, 2017

22 ס"ח התשמ"ה 60.

23 ס"ח התשי"א 52.

24 ס"ח התשי"ט 86.

25 ס"ח התשי"ח 191.

26 שגיא כהן, "פייסבוק: מידע על 47 אלף ישראלים נחשף בפרשת קיימברידג' אנליטיקה", **Ynet** (10 באפריל 2018).

27 39th International Conference of Data Protection and Privacy Commissioners Hong Kong, Sep. 25-29, 2017, Resolution on exploring future options for International Enforcement Cooperation (2017);

28 FTC Earns Prestigious International Award for AshleyMadison.com Data Breach Investigation, FTC (Sep. 27, 2017)

29 ס"ח התשל"ז 266.

30 חוקי א"י, כרך א', עמ' (ע) 439, (א) 467.

31 ס"ח התשס"ב 468.

32 ס"ח התשל"ז 266.

33 ס"ח התשכ"א 192.

34 ס"ח התשנ"ה 170.

35 דיני מדינת ישראל, נוסח חדש 10, עמ' 266.

36 חוק ההגבלים העסקיים (תיקון מס' 13), התשע"ב–2012.

37 חוק הגנת הצרכן (תיקון מס' 39), התשע"ד–2014.

38 ס"ח התשכ"ה 240.

39 סמכות המעקב והפגיעה הגורפת בפרטיות על ידי ה-NSA בארצות הברית, כפי שנתגלה מהמסמכים שחשף סנאודן, הייתה הסיבה העיקרית לביטול ה-safe harbor בארצות הברית (Maximillian Schrems v. Data Protection *Commissioner*, Case C–362/14, October 6, 2015, (ECLI:EU:C:2015:650), ודיונים בהכרה בתאימות הדין ביפן ובאנגליה ל-GDPR עסקו בסמכות המעקב הניתנת לרשויות הביטחון בכל אחת מהמדינות. ראו Andrew D. Murray, *Data Transfers between the EU and UK Post Brexit?*, 7(3) International Data Privacy Law 149 (2017); Claude Moraes, Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection of personal data afforded by Japan (2018q2979 (RSP))

40 ס"ח התש"ס 190.

השוואת נוסחים

בין חוק הגנת הפרטיות, התשמ"א–1981,
לבין נוסח הצעת חוק הגנת הפרטיות, התשע"ט–2019,

ודברי הסבר מקוצרים

פרק א: מטרות, פרשנות ועקרונות יסוד~~פגיעה בפרטיות~~

1. מטרת החוק

חוק זה מטרתו להגן על פרטיותו של אדם, לשם מימוש האוטונומיה של הפרט, ובכלל זה מתן הגנה על המרחב האישי של אדם, צנעת חייו האישיים, סוד שיחו, וזכותו לשלוט במידע אישי על אודותיו ובעיבודו; לשם הבטחת קיומו של הליך דמוקרטי תקין, ולשם מניעת השפעה בלתי הוגנת המבוססת על עיבוד מידע אישי על אודותיו.

העברת ההגדרות מסעיף 3 ו-7 בחוק הקיים לסעיף 2 המוצע.

2. הגדרות

בחוק זה –

"אבטחת מידע אישי" – הגנה על נכונות~~שלמות~~ המידע האישי, סודיותו, זמינותו או שלמותו~~או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין~~;

"אדם", לענין סעיף 1, ההגדרות "חסר ישע", "מידע אישי", "מידע רגיש", "נושא מידע", "קטין" ו-"קשיש" שבסעיף 2, וסעיפים 4, 9, 11, 23(ה), 63(ג), 65(א)(3)(ה), 65(א)(3)(ז), 69 ו-70 ~~סעיפים 2, 7, 13, 14, 17ב, 17ג, 17ו, 17ז, 23א, 23ב ו-25~~ – למעט תאגיד;

"אירוע אבטחה" – אירוע שבו נפגעה אבטחת מידע אישי;

בעל שליטה במידע" – אדם הקובע, לבד או ביחד עם אחר, את המטרות והדרכים לעיבוד מידע אישי;

דברי הסבר

סעיף 1: מטרתו לקדם את ההגנה על פרטיותו של אדם, שהיא זכות אדם חוקתית המעוגנת בחוק-יסוד: כבוד האדם וחירותו.[1] על בסיס ההכרה שהזכות לפרטיות היא זכות רחבה, שלא כל מופעיה מוגדרים במפורש בהצעת החוק, הסעיף מונה רשימה פתוחה של אפשרויות לפגיעה בפרטיות. הרשימה נעה על ציר שבין מניעת פגיעה בבחירה חופשית והבטחת הליך דמוקרטי תקין לבין הגנה על מרחב שבתוכו אדם זכאי להיות עם עצמו וזכותו לשלוט במידע אישי עליו ובעיבודו.[2] ככל זכות אדם אחרת גם הזכות לפרטיות היא יחסית ולא מוחלטת, ועל כן פגיעה בה תיתכן רק לפי דרישות פסקת ההגבלה שבסעיף 8 לחוק-יסוד: כבוד האדם וחירותו ובהתאם להצעת החוק.

סעיף 2: הגדרת **"אבטחת מידע אישי"** מבוססת על הגדרת המונח בסעיף 7 לחוק הגנת הפרטיות הקיים ועל מודל אבטחת המידע המקובל בעולם ובתעשייה, המבוסס על המשולש CIA (Confidentiality, Integrity, Availability): סודיות המידע האישי, נכונותו וזמינותו, כתנאים הדרושים להבטחה שהגישה אל המידע האישי תוגבל רק למי שמורשה לכך.

הגדרת **"אדם"** תואמת את ההגדרה בסעיף 3 לחוק הגנת הפרטיות הקיים, שבדומה להבחנה ב-GDPR, מבחינה בין אדם (natural person) לבין כל ישות משפטית (legal person) ובכלל זה תאגיד.

הגדרת **"אירוע אבטחה"** מבוססת על הגדרת המונח **"אבטחת מידע אישי"** ונועדה להדגיש שאירוע אבטחה הוא כל פגיעה במודל של ה-CIA לאבטחת המידע. ההגדרה מותירה מקום לתוספת של מדרג אירועי אבטחה, בדומה לקבוע בתקנות אבטחת מידע.

הגדרת **"בעל שליטה במידע"** מחליפה את הגדרת "מנהל מאגר מידע" בסעיף 7 לחוק הגנת הפרטיות הקיים ומבוססת על סעיף 4(7) ל-GDPR. מטרתה להגביר את תאימות הצעת החוק ל-GDPR.

"**בקשה לסיוע**" – בקשה לסיוע לרשות חוץ שהוגשה בכתב לרשות להגנת הפרטיות על ידי רשות חוץ;

"**גוף ציבורי**" –

(1)משרדי הממשלה ומוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין;

(2)גוף אחר שׂשר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, ובלבד שבצו ייקבעו סוגי המידע האישי והידיעות שהגוף יהיה רשאי למסור ולקבל;

"**דיני הגנת הפרטיות**" – דינים בתחום הגנת הפרטיות ופרטיות במידע שהרשות להגנת הפרטיות או רשות חוץ מופקדת על ביצועם ואכיפתם, ולעניין זה, משמעותם של מונחים בדיני הגנת הפרטיות במדינת חוץ תהא כמשמעותם בדין שבתחום סמכותה של רשות החוץ;

"**הסכמה**" - הסכמה מדעת ומרצון חופשי, במפורש או מכללא;

"**חוק המחשבים**" – חוק המחשבים, התשנ"ה–1995;

"**חוק המעצרים**" – חוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו–1996;

"**חוקר**" ו"**מפקח**" – מי שהוסמך לכך לפי סעיף 33;

"**חומר מחשב**" ו"**מחשב**" – כהגדרתם בחוק המחשבים;

"**חסר ישע**" – אדם שמחמת מחלתו, ליקויו הרוחני, מעצרו או כל סיבה אחרת אינו יכול לספק לעצמו את צרכי חייו;

"**חפץ**" – כהגדרתו בפקודת המעצר והחיפוש;

מידע "**אישי**" – נתונים על ~~אישיותו של~~ אודות אדם, מזוהה, לרבות נתונים המאפשרים במאמץ סביר את זיהויו של אדם~~מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו~~;

דברי הסבר

הגדרת "**בקשה לסיוע**" מבוססת על הגדרת המונח בסעיף 54יא1 לחוק ניירות ערך, התשכ"ח–1968 למעט ההתייחסות ל"מזכר הבנה". שיתוף המידע האישי בין הרשות להגנת הפרטיות לבין רשות חוץ אינו מותנה, לפי סעיף 32 להצעת החוק, בחתימה על מזכר הבנות.

הגדרת "**גוף ציבורי**" זהה להגדרה בסעיף 23 לחוק הגנת הפרטיות הקיים.

הגדרת "**דיני הגנת הפרטיות**" מבוססת על סעיף 54יא1 לחוק ניירות ערך, תשכ"ח–1968.

הגדרת "**הסכמה**" מבוססת על הגדרת המונח בסעיף 3 לחוק הגנת הפרטיות הקיים, בתוספת דרישת ה"רצון החופשי" כתנאי לתקפות ההסכמה. המטרה היא לחזק את דרישת ההסכמה כדרישה אפקטיבית, לצמצם את השימוש הגובר בהסכמה כדרישה צורנית בלבד וליצור את ההבנה שהסכמה אינה חזות הכול. הסכמה תיחשב לניתנת מ"רצון חופשי" כאשר מוכח שהיא ניתנה לאחר שנושא המידע ידע והבין, או סביר שידע והבין, את מטרת הפגיעה בפרטיותו ואת מידת הפגיעה, הסיכונים הכרוכים בה והאפשרויות העומדות לפניו ונתן את הסכמתו מרצונו החופשי. פרשנות זו עולה בקנה אחד עם תנאיה של דרישת ההסכמה ב-GDPR. עם זאת, ההגדרה מאפשרת לבית המשפט מרחב תמרון באמצעות המונחים "מדעת" וההכרה גם בהסכמה מכללא.

ההגדרות "**חוק המחשבים**", "**חומר מחשב**", ו"**חפץ**" זהות להגדרות בסעיף 23ט להצ"ח תיקון מס' 13.[3]

הגדרת "**חסר ישע**" מבוססת על סעיף 322 לחוק העונשין, התשל"ז–1977.

הגדרת "**מידע אישי**" מחליפה את הגדרת "מידע" בסעיף 7 לחוק הגנת הפרטיות הקיים ומתייחסת לנתונים בלי קשר לפורמט שהם מוצגים בו. ההגדרה מאמצת את מסקנות ועדת שופמן[4] ואת הגדרת "מידע מזוהה" בחוק נתוני אשראי, התשע"ו–2016, ומיועדת ליצור תאימות עם חקיקה השוואתית כגון סעיף 4(1) ל-GDPR, סעיף 2(1) לחוק הפרטיות הקנדי (PIPEDA) וסעיף 6(1) לחוק הפרטיות האוסטרלי.

""מידע אישי מדגמי" – מידע אישי אקראי שבעל שליטה במידע ביצע או מבצע בו פעולות עיבוד;

"מידע רגיש" – מידע אישי שיש בו כדי לזהות אחד מאלה:

(1) נתונים על אישיותו של אדם, וצנעת חייו האישיים;

(2) נתונים על עברו הפלילי של אדם;

(3) נתונים על ~~אישותו, מצב בריאותו, מצבו הכלכלי,~~ דעותיו הפוליטיות ואמונתו הדתית של אדם;

(4) נתונים על מצבו הבריאותי של אדם;

(5) נתוני זיהוי ביומטריים, כהגדרתם בחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע–2009;

(6) מידע גנטי, כהגדרתו בחוק מידע גנטי, התשס"א–2000;

(7) נתונים על מצבו הכלכלי של אדם, לרבות נתוני אשראי כהגדרתם בחוק נתוני אשראי, התשע"ו–2016;

(8) מידע אישי שנקבעה לגביו חובת סודיות בדין;

(9) נתוני תעבורה ונתוני מיקום, כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007, שיש בהם כדי ללמד על אחד מסוגי המידע המנויים בסעיפים קטנים (1)-(8);

(10)~~(1)~~ מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש;

"מסמך" – לרבות פלט כהגדרתו בחוק המחשבים;

"מעבד" – אדם המורשה על ידי בעל שליטה במידע, לפעול מטעמו בעיבוד של מידע אישי;

"נושא מידע" – אדם שנעשה עיבוד של מידע אישי על אודותיו;

"סיוע לרשות חוץ" – דרישת מידע אישי ומסמכים, עריכת חיפוש, תפיסת מסמכים, ניהול חקירה והעברת מידע אישי ומסמכים, לשם ביצוע ואכיפה של דיני הגנת הפרטיות במדינות חוץ ופיקוח על ביצועם;

דברי הסבר

הגדרת **"מידע אישי מדגמי"** לקוחה מסעיף 23י להצ"ח תיקון מס' 13.

הגדרת **"מידע רגיש"** משקפת את ההבנה שמידע רגיש הוא מידע אישי שיש בו כדי לזהות מידע רגיש. ההגדרה שואבת השראה מסעיפים 7 לחוק הגנת הפרטיות הקיים, 23יט(א) להצ"ח תיקון מס' 13 ו-9 ל-GDPR. ס"ק (3) להגדרת "מידע רגיש" מצומצם לאמונתו הדתית של אדם ואינו מתייחס לכל אמונה של אדם כ"מידע רגיש"; ס"ק (8) מבהיר שמידע אישי המוגדר סודי, במסגרת החסיונות המקצועיים שהתפתחו בדין, הוא מידע רגיש, ועל כן העיבוד שלו כפוף להוראות הצעת החוק בנוגע למידע רגיש; ס"ק (9) מפנה לנתוני תעבורה ולנתוני מיקום כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007, שיש בהם כדי להיות מידע רגיש רק אם הם עלולים ללמד על סוגי מידע המנויים בס"ק (1)–(8) להגדרת "מידע רגיש".

הגדרת **"מסמך"** זהה להגדרה בסעיף 23ט בהצ"ח תיקון מס' 13.

הגדרת **"מעבד"** מחליפה את הגדרת "מחזיק, לעניין מאגרי מידע" בסעיף 3 לחוק הגנת הפרטיות הקיים ומבוססת על הגדרת "מעבד" בסעיף 4(8) ל-GDPR.

הגדרת **"נושא מידע"** שואבת השראה מההתייחסות ל "data subject" בסעיף 4(1) ב-GDPR, כאל אדם שהמידע בענייננו מזהה או ניתן לזיהוי.

הגדרת **"סיוע לרשות חוץ"** מבוססת על הגדרת המונח בסעיף 54יא1 לחוק ניירות ערך, התשכ"ח–1968.

"עיבוד" – אחת מהפעולות האלה:

(1) איסוף או תיעוד של מידע אישי בכל דרך, לרבות צילום, הקלטה, העתקה או השגת גישה אליו;

(2) ארגון, החזקה או אחסון של מידע אישי, לרבות הבנייה, שינוי, אחזור, ניתוח, איגום או הצלבה;

(3) גילוי או פרסום של מידע אישי, לרבות העברה, מכירה או העמדה לרשות הציבור;

"פקודת המעצר והחיפוש" – פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט–1969;

"פרסום" – ~~כמשמעותו בסעיף 2 לחוק איסור לשון הרע, תשכ"ה-1965~~ לעניין מידע אישי – הבאת מידע אישי לידיעת הציבור בכל דרך;

"קטין" – אדם שטרם מלאו לו שמונה עשרה שנים;

"קשיש" – אדם שמלאו לו 65 שנים.

"ראש הרשות להגנת הפרטיות~~רשם~~" – מי ש~~מתקיימים בו תנאי הכשירות למינוי שופט של בית משפט השלום, ו~~הממשלה מינתה אותו, בהודעה ברשומות, לעמוד בראש הרשות להגנת הפרטיות~~נהל את פנקס מאגרי מידע (להלן - הפנקס) כאמור בסעיף 12~~;

"הרשות" או **"הרשות להגנת הפרטיות"** – הגוף הציבורי המפקח, האוכף והמסדיר את ההגנה על הזכות לפרטיות בהתאם להוראות חוק זה;

"רשות חוץ" – גוף המופקד על ביצוע ואכיפה של דיני הגנת הפרטיות במדינת חוץ ופיקוח על ביצועם;

דברי הסבר

הגדרת **"עיבוד"** מחליפה את הגדרת "שימוש" בסעיף 3 לחוק הגנת הפרטיות הקיים, שאינה מתאימה למכלול הפעולות אשר ניתן לעשות במידע אישי בעולם דיגיטלי. בחרנו במונח "עיבוד" על פני המונח "שימוש" כדי לחדד את ההבחנה בין המונח השגור לפעולות המבוצעות על ידי משתמשי קצה (end-users) לבין הפעולות הנעשות במידע אישי. ההגדרה המוצעת כוללת רשימה סגורה של שלושה סוגי פעולות במידע אישי: איסוף, ניתוח והפצה; ההגדרה מאפשרת בכך הבנה ברורה יותר של סוגי השימושים ומדגישה שמדובר בטיפוסי פעולות שונים. בנוסף, מאחר שהליבה של תפיסת הפרטיות – שליטתו של האדם במידע אישי עליו, זהות ידועה של מבצע העיבוד והאם מדובר באדם או במכונה – אינה רלוונטית. ההגדרה נמצאת בהלימה עם סעיף 4(2) ל-GDPR.

הגדרת **"פקודת המעצר והחיפוש"** זהה להגדרה בסעיף 23ט בהצ"ח תיקון מס' 13.

הגדרת **"פרסום"** מתייחסת לפרסום מידע אישי, שלא כמו השימוש במונח "פרסום" בהקשרים אחרים בהצעת החוק, ושואבת השראה מהגדרת המונח "פרסום" בסעיף 3 לחוק הגנת הפרטיות הקיים, שמפנה להגדרת המונח בסעיף 2 לחוק איסור לשון הרע, התשכ"ה–1965, ומדגישה ש"פרסום" אינו מוגבל לטכנולוגיה או למדיום מסוים. ההגדרה שואבת השראה גם מהגדרת המונחים "פרסום" ו"מפרסם" בחוק העונשין, התשל"ז–1977, שמדגישה את החשיבות שבחשיפת המידע לציבור, כולו או חלקו, כתנאי ל"פרסום".

הגדרת **"קטין"** זהה להגדרה המוצעת בסעיף 3 להצ"ח פרטיות קטינים, שמטרתה לשפר את הגנת הפרטיות על קטינים מצד הורי הקטין ומצד המדינה ולהתאימה למשפט ההשוואתי.[5]

הגדרת **"קשיש"** מבוססת על ההגדרה המקובלת בארץ ובעולם.

הגדרת **"ראש הרשות להגנת הפרטיות"** מחליפה את הגדרת ה"רשם" בסעיף 7 לחוק הגנת הפרטיות הקיים. עם ביטול ההתייחסות בהצעת החוק למאגרי מידע ולחובת רישום אין הצדקה להתייחסות לתפקיד ספציפי של רישום מאגרי מידע. תנאי הכשירות לתפקיד ראש הרשות מפורטים בסעיף 26 להצעת החוק.

הגדרת **"רשות חוץ"** מבוססת על הגדרת המונח בסעיף 54יא1(א) לחוק ניירות ערך, התשכ"ח–1968.

"**שלמות מידע**" - שמירה על מהימנות ודיוק המידע האישי במהלך עיבודו, ~~זהות הנתונים במאגר מידע למקור שממנו נשאבו,~~ בלא ששונוה, ~~נמסרו~~ או הושמדו ~~ל~~שלא לפי הוראות חוק זה~~רשות כדין~~.

"**תיעוד**" – לעניין פסקה (1) שבהגדרת "עיבוד" ולעניין סעיפים 4(5) ו-65(א)(3)(ה) – לרבות קליטה או שימור של מידע אישי באמצעות חיישני מיקום, חיישני חום או כל אמצעי טכנולוגי אחר;

סעיף 1 לחוק הקיים הופך לסעיף 3 המוצע

3. ~~1.~~ איסור פגיעה בפרטיות

לא יפגע אדם בפרטיות של זולתו אלא לפי הוראות חוק זה~~ללא הסכמתו~~.

סעיף 2 לחוק הקיים הופך לסעיף 4 המוצע

4. ~~1.~~ ~~2.~~ פגיעה בפרטיות ~~מהי~~

פגיעה בפרטיות היא אחת מאלה:

(1) בילוש או התחקות אחרי אדם, העלולים להטרידו~~, או הטרדה אחרת~~;

(2) האזנה האסורה על פי חוק;

(3) צפייה או עיון במידע אישי, לרבות קריאה או האזנה;

(4) צילום אדם כשהוא ברשות היחיד שלא לפי הוראות חוק זה;

(5) פרסום תצלומו של אדם או תוצר של תיעוד אודות אדם בנוגע למצבו או להתנהגותו ברשות ~~ב~~הרבים, שלא לפי הוראות חוק זה, בנסיבות שבהן עלול הפרסום להשפילו או לבזותו, ובכלל זה לאחר אירוע פתאומי שבו נגרמה לאותו אדם פגיעה גופנית או נפשית;~~(4א) פרסום תצלומו של נפגע ברבים שצולם בזמן הפגיעה או סמוך לאחריה באופן שניתן לזהותו ובנסיבות שבהן עלול הפרסום להביאו במבוכה,~~ למעט פרסום תצלום או תוצר של תיעוד בלא השהיות בין רגע הצילום או התיעוד לרגע השידור בפועל שאינו חורג מהסביר באותן נסיבות; ~~לעניין זה, "נפגע" – מי שסבל מפגיעה גופנית או נפשית עקב אירוע פתאומי ושפגיעתו ניכרת לעין;~~

~~(5) העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב, והכל אם אין הכתב בעל ערך היסטורי ולא עברו חמש עשרה שנים ממועד כתיבתו; לעניין זה, "כתב" – לרבות מסר אלקטרוני כהגדרתו בחוק חתימה אלקטרונית, התשס"א-2001;~~

(6) שימוש בשם אדם, בכינויו, בתמונתו או בקולו, שלא לפי הוראות חוק זה~~לשם ריווח~~;

(7) הפרה של חובת סודיות שנקבעה בדין או בהסכם לגבי ענייניו הפרטיים של אדם;

(8) עיבוד של מידע אישי על אודות אדם שלא לפי הוראות חוק זה.

~~הפרה של חובת סודיות לגבי ענייניו הפרטיים של אדם, שנקבעה בהסכם מפורש או משתמע;~~

~~(9) שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה;~~

~~(10) פרסומו או מסירתו של דבר שהושג בדרך פגיעה בפרטיות לפי פסקאות (1) עד (7) או (9);~~

~~(11) פרסומו של ענין הנוגע לצנעת חייו האישיים של אדם, לרבות עברו המיני, או למצב בריאותו, או להתנהגותו ברשות היחיד.~~

דברי הסבר

הגדרת **"שלמות המידע"** מבוססת על סעיף 7 לחוק הגנת הפרטיות הקיים ומותאמת לניסוח חקיקה מודרני. ההגדרה המוצעת משקפת את החשיבות שבשמירה על מהימנות ודיוק המידע האישי במהלך עיבודו ומתירה את שינויו לפי הצעת חוק זו, ולא על פי כל דין כפי שמתירה הגדרת המונח בחוק הקיים.

הגדרת **"תיעוד"** משקפת התאמה למציאות טכנולוגית מתפתחת שיש בכוחה לאפשר עיבוד מידע אישי בדרכים נוספות על צילום, הקבוע בחוק הגנת הפרטיות הקיים, למשל באמצעות חיישנים שונים. ההגדרה אינה מתייחסת ל"תיעוד" בסעיפים 22 ו-39(ב)(5) להצעת החוק העוסקים בתיעוד אירועי אבטחה.

<u>סעיף 3:</u> מבוסס על סעיף 1 לחוק הגנת הפרטיות הקיים. ואולם כחלק מהשינוי בתפיסת ההסכמה בהצעת החוק, הסכמה אינה הכלי היחיד להכשרת פגיעה בפרטיות. פגיעה בפרטיות תיעשה לפי הצעת חוק זו אך ורק בכפוף לסעיף 76 העוסק בשמירת הדינים.

<u>סעיף 4:</u> מבוסס על סעיף 2 לחוק הגנת הפרטיות הקיים ומציג רשימה סגורה של פגיעות אפשריות בפרטיות.

ס"ק (1) מבוסס על סעיף 2(1) בחוק הגנת הפרטיות הקיים, אגב מחיקת המילים "או הטרדה אחרת". מובהר שכל הטרדה, אף אם אינה מאיימת, למשל מעקב באמצעות מכשיר GPS סמוי שהנעקב אינו יודע בכלל על קיומו, עדיין עלולה לפגוע בפרטיותו של אדם.

ס"ק (2) וס"ק (4) זהים לסעיפים 2(2) ו-2(3) לחוק הגנת הפרטיות הקיים (בהתאמה). האזנה שאינה אסורה על פי חוק האזנת סתר או צילום יכולה להיחשב פגיעה בפרטיות גם לפי ס"ק (8).

ס"ק (3) קובע שצפייה או עיון במידע אישי הם פגיעה בפרטיות, אף אם המידע אינו מפורסם וגם אם אין נעשות בו פעולות עיבוד אחרות.[6]

ס"ק (5) מחליף את הפגיעות המתוארות בסעיפים 2(4), 2(4א), ו-2(10) בחוק הגנת הפרטיות הקיים ומוסיף פגיעה בפרטיות בעקבות "פרסום תוצר של תיעוד" (למשל, פרסום איכון הטלפון הסלולרי במועדון חשפנות) כשיש בפרסום כדי להשפיל או לבזות את נושא המידע.

ס"ק (6) מבוסס על סעיף 2(6) בחוק הגנת הפרטיות הקיים, אגב השמטת ההתייחסות ל"לשם ריווח", שאינה רלוונטית לשאלת הפגיעה בפרטיות.

ס"ק (7) מאחד את הוראת סעיפים 2(7) ו-2(8) בחוק הגנת הפרטיות הקיים, אגב השמטת ההבהרה שההסכם יכול להיות במפורש או במשתמע, שאינה רלוונטית.

ס"ק (8) מחליף את סעיפים 2(9)-(11) לחוק הגנת הפרטיות הקיים ומסדיר אירועי פגיעה בפרטיות במידע עקב עיבוד מידע אישי בניגוד להוראות הצעת החוק. בכך מובהר שהסכמה אינה הכלי היחיד להכשרת פגיעה בפרטיות עקב עיבוד מידע אישי, בדומה להוראות ה-GDPR.

סעיף 2(5) לחוק הגנת הפרטיות הקיים לא נכלל בהצעת החוק המוצעת כאן, וזאת משום שהפגיעה בפרטיות המפורטת בו נכללת בס"ק (4), (6) ו-(7) המוצעים.

עיקרון צמידות המטרה שבסעיף 2(9) לחוק הגנת הפרטיות הקיים מעוגן בסעיף 7 להצעת החוק.

סעיף 2א לחוק הקיים הופך לסעיף 5 המוצע.

5. ~~2א.~~ פרסום תצלומו של נפטר

(א) לעניין חוק זה רואים כפגיעה בפרטיות גם פרסום ברבים של תצלום גופת אדם גלויה באופן שניתן לזהותה, אלא אם כן התקיים אחד מאלה:

(1) אותו אדם הסכים בחייו לפגיעה כאמור;

(2) חלפו 15 שנים ממועד פטירתו של אותו אדם;

(3) התקבלה הסכמה לפגיעה כאמור מאת הראשון מבין המפורטים בפסקאות משנה (א) עד (ד), שעודו בחיים, ובלבד שהנפטר לא התנגד בחייו לפגיעה כאמור וילדו או הורהו לא הודיע למפרסם או לאחר מטעמו כי הוא מתנגד לפרסום:

(א) בן זוגו;

(ב) כל ילדיו;

(ג) הוריו;

(ד) כל אחיו;

(4) לא היו לנפטר קרובי משפחה המנויים בפסקה (3) ובית המשפט אישר את הפרסום.

(ב) בן זוגו של נפטר, ילדו, הורהו או אחיו רשיאם להגיש תובענה אזרחית בשל פרסום לפי סעיף זה.

סעיף 3 לחוק הקיים שולב עם סעיף 2 המוצע

~~3. הגדרת מונחים -~~

~~"מחזיק, לענין מאגר מידע" - מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש;~~

~~"צילום" - לרבות הסרטה;~~

~~4. פגיעה בפרטיות~~ סעיף 4 לחוק הקיים הועבר לסעיף 61 המוצע.

~~5. פגיעה בפרטיות - עבירה.~~ סעיף 5 לחוק הקיים הועבר לסעיף 62 המוצע.

~~6. מעשה של מה בכך~~
~~לא תהיה זכות לתביעה אזרחית או פלילית לפי חוק זה בשל פגיעה שאין בה ממש.~~

פרק ב: הגנה על הפרטיות ב~~מאגרי~~ מידע אישי

סעיף 7 לחוק הקיים שולב עם סעיף 2 המוצע

~~7. הגדרות בפרק זה ובפרק ד' –~~

~~"מאגר מידע" - אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט –~~

~~(1) אוסף לשימוש אישי שאינו למטרות עסק; או~~

~~(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;~~

~~"מנהל מאגר" - מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לענין זה;~~

דברי הסבר

סעיף 5: שאלת קיומה של זכות לפרטיות לאחר המוות דורשת מחקר נפרד, שאינו בליבת עבודתנו הנוכחית לגיבוש הצעה לחוק הגנת פרטיות חדש ומעודכן.

סעיפים 3 ו-7 לחוק הקיים: הגדרות **"מחזיק"**, **"מאגר מידע"** ו-**"מנהל מאגר"** בחוק הקיים נמחקו. זאת משום שהנחת היסוד של הצעת החוק היא שאין עוד מקום לחובת רישום מאגרי מידע הקיימת בחוק הגנת הפרטיות הקיים ושבעידן כיום תחימת חובות הגנת הפרטיות לקיומו או הגדרתו של אוסף הנתונים כמאגר מידע פוגעת את היקף הגנת הפרטיות ועוצמתה.

הגדרת **"צילום"** נמחקה שכן היא כלולה תחת הגדרת "עיבוד" והגדרת המונח "תיעוד" בסעיף 2 המוצע.

סעיף 6 לחוק הגנת הפרטיות הקיים לא אומץ בהצעת החוק, שכן הוראתו ש"לא תהיה זכות לתביעה אזרחית או פלילית לפי חוק זה בשל פגיעה שאין בה ממש" מוסדרת בעקרונות הכלליים של דיני הנזיקין ושל דיני העונשין.

סימן א': הוראות כלליות לעניין עיבוד מידע אישימאגרי מידע

8. רישום מאגר מידע והשימוש בו

(א) לא ינהל אדם ולא יחזיק מאגר מידע החייב ברישום לפי סעיף זה, אלא אם כן התקיים אחד מאלה:

(1) המאגר נרשם בפנקס;

(2) הוגשה בקשה לרישום המאגר והתקיימו הוראות סעיף 10(ב1);

(3) המאגר חייב ברישום לפי סעיף קטן (ה) והוראת הרשם כללה הרשאה לניהול והחזקה של המאגר עד רישומו.

(ב) לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר.

(ג) בעל מאגר מידע חייב ברישום בפנקס ועל בעל המאגר לרשמו אם נתקיים בו אחד מאלה:

(1) מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000;

(2) יש במאגר מידע רגיש;

(3) המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה;

(4) המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23;

(5) המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17ג.

(ד) הוראת סעיף קטן (ג) לא תחול על מאגר שאין בו אלא מידע שפורסם לרבים על פי סמכות כדין או שהועמד לעיון הרבים על-פי סמכות כדין.

(ה) הרשם רשאי, מטעמים מיוחדים שיירשמו, להורות על קיום חובת רישום לגבי מאגר הפטור מחובת רישום לפי סעיפים קטנים (ג) ו-(ד); הוראה כאמור תומצא לבעל המאגר ובה יפרט הרשם הוראות לענין ניהול ואחזקת המאגר עד לרישומו.

9. בקשה לרישום

(א) בקשה לרישום מאגר מידע תוגש לרשם.

(ב) בקשה לרישום מאגר מידע תפרט את –

(1) זהות בעל מאגר המידע, המחזיק במאגר ומנהל המאגר, ומעניהם בישראל;

(2) מטרות הקמת מאגר המידע והמטרות שלהן נועד המידע;

(3) סוגי המידע שייכללו במאגר;

(4) פרטים בדבר העברת מידע מחוץ לגבולות המדינה;

(5) פרטים בדבר קבלת מידע, דרך קבע, מגוף ציבורי כהגדרתו בסעיף 23, שם הגוף הציבורי מוסר המידע ומהות המידע הנמסר, למעט פרטים הנמסרים בהסכמת מי שהמידע על אודותיו.

(ג) שר המשפטים רשאי לקבוע בתקנות פרטים נוספים שיפורטו בבקשה לרישום.

(ד) הבעל או המחזיק של מאגר מידע יודיע לרשם על כל שינוי בפרט מהפרטים המפורטים בסעיף קטן (ב) או לפי סעיף קטן (ג) ועל הפסקת פעולתו של מאגר המידע.

10. סמכויות הרשם

(א) הוגשה בקשה לרישום מאגר מידע –

(1) ירשום אותו הרשם בפנקס, תוך 90 ימים מיום שהוגשה לו הבקשה, זולת אם היה לו יסוד סביר להניח כי המאגר משמש או עלול לשמש לפעולות בלתי חוקיות או כמסווה להן, או שהמידע הכלול בו נתקבל, נצבר או נאסף בניגוד לחוק זה או בניגוד להוראות כל דין;

(2) הרשם רשאי לרשום מטרה שונה מזו שפורטה בבקשה, לרשום מספר מטרות למאגר, או להורות על הגשת מספר בקשות תחת הבקשה שהוגשה, והכל אם נוכח לדעת כי הדבר הולם את פעילות המאגר הלכה למעשה;

(3) הרשם לא יסרב לרשום את מאגר המידע לפי פסקה (1) ולא יפעיל סמכויותיו לפי פסקה (2), אלא לאחר שנתן למבקש הזדמנות לטעון את טענותיו.

(ב) (בוטל).

(ב1) לא רשם הרשם את מאגר המידע תוך 90 ימים מיום שהוגשה לו הבקשה, ולא הודיע למבקש על סירובו לרשום או על השהיית הרישום מטעמים מיוחדים שיפרט בהודעתו – רשאי יהיה המבקש לנהל או להחזיק את המאגר אף שאינו רשום.
(ב2) הודיע הרשם למבקש על סירובו לרשום את מאגר המידע, או על השהיית הרישום כאמור בסעיף קטן (ב1) לא יהיה המבקש רשאי לנהל או להחזיק את המאגר, זולת אם בית המשפט קבע אחרת.
(ב3) הרשם ימחק רישומו של מאגר מידע מהפנקס, אם הודיע לו בעל המאגר שהמידע שבאותו מאגר בוער, ואימת הודעה זו בתצהיר; הוחזק מאגר מידע שלא בידי בעל מאגר המידע, תאומת ההודעה גם בתצהיר של המחזיק.
(ג) הרשם יפקח על מילוי הוראות חוק זה והתקנות לפיו.
(ד) שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, יקים בצו, יחידת פיקוח שתפקח על מאגרי המידע, רישומם ואבטחת המידע בהם; גודלה של היחידה יותאם לצורכי הפיקוח.
(ה) הרשם יעמוד בראש יחידת הפיקוח, והוא ימנה את המפקחים לצורך ביצוע הפיקוח לפי חוק זה; לא יתמנה למפקח אלא מי שקיבל הכשרה מקצועית מתאימה בתחום מיחשוב ואבטחת מידע והפעלת סמכויות לפי חוק זה, ומשטרת ישראל לא הביעה התנגדות למינויו מטעמים של שמירה על בטחון הציבור.

סעיף 10(ה1) הועבר לסעיף 34.

(ה1) לצורך ביצוע תפקידיו רשאי מפקח –

(ו) הפר מחזיק או בעל של מאגר מידע הוראות של חוק זה או התקנות לפיו, או לא מילא אחרי דרישה שהפנה אליו הרשם, רשאי הרשם להתלות את תוקפו של הרישום לתקופה שיקבע או לבטל את רישומו של מאגר המידע בפנקס, ובלבד שקודם להתליה או ביטול ניתנה לבעל המאגר הזדמנות להשמיע את טענותיו.
(ז) דין הרשם ודין מי שפועל מטעמו כדין עובד המדינה.

סעיף 10א הועבר לסעיף 74

10א. דו"ח הגנה על הפרטיות..

דברי הסבר

סעיפים 8, 9, 10(א)-(ה), (ו)-(ז) לחוק הקיים
לא אומצו בהצעת החוק. ועדת שופמן (בשנת 2007)[7] ומשרד המשפטים (בתזכיר הצעת החוק לצמצום החובה לרישום מאגרי המידע משנת 2012),[8] המליצו לצמצם את החובה לרישום מאגרי מידע ולהמירה בחלופה טובה יותר – שתביא להפנמה אמיתית של חובות הגנת הפרטיות לפי החוק, כגון חובת הניהול התקין. המלצות אלו התבססו על ההבנה שהתועלת בחובת הרישום קטנה, שהיא אינה מבטיחה בכלל ציות להוראות החוק ושהעיסוק של הרשות להגנת הפרטיות באכיפה של חובת הרישום גורם לבזבוז משאבים חשובים. לדעתנו, ביטול חובת הרישום עדיף על פני צמצומה ולכן אנו מציעים לבטל לחלוטין את חובת הרישום. בעולם דיגיטלי שבו מידע אישי נאגם ונשמר כעניין שבשגרה, חובת רישום מטילה נטל רגולטורי בלתי סביר על כל אדם כמעט שמחזיק ברשותו רשימת שמות של לקוחות, צרכנים או משתמשים בשירות שהוא נותן. יתרה מזו, בעידן של היום תחימת החובות של הגנת הפרטיות לקיומו או להגדרתו של מקבץ הנתונים כמאגר מידע פוגעת בהיקף הגנת הפרטיות ובעוצמתה. לדעתנו, מערך הכלים החלופי להגנת פרטיות במידע אישי המוצע בהצעת החוק נותן מענה מקיף ומדויק יותר להגנת פרטיות מאשר חובת רישום מאגרי מידע.

6. פגיעה מותרת בפרטיות

(א) פגיעה בפרטיות מותרת בהתקיים אחד מאלה:

(1) היא נדרשת לשם מילוי התחייבויות הקבועות בהסכם שנושא המידע הוא צד לו, או לשם נקיטת צעדים המבוקשים על ידי נושא המידע לפני ההתקשרות בהסכם כאמור;

(2) היא נדרשת כדי להגן על אינטרס מהותי של בעל השליטה במידע או צד שלישי שאליו הועבר מידע אישי, ובלבד שהיא אינה מבוצעת על ידי גוף ציבורי במסגרת ביצוע משימותיו על פי דין ושנושא המידע היה יכול לצפות באופן סביר בהתחשב בזמן ובנסיבות שתתרחש פגיעה כאמור.

(3) נושא המידע הסכים לפגיעה בפרטיות.

(ב) פגיעה בפרטיות בדרך של עיבוד מידע רגיש מותרת בהתקיים אחד מאלה:

(1) עיבוד המידע הרגיש נחוץ לצורך מימוש זכויותיו של נושא המידע, או לצורך מימוש זכויותיו או מילוי חובותיו של בעל שליטה במידע, במסגרת יחסי העבודה בין בעל שליטה במידע לנושא המידע ובהתאם לחוק המתיר עיבוד מידע רגיש לצורך מטרות אלו.

(2) עיבוד המידע הרגיש מידתי בהיקפו לצורך ביצוע מחקר סטטיסטי, מדעי או היסטורי שיש אינטרס ציבורי בביצועו.

(3) עיבוד המידע הרגיש נדרש כדי להגן על אינטרס מהותי של בעל השליטה במידע או צד שלישי שאליו הועבר המידע הרגיש ובלבד שעיבוד המידע הרגיש אינו מבוצע על ידי גוף ציבורי במסגרת ביצוע משימותיו על פי דין ושנושא המידע הסכים במפורש לעיבוד המידע הרגיש על אודותיו; היה העיבוד לפי פסקה (3) להגדרת עיבוד בסעיף 2 לחוק - נושא המידע הסכים במפורש קודם לביצוע עיבוד כאמור.

7. דרישת קיום המטרה

לא יעבד בעל שליטה במידע מידע אישי אלא למטרה שלשמה נאסף או נמסר המידע האישי כמפורט בהודעה לפי סעיף 9 או למטרה הדומה למטרה שלשמה נאסף או נמסר המידע האישי; בבואו לבחון את קיומה של מטרה דומה כאמור, ישקול בעל שליטה במידע, בין השאר, את אלה:

(1) הקשר בין המטרה לשמה נאסף או נמסר המידע האישי לבין מטרת העיבוד שהוא מבקש לבצע;

(2) הנסיבות שבהן נאסף המידע האישי, קיומה של מערכת יחסים בין נושא המידע לבין בעל השליטה במידע ואת ציפייתו הסבירה של נושא המידע בנוגע לעיבוד נוסף של המידע האישי, מעבר למטרה לשמה נאסף או נמסר;

(3) האם המידע האישי כולל מידע רגיש;

(4) השלכות אפשריות של העיבוד הנוסף שהוא מבקש לבצע.

דברי הסבר

סעיף 6: מגדיר, בדומה לסעיפים 6 ו-9 ל-GDPR, את הבסיסים הלגיטימיים לפגיעה בפרטיות, לרבות בדרך של עיבוד מידע אישי או מידע רגיש.

התממה (אנונימיזציה) כשלעצמה אינה יכולה לשמש בסיס משפטי להתרת עיבוד מידע אישי,[9] כפי שעולה גם מסעיף 26 להקדמה ל-GDPR. הקביעה אם המידע המותמם אינו מאפשר זיהויו של נושא המידע תיעשה מתוך בחינת כל האמצעים שסביר שיעשה בהם שימוש לשם זיהוי חוזר של מידע לאחר התממתו. סבירות השימוש באמצעים תיקבע לפי מדדים אובייקטיביים, כגון עלות הזיהוי החוזר, פרק הזמן שיש להשקיע בביצוע זיהוי חוזר, הטכנולוגיה הזמינה בזמן עיבוד המידע המותמם והתפתחויות טכנולוגיות צפויות באותה עת.

ס"ק (א)(1) מבוסס על סעיף 6(1)(b) ל-GDPR ומתיר פגיעה בפרטיות כאשר היא נדרשת לשם מילוי מחויבות בהסכם שנושא המידע הוא צד לו או כניסה להסכם כאמור.

ס"ק (א)(2) מבוסס על סעיף 6(1)(f) ל-GDPR וקובע שפגיעה בפרטיות מותרת כאשר היא נחוצה למימוש אינטרס מהותי של בעל השליטה במידע או של צד שלישי שאליו הועבר מידע אישי, ובלבד שסביר שנושא המידע צפה, בהתחשב בזמן ובנסיבות שתתרחש פגיעה כאמור. למשל, כאשר הפגיעה בפרטיות היא בדרך של עיבוד מידע אישי שנחוץ לשם העברתו בין חברות קשורות או לשם אבטחת מידע אישי. הסעיף אינו חל על גוף ציבורי המחויב לפעול בהתאם להסמכה בדין ולא על פי מבחן סבירות ומימוש אינטרס מהותי שלו.

ס"ק (א)(3) מבוסס על סעיף 6(1)(a) ל-GDPR ומתיר פגיעה בפרטיות בהסכמת נושא המידע. ס"ק (א)(3) נמצא בסוף רשימת הבסיסים הלגיטימיים כדי לחדד את שינוי התפיסה שבעקבותיו ייטיב בעל שליטה במידע לבדוק אם עומדים לרשותו בסיסים לגיטימיים אחרים לפגיעה בפרטיות קודם שיפנה להכשרת הפגיעה בפרטיות של נושא המידע על ידי קבלת הסכמה.

ס"ק (ב)(1) מבוסס על סעיף 9(2)(b) ל-GDPR ומתיר פגיעה בפרטיות בדרך של עיבוד מידע רגיש, למשל נתונים ביומטריים, לצורך מימוש זכויותיהם של בעל שליטה במידע או של נושא מידע או לצורך מילוי חובותיו של בעל שליטה במידע במסגרת יחסי העבודה בין בעל שליטה במידע לנושא המידע.

ס"ק (ב)(2) שואב השראה מסעיף 9(2)(j) ל-GDPR ומתיר פגיעה בפרטיות בדרך של עיבוד מידע רגיש במידה הדרושה לצורך מחקר מדעי, סטטיסטי או היסטורי שיש אינטרס ציבורי בביצועו.

ס"ק (ב)(3) מתיר פגיעה בפרטיות בדרך של עיבוד מידע רגיש לפי האיזון שבין האינטרס המהותי של בעל שליטה במידע לאינטרס המהותי של נושא המידע, בדומה לס"ק (א)(2). הסעיף אינו מסתפק במבחן הציפייה הסבירה אלא מחייב קבלת הסכמה מפורשת של נושא המידע. רק כאשר מדובר בגילוי או בפרסום של מידע רגיש, כלומר עיבוד לפי פסקה (3) להגדרת המונח "עיבוד" בסעיף 2 להצעת החוק, נדרשת הסכמתו המפורשת של נושא המידע קודם לביצוע הגילוי או הפרסום – כדי להגביר את שליטתו של נושא המידע במידע רגיש עליו וכדי לוודא שהוא מודע למכלול פעולות העיבוד האפשריות במידע הרגיש עליו.

<u>**סעיף 7:**</u> מבוסס על סעיף 2(9) לחוק הגנת הפרטיות הקיים ושואב השראה מסעיפים 5(1) ו-6(4) ל-GDPR. הסעיף מעגן את דרישת קיום המטרה כתנאי לפגיעה בפרטיות בדרך של עיבוד מידע אישי או מידע רגיש לפי סעיף 6 להלן ומכיר בצורך בגמישות ובדינמיות בעיבוד מידע אישי על ידי קביעת מנגנון להכרה בקיומן של מטרות דומות.

8. הסכמה לעניין פגיעה בפרטיותו של קטין

(א) פגיעה בפרטיותו של קטין מתחת לגיל 13 לפי סעיף 6(א)(3) תיעשה אך ורק בהסכמת אחד מהוריו או אפוטרופוס שנתמנה לו כדין, או לפי הסמכה מפורשת בדין.

(ב) לא יעבד בעל שליטה מידע רגיש לפי סעיף 6(ב)(3) על אודות קטין מתחת לגיל 16 אלא בהסכמת אחד מהוריו או אפוטרופוס שנתמנה לו כדין, או לפי הסמכה מפורשת בדין.

(ג) ראש הרשות להגנת הפרטיות יקבע הנחיות בדבר הדרכים לאימות גילו של קטין ולווידוא קבלת הסכמת הוריו או האפוטרופוס שלו, כאמור בסעיפים קטנים (א) ו-(ב).

סעיף 11 לחוק הקיים הופך לסעיף 9 המוצע.

9. ~~11.~~ חובת מתן הודעה~~מבקש מידע~~

(א) פניה לאדם לקבלת מידע אישי לשם עיבודו~~החזקתו או שימוש בו במאגר מידע~~ תלווה בהודעה ~~שיצויינו בה~~ בשפה ברורה בה נאסף המידע האישי, על כוונת בעל שליטה במידע לעבד את המידע האישי, תוך ציון כל אלה–

(1) שמו של בעל שליטה במידע, מענו ודרכי ההתקשרות עימו;

~~(1)~~(2) אם חלה על אותו אדם חובה חוקית למסור את המידע האישי, או שמסירת המידע תלויה ברצונו ובהסכמתו, ותוצאות אי הסכמה למסירת המידע האישי;

~~(2)~~(3) המטרה אשר לשמה מבוקש העיבוד ונחיצות המידע האישי להגשמתה;

(4) זכות החזרה מהסכמה לעיבוד מידע אישי לפי סעיף 10, זכות העיון במידע האישי לפי סעיף 11, הזכות לקבלת הסבר לפי סעיף 12, זכות תיקון המידע האישי לפי סעיף 13, הזכות לניוד מידע אישי לפי סעיף 14 וזכות המחיקה של מידע אישי לפי סעיף 15, והדרכים למימוש הזכויות כאמור;

(5) למי יימסר המידע האישי ומטרות המסירה.

~~(3)~~(ב) שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, יקבע את דרכי ההצגה של ההודעה לפי סעיף קטן (א), לרבות הצגתה במתכונת דיגיטלית, אופן ניסוחה ומידת הבלטתה בהתחשב, בין היתר, בקהלי היעד שלה.

~~12.פנקס מאגרי מידע~~

~~(א) הרשם ינהל פנקס מאגרי מידע אשר יהיה פתוח לעיונו של הציבור.~~

~~(ב) הפנקס יכיל את הפרטים לרישום מאגר המידע כאמור בסעיף 9.~~

~~(ג) על אף הוראות סעיפים קטנים (א) ו-(ב), במאגר של רשות בטחון, הפרטים המפורטים בסעיף 9(ב)(3), (4) ו-(5) לא יהיו פתוחים לעיונו של הציבור.~~

סימן ב': זכויות נושא המידע

10. זכות החזרה מהסכמה

(א) נושא המידע רשאי בכל עת לחזור בו מהסכמתו לפגיעה בפרטיותו לפי סעיף 6(א)(3) או 6(ב)(3) לעיל;

(ב) מבלי לגרוע מהוראות סעיף קטן (א) לעיל, קטין מעל גיל 13 רשאי לחזור בו מהסכמה לפי סעיף 6(א)(3) וקטין מעל גיל 16 רשאי לחזור בו מהסכמה לפי סעיף 6(ב)(3), בין שההסכמה ניתנה על ידו ובין שניתנה על ידי הורה או אפוטרופוס. היה הקטין מתחת

לגיל הכשרות למתן הסכמה לפי סעיף 8 לעיל, רשאי אחד מהוריו או אפוטרופוס שנתמנה לו כדין, או לפי הסמכה מפורשת בדין לחזור מהסכמה כאמור.

(ג) חזר נושא המידע מהסכמה כאמור בסעיף קטן (א) או (ב), לא תפגע חוקיות עיבוד המידע שנעשה על בסיס הסכמת נושא המידע עד לאותו מועד.

דברי הסבר

סעיף 8: שואב השראה מסעיפים 11ב להצ"ח פרטיות קטינים, 312.5 ל-COPPA האמריקני ו-8 ל-GDPR ומאזן בין הגנה על ילדים לבין ההכרה ביכולתם של ילדים מעל גיל 13 לקבל החלטות עבור עצמם בעניינים שתוצאותיהם אינן גורליות. מטרתו לתמרץ חברות הטכנולוגיה ליישם טכנולוגיות מתאימות ולהבטיח בכך זהירות יתרה בעת פגיעה בפרטיות של קטינים, בין השאר בדרך של עיבוד מידע אישי ומידע רגיש עליהם.

בס"ק (א) קבענו שגיל 13 הוא הגיל הקובע לעניין הסכמה לעיבוד מידע אישי, בדומה ל-COPPA האמריקני שהוא הדין הוותיק ביותר בנושא. הגיל הקובע לעניין הסכמה לעיבוד מידע רגיש הוא 16 לפי ס"ק (ב). מגיל 16 ועד גיל 18 יחול ההסדר הקבוע בחוק הכשרות המשפטית והאפוטרופסות, התשכ"ו–1962,[10] הבוחן אם הסכמת הקטין לעיבוד מידע רגיש עליו בנסיבות המקרה היא פעולה שדרכם של קטינים לעשות.

סעיף 8 אינו מחייב תיעוד הסכמת קטין כמוצע בסעיף 11ב(5) להצ"ח פרטיות קטינים, שכן דרישה זו עלולה להטיל עומס בלתי סביר על בעל שליטה במידע והשלכותיה בפועל עלולות להיות זהות לחובת רישום מאגרי מידע הקיימת כיום.

סעיף 9: מבוסס על סעיף 11 בחוק הגנת הפרטיות הקיים, סעיף 11א להצ"ח פרטיות קטינים ותיקונים שהוצעו על ידי ועדת שופמן.[11]

סעיף 12 לחוק הקיים שעוסק בפנקס מאגרי המידע וניהולו על ידי הרשם לא אומץ בהצעת החוק. אין הצדקה לאימוצו שכן חובת רישום מאגרי מידע לפי חוק הגנת הפרטיות הקיים לא אומצה גם היא בהצעת החוק.

סעיף 10: שואב השראה מסעיפים 7(3) ל-GDPR, 4.3.8 לחוק הפרטיות הקנדי (PIPEDA, Schedule 1, §4.3.8) ו-13ב להצ"ח פרטיות קטינים. הסעיף מעגן זכות מוחלטת לחזרה מההסכמה של כל אדם, לרבות קטין, במטרה להביא לשינוי תפיסתי ולהפסקת השימוש בהסכמה ככלי חסר משמעות וכ"מכבסה" להתחמקות מן הדרישות של חוק הגנת הפרטיות הקיים. על בעל שליטה במידע המבקש לפגוע בפרטיותו של אדם לבחון תחילה אם אחד מן הבסיסים הלגיטימיים, מלבד מהסכמה, המפורטים בסעיף 6 להצעת החוק מתיר לו לבצע את הפגיעה האמורה. רק בהיעדרם של בסיסים לגיטימיים כאלה יבקש בעל שליטה במידע את הסכמתו של נושא המידע לפגיעה בפרטיותו. במקרה כזה יהיה עליו להיערך מראש לאפשרות שנושא המידע יחזור בו מהסכמתו. חזרת נושא המידע בו מהסכמתו לא תפגע בחוקיות של הפגיעה בפרטיות שנעשתה על בסיס ההסכמה של נושא המידע עד למועד חזרתו מן ההסכמה. הפְסָקה של פגיעה בפרטיות בגלל חזרה מהסכמה יכולה להתרחש רק כאשר אף אחד מן הבסיסים הלגיטימיים האחרים המפורטים בסעיף 6 להצעת החוק, מלבד הסכמת נושא המידע, אינו מתיר את עיבוד המידע האישי המבוקש על ידי בעל שליטה במידע.

סעיף 13 לחוק הקיים הופך לסעיף 11 המוצע.

11. ~~13.~~ זכות עיון במידע אישי

(א) כל אדם זכאי לקבל~~לעיין~~ בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, מבעל שליטה במידע מענה לשאלה האם הוא עושה פעולת עיבוד במידע אישי על אודותיו~~שעליו המוחזק במאגר מידע~~.

(ב) כל נושא מידע זכאי לקבל לידיו ולעיין בעצמו, או על ידי בא כוחו שהרשהו בכתב או על ידי אפוטרופסו, בכל אחד מאלה: ~~בעל מאגר מידע יאפשר עיון במידע, לפי בקשת אדם כאמור בסעיף קטן (א) (להלן - המבקש), בשפה העברית, הערבית או האנגלית.~~

(1) עותק מהמידע האישי על אודותיו שנעשתה בו פעולת עיבוד;

(2) מידע בנושאים הבאים:

(א) מטרת עיבוד המידע האישי על אודותיו;

(ב) זהותם של מקבלי המידע האישי על אודותיו או הסוגים של מקבלי המידע האישי על אודותיו, שאליהם הועבר או יועבר המידע האישי, ובפרט בנוגע למקבלי מידע אישי במדינות חוץ ומקבלי מידע אישי שהם ארגונים בינלאומיים;

(ג) אם המידע האישי על אודותיו לא נאסף מהמבקש עצמו – זהותו של מקור המידע האישי;

(ג) הגיש נושא מידע בקשה לעיין במידע אישי על אודותיו כאמור בסעיף זה, יידע אותו בעל השליטה במידע על זכויותיו לפי סימן זה.

(ד) המידע האישי המבוקש וכן פרטי המידע הנוספים המבוקשים יימסרו לעיון המבקש בשפה שבה נאסף המידע האישי ובתבנית דיגיטלית מקובלת.

(ה)~~(ג)~~ על אף האמור בסעיף זה, בעל שליטה במידע~~המאגר~~ רשאי לסרב לבקשה לעיון, בהתקיים אחד מאלה:

(1) ~~שלא למסור למבקש~~ המידע האישי המתייחס למצבו הרפואי או הנפשי של מבקש העיון ~~אם~~ ולדעת~~ו~~ בעל השליטה במידע, עיון בו ~~המידע~~ עלול לגרום נזק חמור לבריאותו הגופנית או הנפשית של המבקש או לסכן את חייו; במקרה זה ימסור בעל המאגר את המידע לרופא או לפסיכולוג מטעמו של המבקש.

(2) מתן זכות העיון כמבוקש עלול לדעת בעל השליטה במידע לפגוע בחיי אדם;

(3) מתן זכות העיון כמבוקש עלול לדעת בעל השליטה במידע לפגוע במידה העולה על הנדרש בזכויותיו של צד שלישי שאינו בעל השליטה במידע או המעבד;

(ו) ~~(גד)~~ אין בהוראות סעיף זה כדי לחייב למסור מידע בניגוד לחסיון שנקבע לפי כל דין, אלא אם כן המבקש הוא מי שהחסיון נועד לטובתו.

בסעיף קטן זה, "דין" – לרבות הלכה פסוקה.

(ז) אין בהוראות סעיף זה כדי לחייב למסור מידע אישי בניגוד לדין.

~~(ד) האופן, התנאים והתשלום למימושה של זכות העיון במידע ייקבעו בתקנות.~~

(ח) ~~(ה)~~ הוראות סעיף זה וסעיף 13א לא יחולו –

(1) על מאגר מידע של רשות בטחון כמשמעותה בסעיף 19(ג);

(1א) על מאגר מידע של שירות בתי הסוהר;

(2) על מאגר מידע של רשות מס כמשמעותה בחוק לתיקון דיני מסים (חילופי ידיעות בין רשויות מס), תשכ"ז–1967;

(3) כשבטחון המדינה, יחסי חוץ שלה או הוראות חיקוק מחייבים שלא לגלות לאדם מידע שעליו;

(4) על מאגר מידע של גופים אשר שר המשפטים בהתייעצות עם שר הבטחון או עם שר החוץ, לפי הענין, ובאישור ועדת החוץ והבטחון של הכנסת, קבע כי הוא כולל מידע שבטחון המדינה או יחסי החוץ שלה מחייבים שלא לגלותו (להלן – מידע סודי), ובלבד שאדם המבקש לעיין במידע שעליו המוחזק באותו מאגר יהיה זכאי לעיין במידע שאינו מידע סודי;

(5) על מאגר מידע אודות חקירות ואכיפת החוק של רשות המוסמכת לחקור על פי דין בעבירה, אשר שר המשפטים קבע אותה בצו, באישור ועדת החוקה חוק ומשפט של הכנסת;

(6) על מאגר מידע שהוקם לפי סעיף 28 לחוק איסור הלבנת הון, תש"ס–2000.

הנושא מצריך דיון נפרד, שאינו בליבת עבודתנו הנוכחית לגיבוש הצעה לחוק הגנת פרטיות חדש ומעודכן.

~~13א. עיון במידע שאינו בהחזקת בעל המאגר בלי לגרוע מהוראות סעיף 13 –~~

~~(1) בעל מאגר מידע, המחזיק אותו אצל אחר (בסעיף זה - המחזיק), יפנה את המבקש אל המחזיק, תוך ציון מענו, ויורה למחזיק, בכתב, לאפשר למבקש את העיון;~~

~~(2) פנה המבקש תחילה למחזיק, יודיע לו המחזיק אם הוא מחזיק מידע עליו, וכן את שם בעל מאגר המידע ואת מענו.~~

12. זכות לקבל הסבר

קיבל בעל שליטה במידע החלטה שיש לה השלכה משמעותית על זכות או חובה על פי דין של נושא מידע, המבוססת, במלואה או ברובה, על עיבוד מידע אישי על אודותיו באמצעות תהליכים ואמצעים אוטומטיים, יהיה נושא המידע זכאי לקבל מבעל שליטה במידע הסבר בהיקף סביר ובשפה מובנית על אופן קבלת ההחלטה.

13. ~~14.~~ זכות תיקון מידע אישי

סעיף 14 לחוק הקיים הופך לסעיף 13 המוצע

(א) נושא מידע~~אדם~~ שעיין במידע אישי על אודותיו~~שעליו~~ ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל שליטה~~המאגר~~ ב~~ה~~מידע, ~~ואם הוא תושב חוץ – למחזיק מאגר המידע,~~ בבקשה לתקן את המידע האישי ~~או למוחקו~~.

(ב) הוגשה ~~הסכים בעל מאגר המידע ל~~בקשה כאמור בסעיף קטן (א), על בעל שליטה במידע לנקוט את אחת מהפעולות הבאות, בהתחשב במטרה שלשמה בוצע עיבוד המידע האישי וסוג המידע האישי שבו מדובר:

(1) למחוק את המידע האישי, כולו או חלקו;

(2) לתקן את המידע האישי;

(3) להשלים את המידע האישי שבשליטתו;

(ג) ~~יבצע את השינויים הנדרשים במידע שברשותו ו~~בעל שליטה במידע יודיע על הפעולה שנקט לפי סעיף זה, בתוך 30 יום ממועד נקיטת

הפעלה, ~~עליהם~~ לכל מי שקיבל ממנו את המידע ~~בתקופה שנקבעה בתקנות~~ האישי במהלך תקופה של שנתיים שקדמו למועד קבלת בקשת התיקון.

(ד) על אף האמור בסעיף זה, מצא בעל שליטה במידע שהמידע האישי שבשליטתו נכון, מעודכן ומלא, רשאי הוא לס~~י~~רב ~~בעל מאגר המידע~~ ל~~מלא~~בקשה כאמור בסעיף קטן (א), ובלבד שינמק את סירובו בכתב~~יודיע על כך למבקש, באופן ובדרך שנקבעו בתקנות~~.

(ה) מעבד~~מחזיק~~ חייב למחוק, לתקן או להשלים את המידע האישי, אם בעל השליטה~~מאגר ה~~במידע הסכים לתיקון המבוקש או שבית משפט ציווה על התיקון.

דברי הסבר

סעיף 11: מבוסס על סעיף 13 לחוק הגנת הפרטיות הקיים, ושואב השראה מסעיפים 4.9 ל – PIPEDA בקנדה, ו-15 ל-GDPR.

ס"ק (א) מתייחס ל"אדם" ולא ל"נושא מידע", שכן בשלב זה עדיין לא בטוח שבעל שליטה במידע אכן מעבד מידע אישי על הפונה.

ס"ק (ב)(2)(ג) מבוסס על סעיף 15(1)(g) ל-GDPR ומחיל את זכות העיון גם על מקור המידע האישי, כאשר זה לא נאסף מנושא המידע עצמו. על מנת להימנע מפגיעה בעבודה עיתונאית ובחיסיון של מקורות עיתונאיים, ס"ק (ו) – המבוסס על סעיף 13(ג1) לחוק הגנת הפרטיות הקיים ועל סעיף 3(ד)(7) לחוק סדר הדין הפלילי[12] – מחריג מידע אישי שיש בגילויו כדי לפגוע בחיסיון על פי דין, לרבות חיסיון עיתונאי.

גביית תשלום בעבור מימוש זכות העיון תיעשה מכוח הסמכות הכללית לקביעת תשלומים בעבור מימוש זכות מזכויותיו של נושא המידע לפי סעיף 16(ב) להצעת החוק.

ס"ק (ד) מבוסס על סעיף 13(ב) לחוק הגנת הפרטיות הקיים. ואולם כדי להימנע מהטלת עלויות כבדות על בעל השליטה במידע או המעבד הסעיף אינו דורש לספק את המידע האישי באחת משלוש השפות – עברית, ערבית או אנגלית – אלא מסתפק בדרישה שהמידע האישי יימסר לעיון בשפה שבה הוא נאסף מלכתחילה ובתבנית דיגיטלית שמקובלת במשק באותה העת.

ס"ק (ה)(1) מבוסס על סעיף 13(ג) לחוק הגנת הפרטיות הקיים בשינויים המתחייבים מהסרת ההתייחסות בהצעת החוק למאגרי מידע.

ס"ק (ה)(1) מבוסס על סעיף 13(ג) לחוק הגנת הפרטיות הקיים, בשינויים המתחייבים מהסרת ההתייחסות למאגרי מידע בהצעת החוק. הסייגים בס"ק (ה)(1) ו-(ה)(2) שואבים השראה גם מסעיף 13(ד) לחוק זכויות החולה, התשנ"ו–1996, המתיר למטפל להימנע ממסירת מידע רפואי למטופל אם מסירתו עלולה לגרום נזק חמור לבריאותו הגופנית או הנפשית של המטופל.

הסייגים בס"ק (ה)(2) ו-(ה)(3) שואבים השראה מסעיף 15(4) ל-GDPR, אך צמצמנו את החריג כך שהוא אינו מתיר לבעל השליטה במידע לסרב לבקשת העיון בנימוק שהעיון עלול לפגוע בזכויותיו של בעל השליטה עצמו, למשל בזכויות הקניין הרוחני שלו או של המעבד.

מובהר שבנסיבות המפורטות בס"ק (ו) ו-(ז), כאשר חל על המידע האישי חיסיון או כאשר מסירתו היא בניגוד לדין, אין לבעל שליטה במידע שיקול הדעת אם להתיר את העיון אם לאו, בניגוד לשיקול הדעת הנתון לו ביישום החריגים לזכות העיון המפורטים בסעיף קטן (ה).

ס"ק (ח) מבוסס על סעיף 13(ה) לחוק הגנת הפרטיות הקיים. הנושא מצריך דיון שאינו בליבת עבודתנו הנוכחית לגיבוש הצעת חוק הגנת פרטיות חדש ומעודכן.

סעיף 13א לחוק הגנת הפרטיות הקיים שעוסק בעיון במידע שאינו בהחזקת בעל המאגר לא אומץ בהצעת החוק. עם זה, הוראה דומה להוראת סעיף 13א לחוק הגנת הפרטיות הקיים שולבה בסעיף 16 להצעת החוק.

סעיף 12: שואב השראה מפרשנות שניתנה בסעיף 71 להקדמה ל-GDPR לסעיף 22 ל-GDPR. על פי פרשנות זו – כחלק מזכותו של נושא המידע שלא תתקבל החלטה בעלת השלכות משפטיות או משמעותיות אחרות עליו, אשר מבוססת רק על עיבוד אוטומטי של מידע אישי – נתונה לנושא המידע גם הזכות לקבל מבעל שליטה במידע הסבר שיכלול את פירוט אופן קבלת החלטה המבוססת על ניתוח אוטומטי של המידע האישי עליו.

מאחר שתכליתה של הזכות של נושא המידע להתנגד לקבלת החלטה כאמור היא הזכות לכבוד ולא הזכות לפרטיות, ומשום שזכותו של נושא המידע להתנגד כאמור מטילה נטל לא מוצדק על חברות מסחריות – שיחויבו להותיר מעורבות אנושית בתהליכים שניתן לייעלם ולבצעם על ידי שימוש בטכנולוגיה בלבד – סעיף 12 להצעת החוק מאמץ רק את הזכות של נושא המידע לקבל הסבר מידתי מבחינת היקפו כאשר ההחלטה בעניינו משפיעה משמעותית על זכות או חובה על פי דין של נושא המידע וכאשר היא מבוססת במלואה או ברובה על עיבוד מידע אישי על נושא המידע באמצעות תהליכים אוטומטיים או אמצעים אוטומטיים.

מטרת הזכות לקבל הסבר נועדה למנוע מצב קפקאי שבו מתקבלת החלטה בעניינו של נושא המידע שאינה ברורה לו ואין ביכולתו להבינה ושיש לה השפעה משמעותית על זכות או חובה שלו על פי דין. בדרך זו תחוזק השקיפות בפעולותיהם של בעלי שליטה במידע, והם יחויבו לשקול, ואף להנגיש, את הפרמטרים מתוך המידע האישי שנעשה בהם שימוש בעת קבלת החלטה בעניינו של אדם.

סעיף 13: מבוסס על סעיף 14 לחוק הגנת הפרטיות הקיים ושואב השראה מסעיפים 16 ל-GDPR ו-13 לחוק הפרטיות האוסטרלי. הסעיף מוגבל, לפי ס"ק (א), לתיקון מידע אישי בלבד. נושא המידע אינו רשאי לבקש את מחיקתו, כלשון סעיף 14(א) לחוק הגנת הפרטיות הקיים. זכות המחיקה מעוגנת בנפרד בסעיף 15 בהצעת החוק. לבעל שליטה במידע מסור שיקול הדעת, לפי ס"ק (ב), אם לתקן, להשלים או למחוק את המידע האישי, הכול בהתאם למטרת העיבוד וסוג המידע האישי.

ס"ק (ג) מבוסס על סעיף 14(ב) לחוק הגנת הפרטיות הקיים, אך קובע פרק זמן של כשנתיים למתן הודעה לצדדים שלישיים שאליהם העביר בעל שליטה במידע את המידע האישי.

בעל שליטה במידע שמצא שהמידע שברשותו מלא, מעודכן ונכון ללא התיקון המבוקש, רשאי לפי ס"ק (ד), שמבוסס על סעיף 14(ג) לחוק הגנת הפרטיות, לסרב לבקשת תיקון מנימוקים שיירשמו.

ס"ק (ה) מבוסס על סעיף 14(ד) לחוק הגנת הפרטיות הקיים ומחייב את המעבד לפעול בהתאם לפעולות שנקט בעל השליטה במידע לפי ס"ק (ב).

~~2.~~14. הזכות לניוד מידע אישי

(א) כל נושא מידע זכאי, בהתאם לבקשה שהגיש לבעל שליטה במידע, שבשליטתו המידע האישי על אודותיו, לקבל לידיו מבעל שליטה במידע, את המידע אישי כאמור, בתבנית דיגיטלית מקובלת, ולהעבירו, על פי שיקול דעתו, בעצמו או לפי הוראת סעיף קטן (ד), לכל בעל שליטה במידע אחר (להלן – הזכות לניוד מידע אישי).

(ב) הזכות לניוד מידע אישי חלה על מידע אישי שעובד לפי הוראות סעיף 6 על אודות נושא המידע.

(ג) הזכות לניוד מידע אישי אינה חלה על מידע אישי שבעל שליטה במידע או המעבד הסיקו באמצעות עיבוד שנעשה לפי הוראות סעיף 6.

(ד) הוגשה בקשה לניוד מידע אישי כאמור בסעיף קטן (א), יעביר בעל שליטה במידע את המידע האישי על אודות מבקש הניוד לבעל שליטה במידע המבוקש על ידו, בהתאם לבקשה ובכפוף למגבלות טכנולוגיות. בעל שליטה במידע שאליו ינויד המידע האישי על פי סעיף זה, יהיה כפוף להוראות חוק זה במלואן.

(ה) בעל שליטה במידע שהוגשה לו בקשה לנייד מידע אישי כאמור בסעיף קטן (א), יידע את מבקש הניוד שאין בניוד המידע האישי לפי סעיף זה כדי להביא להפסקת עיבוד מידע אישי על אודותיו, וכי יש באפשרותו של מבקש הניוד לחזור בו מהסכמתו, במידה שניתנה, לפי סעיף 10 לחוק, או לפנות אל בעל השליטה במידע בבקשה למחוק את המידע האישי על אודותיו לפי סעיף 15.

(ו) על אף האמור בסעיף זה, בעל שליטה במידע רשאי לסרב לבקשה לפי סעיף קטן (א), אם לדעתו יש בניוד המידע האישי בהתאם לבקשה כדי לפגוע במידה העולה על הנדרש בזכויותיו של צד שלישי או במילוי חובותיו לפי דין.

(ז) שר המשפטים רשאי לקבוע בתקנות סוגים של בעלי שליטה במידע שהוראות סעיף זה לא יחולו עליהם.

15. זכות המחיקה של מידע אישי

(א) כל נושא מידע זכאי לדרוש מבעל שליטה במידע למחוק מידע אישי על אודותיו בהתקיים אחד מאלה:

(1) המידע האישי אינו נחוץ עוד למילוי המטרה שלשמה נאסף;

(2) נושא המידע חזר בו מהסכמתו לעיבוד מידע אישי לפי סעיף 10 ולא מתקיים אף אחד מהתנאים לפי סעיף 6(א)(1)-(2) או 6(ב)(1)-(2) המתירים את המשך עיבוד המידע האישי;

(3) עיבוד המידע האישי נעשה בניגוד להוראות חוק זה.

(ב) בעל שליטה במידע שהתבקש למחוק מידע אישי לפי סעיף קטן (א), ינקוט את הצעדים הסבירים בנסיבות העניין ובהתחשב בטכנולוגיה הקיימת באותה עת ובעלותה, על מנת למחוק את המידע האישי שבשליטתו, ואם העביר את המידע האישי - ליידע כל בעל שליטה אחר אליו העביר את המידע האישי שנושא המידע ביקש למחוק את המידע האישי וכל קישור אליו או העתק שלו;

(ג) על אף האמור בסעיף זה, בעל שליטה במידע רשאי לסרב לבקשת מחיקה לפי סעיף קטן (א), בהתקיים אחד מאלה:

(1) מחיקת המידע האישי תפגע במידה העולה על הנדרש בזכות לחופש ביטוי או בזכות הציבור לדעת;

(2) עיבוד המידע האישי דרוש לשם מילוי חובה חוקית;

(3) מחיקת המידע האישי תפגע במידה העולה על הנדרש ביכולתו של בעל השליטה במידע או המעבד להתגונן בתביעות משפטיות, או לבצע משימה המוטלת עליו למטרות אירכוב, מחקר מדעי, מחקר סטטיסטי שיש אינטרס ציבורי בביצועם.

16. מימוש זכויות נושא המידע

(א) בעל שליטה במידע ינקוט אמצעים סבירים כדי לוודא שהמבקש לחזור בו מהסכמתו לפי סעיף 10, לעיין במידע אישי לפי סעיף 11, לקבל הסבר לפי סעיף 12, לתקן מידע אישי לפי סעיף 13, לנייד מידע אישי לפי סעיף 14 או למחוק מידע אישי לפי סעיף 15 (להלן – "זכויות נושא המידע"), הוא אכן נושא המידע, בטרם מתן מענה לבקשה.

(ב) על בעל שליטה במידע לאפשר מימוש זכויות נושא המידע בכתב או בפורמט דיגיטלי ובתבנית מקובלת בתוך 14 ימים ממועד קבלת בקשה למימוש זכות מזכויות נושא המידע. בגין מימוש זכות מזכויות נושא המידע רשאי בעל שליטה במידע לגבות סכום שלא יעלה על ____ שקלים חדשים.

(ג) פנה נושא המידע למעבד בבקשה למימוש זכות מזכויות נושא המידע, יעביר לו המעבד בתוך 14 ימים מיום קבלת הבקשה את שם בעל השליטה במידע שבשליטתו מצוי המידע האישי נשוא הפנייה ואת דרכי הפנייה אליו. אין בהוראת סעיף קטן זה כדי לחייב למסור מידע אישי בניגוד לחיסיון שנקבע לפי כל דין, אלא אם כן המבקש הוא מי שהחיסיון נועד לטובתו. בסעיף קטן זה, "דין" – לרבות הלכה פסוקה.

(ד) סירב בעל שליטה במידע לבקשת נושא מידע למימוש זכות מזכויות נושא המידע, כאמור בסעיפים 11(ה)-(ח), 13(ד), 14(ו), או 15(ג), יודיע על כך למבקש בכתב או בפורמט דיגיטלי ובתבנית מקובלת בתוך 14 ימים ממועד קבלת הבקשה למימוש זכות מזכויות נושא המידע, תוך פירוט הנימוקים לסירוב.

סעיף 15 לחוק הקיים הופך לסעיף 17

17. ~~15.~~ תובענה לבית המשפט

על סירובו של בעל שליטה~~מאגר~~ במידע לבקשת נושא מידע למימוש זכות מזכויות נושא המידע, כאמור בסעיפים 11(ה)-(ח), 13(ד), 14(ו), או 15(ג), ~~לאפשר עיון כאמור בסעיף 13 או בסעיף 13א ועל הודעת סירוב כאמור בסעיף 14(ג),~~ רשאי נושא~~מבקש~~ המידע להגיש תובענה לבית המשפט באופן ובדרך שנקבעו בתקנות.

דברי הסבר

סעיף 14: שואב השראה מסעיף 20 ל-GDPR ומעגן את זכותו של נושא המידע לנייד מידע אישי עליו לבעלי שליטה במידע נוספים לפי שיקול דעתו. מטרת זכות הניוד היא לחזק את השליטה של נושא המידע במידע האישי עליו, לשכלל את השוק על ידי עידוד התחרות בין בעלי שליטה שונים במידע, להקטין את תלותם של נושאי מידע בפלטפורמות שירותי מידע אחת או בבעל שליטה אחד במידע ולמנוע את הגבלתם לאותה הפלטפורמה או לאותו בעל שליטה במידע.

לפי ס"ק (א), על בעל שליטה במידע לנייד את המידע האישי שיש ברשותו על מבקש הניוד למבקש הניוד עצמו או לבעל שליטה במידע אחר, על פי בקשת מבקש הניוד. ניוד המידע האישי ייעשה בתבנית דיגיטלית המקובלת במשק באותה העת.

כן נדרש בס"ק (ד) שהניוד יהיה אפשרי מבחינה טכנית, כלומר שאפשר להעביר את המידע האישי בדרך מאובטחת ובתנאי שלבעל השליטה במידע המקבל יש היכולות הטכניות לקבל את המידע האישי.

לפי ס"ק (ב), המידע האישי שזכות הניוד חלה עליו הוא כל מידע אישי שעובד לפי ההוראות שבסעיף 6 להצעת החוק. הסעיף מרחיב בכך את זכות הניוד מזו הקבועה בסעיף 20 ל-GDPR, המצומצמת רק למידע אישי שעובד בהסכמת נושא המידע. ההרחבה נחוצה על מנת להגשים את מטרת זכות הניוד. עם זאת, לפי ס"ק (ג), המבוסס על סעיף 20(1) ל-GDPR, זכות הניוד חלה רק על המידע האישי הגולמי שעובד לפי סעיף 6. זכות הניוד לא חלה על מידע אישי שבעל השליטה במידע או

שהמעבד הסיקו אותו באמצעות עיבוד מידע אישי לפי סעיף 6 להצעת החוק.

לפי ס"ק (ה), בעל שליטה במידע שהניוד התבקש ממנו צריך ליידע את נושא המידע מבקש הניוד שאין בניוד המידע האישי כדי להביא להפסקת עיבודו או למחיקתו. המטרה של חובת היידוע היא למנוע היווצרות רושם מוטעה שלפיו המידע האישי אינו נמצא עוד ברשותו של בעל השליטה במידע.

ס"ק (ו) שואב השראה מסעיף 20(4) ל-GDPR ומתיר לבעל שליטה במידע לסרב לבקשת ניוד כאשר זכות הניוד עלולה לפגוע במידה העולה על הנדרש בזכויותיהם של צדדים שלישיים או במילוי חובותיו של בעל השליטה במידע לפי דין.

ס"ק (ז) מסמיך את שר המשפטים לקבוע שבעלי שליטה במידע מסוימים יוחרגו מתחולת הסעיף מסיבות הקשורות בגודלם, במשך הזמן שחלף מרגע היווסדם או בנתח השוק שהם מחזיקים. המטרה היא להתמודד עם החשש שזכות הניוד עלולה לפגוע קשות דווקא בעסקים קטנים ובינוניים, שיתקשו להתמודד עם העברת מידע אישי מהם בשלבי הפעילות הראשונית שלהם, ולהביא בסופו של דבר להיחלשות התחרות ולהתחזקות החברות הגדולות.

<u>סעיף 15</u>: שואב השראה מסעיף 17 ל-GDPR ומעגן את זכות המחיקה, המכונה גם "הזכות להישכח".

ס"ק (א) מעגן את זכות נושא המידע, לרבות קטין, לדרוש את מחיקת מידע אישי עליו במקרים המנויים בסעיף. בה בעת, ס"ק (ב) מכיר בקושי האפשרי ליישם את זכות המחיקה, ובסכנה שזכות זו עלולה להתברר בעתיד כנטל בלתי סביר על כתפי חברות הטכנולוגיה. משום כך, מימוש זכות המחיקה על ידי בעל שליטה במידע, כלומר מחיקת המידע האישי וידוע בעלי שליטה נוספים שאליהם העביר את המידע האישי, תעשה לפי מבחן הסבירות ולפי נסיבות העניין, הטכנולוגיה הקיימת באותה העת ומחירה.

ס"ק (ג) מונה את הנסיבות שבהן יותר לבעל שליטה במידע לסרב לבקשת המחיקה.

<u>סעיף 16</u>: ס"ק (א) שואב השראה מחובת הזהירות הקבועה בסעיף 45 לחוק הפרטיות בניו-זילנד, שלפיה טרם מתן מענה לזכות העיון והתיקון יש לוודא שהמבקש הוא אכן נושא המידע.

ס"ק (ב) מבוסס על סעיפים 13(ד) ו-29א(ד) לחוק הגנת הפרטיות הקיים ועל תקנה 6 לתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי דין בערעור על סירוב לבקשת עיון), התשמ"א-1981, וקובע פרקי זמן למימוש כל אחת מן הזכויות של נושא המידע ומנגנון לגביית תשלום בגין מימוש זכויות נושא המידע.

ס"ק (ג) מבוסס על סעיף 13א(2) לחוק הגנת הפרטיות הקיים אך תחולתו רחבה יותר וחלה על כלל זכויות נושא המידע. עם זאת, הסעיף מאפשר למעבד להימנע ממענה שנדרש על פי הסעיף אם המענה יביא לחשיפת מידע שחל עליו חיסיון, למשל כאשר המעבד הוא חוקר פרטי או עיתונאי עצמאי עצם העברת פרטי יצירת הקשר עם בעל שליטה במידע עשויה להוות הודאה בכך שהמעבד אכן מעבד מידע אישי על נושא המידע.

ס"ק (ד) מחייב את בעל השליטה במידע לתת הודעת סירוב בתגובה לבקשת נושא המידע לממש זכות מזכויות נושא המידע.

<u>סעיף 17</u>: מבוסס על סעיף 15 לחוק הגנת הפרטיות הקיים ומעגן את הזכות לערער לבית המשפט על החלטת בעל שליטה לסרב לכל אחת מזכויות נושא המידע.

<u>סימן ג': חובות בעל השליטה במידע והמעבד</u>

<u>18. מעבד המידע</u>

<u>(א) מעבד יפעל על פי הוראות חוק זה ועל פי הנחיות בעל שליטה במידע.</u>

<u>(ב) על בעל שליטה במידע להבטיח שהמעבד נקט את כל האמצעים הדרושים לעיבוד מידע אישי וכיבוד זכויותיו של נושא המידע לפי חוק זה.</u>

<u>19. עיצוב לפרטיות</u>

<u>(א) בעל שליטה במידע יתכנן, יעצב ויפעיל, ככל שניתן, באמצעות הטמעת אמצעים טכנולוגיים וכן כללים פנים-ארגוניים, מערכות לעיבוד של מידע אישי, באופן שיבטיח את התאמתן להוראות חוק זה.</u>

<u>(ב) תכנון, עיצוב והפעלה של מערכות לעיבוד של מידע אישי כאמור בסעיף קטן (א), ייעשו בהתחשב בכל אלה: הטכנולוגיות הזמינות באותה עת ועלותן; אופי העיבוד של המידע האישי, וכן היקפו ומטרתו של העיבוד; והסכנות הצפויות לפגיעה בפרטיותו של נושא המידע עקב עיבוד המידע האישי על אודותיו.</u>

דברי הסבר

<u>סעיף 18:</u> שואב השראה מסעיפים 29 ו-28(1) ל-GDPR ומיועד להבהיר שעל בעל שליטה במידע להבטיח שמעבד מידע אישי שעימו הוא מתקשר נוקט את כל האמצעים הנדרשים, בכלל זה אמצעים טכניים וארגוניים, כדי לכבד את זכויותיו של נושא המידע לפי הצעת החוק ולהבטיח שעיבוד המידע האישי ייעשה בהתאם להוראות הצעת החוק.

<u>סעיף 19:</u> שואב השראה מסעיף 25 ל-GDPR. מטרתו להטיל על בעל שליטה במידע את החובה להבטיח הטמעת אמצעי הגנה על פרטיות במידע אישי באופן יזום מניעתי – החל בשלבי התכנון והפיתוח של המערכות לעיבוד מידע אישי, עבור בהטמעתן וכלה בהפעלתן – כל זה באמצעות אימוץ הדרישות ל"פרטיות כברירת מחדל" (privacy by default") ול"עיצוב לפרטיות" (privacy by design").

לדוגמה, על בעל שליטה במידע למזער ככל האפשר את עיבוד המידע האישי, לפעול להתממת מידע אישי, לעבד מידע אישי בשקיפות, לאפשר לנושא המידע לנטר את עיבוד המידע האישי עליו ולשפר בתכיפות גבוהה את אמצעי האבטחה. בעיצוב, בתכנות ובבחירת אפליקציות, שירותים או מוצרים המבוססים על עיבוד מידע אישי, בעל שליטה במידע או המעבד צריכים להתחשב בזכויותיו של נושא המידע ולוודא שהעיצוב, התכנות, האפליקציות, השירותים או כל טכנולוגיה אחרת המשמשת אותם לעיבוד מידע אישי מסייעים או שאינם פוגעים במילוי חובותיהם לפי הצעת החוק.

20. תסקיר השפעה על הפרטיות

(א) בעל שליטה במידע יכין תסקיר השפעה על הפרטיות (בסעיף זה – תסקיר ההשפעה על הפרטיות) כאשר בכוונתו לעשות אחד מאלה:

(1) לבצע עיבוד מידע אישי, שבהתחשב בהיקפו ומטרתו, סביר שיביא לפגיעה בזכויות צדדים שלישיים;

(2) לבצע עיבוד מידע אישי בהיקף נרחב העשוי להשפיע על מספר רב של נושאי מידע;

(3) לבצע עיבוד מידע אישי באופן אוטומטי או בעיקר אוטומטי לשם הערכת מאפייני האישיות של נושא המידע וקבלת החלטות בעלות השלכות משמעותיות על זכויות או חובות לפי דין של נושא המידע;

(4) לבצע עיבוד מידע רגיש בהיקף נרחב;

(ב) תסקיר ההשפעה על הפרטיות יכלול התייחסות, בין השאר, להיקף המידע האישי הנאסף, לעיצוב לפרטיות לפי סעיף 19 ולאמצעי אבטחת מידע אישי שינקטו על ידי בעל שליטה במידע לפי סעיף 21.

(ג) תסקיר ההשפעה על הפרטיות לפי סעיף קטן (א) יוכן לפני תחילת העיבוד של המידע אישי ולפני אימוץ טכנולוגיה חדשה לעיבוד המידע אישי, וכן אחת ל-18 חודשים לפחות.

~~16.סודיות~~

~~לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך ביצוע עבודתו או לביצוע חוק זה או על פי צו בית משפט בקשר להליך משפטי; אם הוגשה הבקשה לפני תחילת ההליך תידון הבקשה בבית משפט השלום. המפר הוראות סעיף זה, דינו - מאסר 5 שנים.~~

דברי הסבר

סעיף 20: מעגן חובה כללית על בעל שליטה במידע לערוך סקר סיכונים לפגיעה בפרטיות. חובה דומה נמצאת כיום בתקנה 5 לתקנות אבטחת מידע, אך היא מוגבלת רק למאגרי מידע שנדרשת בעניינם רמת אבטחה גבוהה.[13] בעתיד נפעל להצעת תיקון לתקנות אבטחת מידע על פי המוצע בסעיף זה.

ס"ק (א) שואב השראה מסעיפים 35(1) ו-35(3) ל-GDPR. הסעיף מעגן חובה כללית על בעל שליטה במידע לערוך תסקיר השפעה על הפרטיות בהתאם לפעולות העיבוד שברצונו לעשות, ולפי מבחן סבירות שיתחשב במטרת העיבוד, בהיקפו ובסוג המידע האישי המעובד.

סעיף 16 לחוק הפרטיות הקיים שעוסק בחובת הסודיות, לא אומץ בהצעת החוק. החובה לשמור על סודיות המידע האישי והעונש בגין הפרתה שולבו בסעיפים 21 ו-62 להצעת החוק.

סעיף 17 לחוק הקיים הפך לסעיף 21 המוצע

21. 17. אחריות לאבטחת מידע אישי

בעל מאגר שליטה במידע או מעבד, יהיו אחראים, ביחד ובנפרד, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע האישי שבשליטתם או ברשותם וינקטו אמצעים סבירים לצורך אבטחתו, בהתאם לתקן מקובל של אבטחת מידע ולעלותו הכספית, ובהתחשב בסוג המידע האישי, מטרת העיבוד, היקפו, הסכנות הצפויות לפגיעה בפרטיות עקב שימוש לרעה בו, אובדן, שינוי, גילוי, גישה בלתי מורשית אליו או מחיקה בלתי חוקית או מקרית שלו שבמאגר המידע.

22. תיעוד ודיווח על אודות אירוע אבטחה

(א) בעל שליטה במידע אחראי לתיעוד כל אירוע אבטחה שאירע בנוגע למידע האישי שבשליטתו; תיעוד כאמור יבוסס, ככל האפשר, על רישום אוטומטי.

(ב) בעל שליטה במידע ידווח לרשות להגנת הפרטיות על אירוע אבטחה תוך זמן סביר מהמועד שנודע לו על התרחשותו, בהתקיים אלה:

(1) אירוע האבטחה הוביל לעיבוד לא מורשה של מידע אישי או לנסיבות שסביר להניח שיגרמו לעיבוד לא מורשה של מידע אישי;

(2) סביר להניח שאירוע האבטחה יגרום נזק חמור לנושא המידע;

(3) בעל השליטה במידע אינו יכול למנוע את הנזק החמור לנושא המידע באמצעות נקיטת פעולה מתקנת;

בסעיף זה, "פעולה מתקנת"– פעולה שעל בעל שליטה במידע לנקוט לבירור הסיבות שהובילו לאירוע האבטחה, למניעת הישנות אירוע האבטחה ולמיזעור השלכות אירוע האבטחה על זכויות של נושא המידע לפי חוק זה.

(ג) לאחר הדיווח לרשות להגנת הפרטיות כאמור בסעיף קטן (ב), יודיע בעל שליטה במידע לנושא המידע, תוך זמן סביר, על אירוע האבטחה, אלא בהתקיים אחד מאלה:

(1) מתן ההודעה עלול להביא לחשיפת מידע אישי שחל לגביו חיסיון לפי כל דין, אלא אם כן נושא המידע הוא מי שהחיסיון נועד לטובתו; בפסקה זו, "דין" – לרבות הלכה פסוקה;

(2) מתן הודעה כאמור לכל נושא מידע העלול להיפגע מאירוע האבטחה מטיל על בעל שליטה במידע נטל בלתי סביר; במקרה זה, יפרסם בעל שליטה במידע הודעה לכלל הציבור על אודות אירוע האבטחה.

(ד) אירע אירוע אבטחה, יודיע על כך המעבד לבעל שליטה במידע באופן מיידי.

(ה) שר המשפטים יקבע תקנות בעניינים הבאים:

(1) סוגי אירועי אבטחה וסוגי בעלי שליטה במידע הפטורים מחובת הדיווח לפי סעיף קטן (ב);

(2) אופן מתן ההודעות לפי סעיפים קטנים (ב) עד (ד) ותוכנן.

(3) מהן הפעולות המתקנות שעל בעל שליטה במידע לנקוט במקרה של אירוע אבטחה.

17א. מחזיק במאגרים של בעלים שונים

(א) מחזיק במאגרי מידע של בעלים שונים יבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בינו לבין בעליו של אותו מאגר.

(ב) מחזיק שברשותו חמישה מאגרי מידע לפחות, החייבים ברישום לפי סעיף 8, ימסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשותו, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על האבטחה כאמור בסעיף 17ב.

דברי הסבר

<u>סעיף 21:</u> מבוסס על סעיף 17 לחוק הגנת הפרטיות הקיים ושואב השראה מסעיפים 32 ל-GDPR, 4.7 לנספח 1 לחוק הפרטיות הקנדי, 11.1 לחוק הפרטיות האוסטרלי ו-5 לחוק הפרטיות הניו זילנדי. הסעיף מעגן חובת אבטחת מידע כללית לפי תקן מקובל של אבטחת מידע ולפי מבחן סבירות שיתחשב גם בסוג המידע האישי, במטרת העיבוד והיקפו ובסכנות הצפויות לפגיעה בפרטיות. החובה לאבטחת מידע כוללת גם שמירה על הסודיות של מידע אישי.

<u>סעיף 22:</u> הסעיף מעגן את החובה לתעד אירועי אבטחת מידע אישי הקבועה כיום בתקנה 11 לתקנות אבטחת מידע ולתקנה על בסיס סעיפים 33 ו-34 ל-GDPR והתיקון לחוק האוסטרלי להגנת פרטיות במידע.[14] בעתיד נפעל לקדם הצעת תיקון לתקנות אבטחת מידע על פי המוצע בסעיף זה.

ההסדר הקבוע בתקנה 11 לתקנות אבטחת מידע מחייב בעל שליטה במידע לדווח לנושא מידע על אירוע אבטחת מידע רק במקרה של אירוע אבטחה חמור ורק כאשר ראש הרשות להגנת הפרטיות, לאחר היוועצות עם ראש מערך הסייבר, הורה על מתן הודעה כאמור. חובת ההיוועצות עם ראש מערך הסייבר עלולה לגרום סרבול בירוקרטי מיותר.

ההסדר המוצע בסעיף 22 מחייב בעל שליטה במידע לדווח לראש הרשות להגנת הפרטיות על אירוע אבטחת מידע רק כאשר האירוע גרם פגיעה בזכות לפרטיות, בהתאם לתנאים המפורטים בס"ק (ב) ובהתבסס על התיקון לחוק הפרטיות האוסטרלי. להסדר המוצע שלוש מטרות: האחת - להימנע מהטלת נטל לא סביר על בעל שליטה במידע לדווח על כל אירוע אבטחה גם אם לא נגרמה בגינו פגיעה בפרטיות (למשל, כאשר עובד לקח הביתה בטעות התקן נייד שנושא מידע אישי אבל לא השתמש בו והחזירו למחרת היום למקום העבודה); השנייה – להימנע מהטלת חובת דיווח פומבית מיידית שיש בכוחה לגרום לחשיפת אירועי סייבר באופן שעלול לפגוע בהתמודדות עם האירוע בזמן אמת; והשלישית – להימנע מהפיכת פעולת הדיווח לפעולה טכנית בעיקרה ומהצפת הרשות להגנת הפרטיות.

ס"ק (ג) מטיל על בעל שליטה במידע את החובה לדווח לנושא מידע על אירוע אבטחה שהביא לפגיעה בפרטיותו בתוך פרק זמן סביר ורק לאחר שמסר דיווח, כנדרש לפי סעיף קטן (ב), לראש הרשות להגנת הפרטיות. לחלופין, חובת הודעה פומבית תחול רק כאשר הודעה לכל נושא מידע שעלול להיפגע מאירוע האבטחה תדרוש מאמץ לא סביר מבעל שליטה במידע.

ס"ק (ד) מבוסס על סעיף 33(2) ל-GDPR ומחייב את המעבד לדווח לבעל שליטה במידע על התרחשותו של אירוע אבטחה.

ס"ק (ה)(1) מסמיך את שר המשפטים להחריג בתקנות אירועי אבטחה ובעלי שליטה במידע מסוימים מחובת התיעוד והדיווח. הסעיף מתכתב עם ההבחנה הקיימת בתקנות אבטחת מידע שחובת התיעוד והדיווח חלה רק במקרים של "אירוע אבטחה חמור".

כדי להגביר את הגמישות בהחלת חובת הדיווח לפי הוראת סעיף 22 הותרנו בסעיפים קטנים בס"ק (ה)(2) ו-(ה)(3) את הקביעה מה יכלול דיווח על אירוע אבטחה ומהי פעולה שתיחשב "פעולה מתקנת" לתקנות. ככלל, דיווח כאמור צריך לכלול פרטים מזהים ופרטי יצירת קשר עם בעל שליטה במידע, תיאור של אירוע האבטחה ונסיבותיו, תיאור המידע האישי שעובד או סביר שיעובד בלי הרשאה כתוצאה מאירוע האבטחה ופירוט הפעולות המתקנות שביצע בעל שליטה במידע עד למועד הדיווח ואלו שהוא עתיד לבצע. בדיווח לנושא המידע יש לכלול גם פרטים על הפעולות שרצוי שנושא המידע יבצע עקב אירוע האבטחה.

<u>סעיף 17א לחוק הגנת הפרטיות הקיים</u> שעוסק בחובותיו של מחזיק במאגרים של בעלים שונים לא אומץ בהצעת החוק. הצעת החוק אינה כוללת התייחסות למאגרי מידע או ל"מחזיק". נוסיף עוד כי חובותיו של מעבד מוסדרות בסעיף 18 להצעת החוק.

סעיף 17ב לחוק הקיים הפך לסעיף 23 המוצע.

23. 17ב. ממונה על הגנת הפרטיות במידעאבטחה

(א) בעל שליטה במידע ומעבד ימנו, כל אחד מטעמו, ממונה על הגנת הפרטיות במידע העומד בתנאי הכשירות שנקבעו לפי סעיף קטן (ו), בהתקיים אחד מאלה:הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן - הממונה):

(1) מחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8;

(1) בעל שליטה במידע או המעבד, לפי העניין, הוא גוף ציבורי כהגדרתו בסעיף 23;

(2) בעל שליטה במידע או המעבד, לפי העניין, מבצע עיבוד מידע אישי על 200,000 נושאי מידע לפחות;

(3) בעל שליטה במידע או המעבד, לפי העניין, מבצע עיבוד מידע רגיש על 100,000 נושאי מידע לפחות.בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.

(ב) הממונה על הגנת הפרטיות במידע יפעל להבטחת קיום הוראות חוק זה על ידי בעל שליטה במידע או המעבד, לפי העניין, ויהיה אחראי לטיפול בפניות הציבור וכן בפניות של ראש הרשות להגנת הפרטיות, בנוגע לקיום הוראות חוק זה.בלי לגרוע מהוראות סעיף 17, הממונה יהיה אחראי לאבטחת המידע במאגרים המוחזקים ברשות הגופים כאמור בסעיף קטן (א).

(ג) בעל שליטה במידע או המעבד, לפי העניין, יספק לממונה על הגנת הפרטיות במידע את התנאים הדרושים למילוי תפקידו, לרבות עצמאות בביצוע תפקידיו לפי חוק זה.

(ד) לא ימונה כממונה על הגנת הפרטיות במידע מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה.

(ה) פרטי יצירת הקשר עם הממונה על הגנת הפרטיות במידע ימסרו על פי דרישה או יפורסמו בהתאם להחלטת בעל שליטה במידע או המעבד, לפי העניין. לכל אדם הזכות לפנות לממונה על הגנת הפרטיות במידע בכל הקשור לעיבוד מידע אישי על אודותיו ומימוש זכויות נושא המידע לפי חוק זה.

(ו) שר המשפטים יקבע בתקנות את תנאי הכשירות הנדרשים למינוי ממונה על הגנת הפרטיות במידע ואת הפעולות שעליו לבצע למילוי תפקידו לפי חוק זה, וכן רשאי שר המשפטים, בתקנות, לשנות את מספר נושאי המידע הקבועים בפסקאות (2) או (3) של סעיף קטן (א), לפטור סוגים מסוימים של בעלי שליטה או מעבדים מחובת מינוי ממונה על הגנת פרטיות במידע לפי סעיף קטן (א) או לחייבם במינוי כאמור.

סימן ד': שונות

24. תחולת הוראות פרק ב'

הוראות פרק ב' יחולו על אלה:

(1) בעל שליטה במידע או מעבד המאוגדים או פועלים במדינת ישראל, בין אם עיבוד המידע האישי נעשה בתחומי מדינת ישראל ובין אם לאו;

(2) כל פעולת עיבוד של מידע אישי על אודות נושא מידע הנמצא במדינת ישראל, בין אם בעל השליטה במידע או המעבד נמצאים או מאוגדים בישראל ובין אם לאו, ובלבד

<u>שמטרת עיבוד המידע האישי היא אחת מאלה:</u>
<u>(א) מתן טובין או שירות לנושא מידע הנמצא בישראל;</u>
<u>(ב) ניטור התנהגות של נושא מידע המתבצעת במדינת ישראל.</u>

דברי הסבר

<u>**סעיף 23:**</u> משלב בין החובה למנות ממונה אבטחת מידע לפי סעיף 17ב לחוק הגנת הפרטיות הקיים ולפי תקנה 3 לתקנות אבטחת מידע לבין החובה למנות ממונה פרטיות לפי סעיפים 37 ו-39 ל-GDPR, 4.1 לנספח 1 לחוק הפרטיות הקנדי ו-23 לחוק הפרטיות הניו זילנדי. בעתיד נפעל לקדם הצעת תיקון לתקנות אבטחת מידע על פי המוצע בסעיף זה.

החובה למנות ממונה על הגנת פרטיות במידע תיקבע לפי ס"ק (א) בהתאם למיהות הגוף המבצע עיבוד (גוף ציבורי) ובהתאם להיקף העיבוד של מידע אישי או מידע רגיש. בדרך זו החובה אינה מצומצמת יתר על המידה, כקבוע כיום בסעיף 17ב לחוק הגנת הפרטיות, אבל גם אינה רחבה מדי ועל כן אינה מטילה נטל לא סביר על גופים קטנים.

ס"ק (א) ו-(ו) קובעים את תנאי הכשירות הנדרשים למינוי, וס"ק (ג) מטיל על בעל שליטה ועל מעבד את האחריות לתת לממונה על הגנת הפרטיות במידע את תנאי ההעסקה המתאימים, לרבות פניות לביצוע התפקיד מבחינת עומס המשימות שיוטל עליו ועצמאות בביצוע תפקידו – כדי להבטיח שיפעל למילוי הוראות חוק זה בלי לחשוש למעמדו בחברה או להמשך העסקתו.

ס"ק (ב) מפרט מסגרת כללית לתפקידי הממונה על הגנת הפרטיות. ס"ק (ד) מבוסס על סעיף 17ב(ג) לחוק הגנת הפרטיות הקיים. ס"ק (ה) שואב השראה מסעיף 4.1.2 לחוק הפרטיות הקנדי וקובע שפרטי יצירת הקשר עם הממונה על הגנת הפרטיות יימסרו על פי דרישה או יפורסמו בהתאם להחלטת בעל שליטה במידע או מעבד. הסעיף אינו מטיל חובה להעביר לרשות להגנת הפרטיות את פרטי הקשר עם הממונה על הגנת הפרטיות במידע, בדומה לסעיף 37(7) ל-GDPR, שכן חיוב כאמור כמוהו כהחזרת החובה לרישום מאגרי מידע, שהטעמים להסרתה הוסברו בדברי ההסבר למחיקת סעיפים 8, 9, 10(א)-(ה), (ו)-(ז) לחוק הפרטיות הקיים.

ס"ק (ו) מסמיך את שר המשפטים לשנות את התנאים לכינונה של החובה למינוי ממונה על הגנת הפרטיות וכן לפרט את הכישורים הנדרשים להתאמתו לתפקיד.

<u>**סעיף 24:**</u> שואב השראה מסעיף 3 ל-GDPR. מטרתו לקבוע שבהתקיים אחת החלופות המפורטות בסעיף תהא תחולת הוראות פרק ב' להצעת החוק חוץ-טריטוריאלית. המטרה היא למנוע מבעלי שליטה במידע להתחמק מציות להוראות החוק על ידי העברת מידע אישי על נושאי מידע ישראלים לחוות שרתים הממוקמות במדינות שאינן מחייבות הגנת פרטיות ברמה דומה לזו שבישראל.

לצורך החלה חוץ-טריטוריאלית של פרק ב' אין די בכך שאתר האינטרנט או כתובת הדוא"ל של בעל השליטה במידע או המעבד זמינים לקהל בישראל או שעיבוד המידע האישי נעשה בשפה העברית. לעומת זאת, מתן האפשרות ליצור קשר עם בעל השליטה במידע או עם המעבד דרך אתר אינטרנט בשפה העברית; מתן האפשרות להזמין טובין או שירות בשפה העברית או באמצעות תשלום במטבע ישראלי, תשלום למנוע חיפוש בתמורה להצגת האתר במיקום גבוה בתוצאות החיפוש בתגובה לשאילתות חיפוש מישראל – מלמדים על כוונתו של בעל שליטה במידע או של מעבד להציע שירות או טובין לנושאי מידע בישראל.

25. נציגות בעל שליטה במידע או מעבד בישראל

(א) בעל שליטה במידע או מעבד, לפי העניין, המבצע עיבוד מידע רגיש על אודות 500,000 נושאי מידע לפחות, או המבצע עיבוד מידע אישי על אודות 1,000,000 נושאי מידע לפחות, ומתקיימים תנאי סעיף 24(2), חובה עליו למנות בכתב נציג שמקום מושבו במדינת ישראל ואשר ישמש כתובת לפניות הרשות להגנת הפרטיות או נושאי המידע בכל הקשור ליישום הוראות חוק זה.

(ב) חובת מינוי נציג לפי סעיף קטן (א) לעיל לא תחול כאשר בעל שליטה במידע או המעבד, לפי העניין, הוא גוף ציבורי.

~~סימן ב': דיוור ישיר~~

~~17ג. הגדרות~~
~~בסימן זה –~~
~~"דיוור ישיר" - פניה אישית לאדם, בהתבסס על השתייכותו לקבוצת אוכלוסין, שנקבעה על פי איפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע;~~
~~"פניה" - לרבות בכתב, בדפוס, בטלפון, בפקסימליה, בדרך ממוחשבת או באמצעי אחר;~~
~~"שירותי דיוור ישיר" - מתן שירותי דיוור ישיר לאחרים בדרך של העברת רשימות, מדבקות או נתונים בכל אמצעי שהוא.~~

~~17ד. דיוור ישיר~~
~~לא ינהל אדם ולא יחזיק מאגר מידע המשמש לשירותי דיוור ישיר, אלא אם כן הוא רשום בפנקס ואחת ממטרותיו הרשומות היא שירותי דיוור.~~

~~17ה. ציון מקור המידע~~
~~לא ינהל אדם ולא יחזיק מאגר מידע המשמש לשירותי דיוור ישיר, אלא אם כן יש בידו רישום המציין את המקור שממנו קיבל כל אוסף נתונים המשמש לצורך מאגר המידע ומועד קבלתו, וכן למי מסר כל אוסף נתונים כאמור.~~

~~17ו. מחיקת מידע ממאגר מידע המשמש לדיוור ישיר~~
~~(א) כל פניה בדיוור ישיר תכיל באופן ברור ובולט –~~
~~(1) ציון כי הפניה היא בדיוור ישיר, בצירוף ציון מספר הרישום של המאגר המשמש לשירותי דיוור ישיר בפנקס מאגרי מידע;~~
~~(2) הודעה על זכותו של מקבל הפניה להימחק מן המאגר כאמור בסעיף קטן (ב), בצירוף המען שאליו יש לפנות לצורך כך;~~
~~(3) זהותו ומענו של בעל מאגר המידע שבו מצוי המידע שעל פיו בוצעה הפניה, והמקורות שמהם קיבל בעל המאגר מידע זה.~~
~~(ב) כל אדם זכאי לדרוש, בכתב, מבעל מאגר מידע המשמש לדיוור ישיר, שמידע המתייחס אליו יימחק ממאגר המידע.~~
~~(ג) כל אדם זכאי לדרוש, בכתב, מבעל מאגר המידע המשמש לשירותי דיוור ישיר או מבעל מאגר המידע שבו מצוי המידע שעל-פיו בוצעה הפניה, כי מידע המתייחס אליו לא יימסר לאדם, לסוג בני אדם או לאנשים מסויימים, והכל לפרק זמן מוגבל או קבוע.~~
~~(ד) הודיע אדם לבעל מאגר המידע על דרישתו כאמור בסעיפים קטנים (ב) או (ג), יפעל בעל המאגר בהתאם לדרישה ויודיע לאדם, בכתב, כי פעל על פיה.~~
~~(ה) לא הודיע בעל מאגר המידע כאמור בסעיף קטן (ד) תוך 30 ימים מיום קבלת הדרישה, רשאי האדם שהמידע מתייחס אליו לפנות לבית משפט השלום בדרך שנקבעה בתקנות, כדי שיורה לבעל מאגר המידע לפעול כאמור.~~
~~(ו) הזכויות לפי סעיף זה של נפטר שרשום במאגר מידע נתונות גם לבן זוגו, לילדו, להורהו או לאחיו.~~

~~17ז. תחולה על ידיעות~~
~~הוראות סימן זה יחולו על ידיעות הנוגעות לענייניו הפרטיים של אדם, אף שאינם בגדר~~

~~מידע, כשם שהן חלות על מידע.~~

~~17ח. אי תחולה על גוף ציבורי~~
~~סימן זה לא יחול על גוף ציבורי כמשמעותו בסעיף 23(1) במילוי תפקידיו על פי דין.~~

~~17ט. שמירת דינים~~
~~הוראות סימן זה באות להוסיף על הוראות כל דין.~~

~~פרק ג': הגנות~~

~~18.הגנות מה הן~~ סעיף 18 לחוק הגנת הפרטיות הקיים הועבר לסעיף 65 המוצע.

~~19.פטור~~ סעיף 19 לחוק הגנת הפרטיות הקיים הועבר לסעיף 66 המוצע.

~~20.נטל ההוכחה~~ סעיף 20 לחוק הגנת הפרטיות הקיים הועבר לסעיף 65.

~~21.הפרכה של טענות הגנה~~ סעיף 21 לחוק הגנת הפרטיות הקיים הועבר לסעיף 67 המוצע.

~~22.הקלות~~ סעיף 22 לחוק הגנת הפרטיות הקיים הועבר לסעיף 64 המוצע.

דברי הסבר

סעיף 25: שואב השראה מסעיף 27 ל-GDPR. מטרתו להקל על אכיפת ההוראות שבהצעת החוק גם על תאגידי ענק בינלאומיים שאין להם נציגות משפטית מקומית ולהימנע מפגיעה בתחרות ומהדרת שחקנים בינלאומיים מתחומי מדינת ישראל.

סימן ב': דיוור ישיר בחוק הקיים נמחק. נושא הדיוור הישיר אינו חלק מהגנת הזכות לפרטיות וצריך להיות מטופל בחוקים אחרים כגון סעיף 30א לחוק התקשורת (בזק ושידורים), התשמ"ב–1982.

פרק ג: הרשות להגנת הפרטיות וסמכויות פיקוח, אכיפה ובירור מינהלי

סימן א': הרשות להגנת הפרטיות

26. ראש הרשות להגנת הפרטיות

מי שמתקיימים בו תנאי הכשירות להתמנות לשופט של בית משפט מחוזי ומונה על ידי הממשלה, בהודעה ברשומות, לנהל את הרשות להגנת הפרטיות.

27. תקציב הרשות

תקציב הרשות להגנת הפרטיות ייקבע בחוק התקציב השנתי, בסעיף תקציב נפרד, כמשמעותם בחוק יסודות התקציב, התשמ"ה–1985; הממונה על סעיף תקציב זה לעניין החוק האמור יהיה ראש הרשות להגנת הפרטיות.

28. עסקאות הרשות

לצורך ביצוע הוראות חוק זה, מורשה ראש הרשות להגנת הפרטיות, יחד עם חשב הרשות, לייצג את הממשלה בעסקאות כאמור בסעיפים 4 ו 5 לחוק נכסי המדינה, התשי"א-1951, למעט עסקאות במקרקעין, ולחתום בשם המדינה על מסמכים הנוגעים לעסקאות כאמור.

29. עובדי הרשות להגנת הפרטיות

(א) עובדי הרשות להגנת הפרטיות יהיו עובדי המדינה ויחולו עליהם הוראות חוק שירות המדינה (מנויים), התשי"ט–1959, ואולם ראש הרשות מורשה, באישור שר המשפטים, יחד עם חשב הרשות, לייצג את המדינה בעשיית חוזים מיוחדים עם עובדים.

(ב) עובדי הרשות יפעלו לפי הוראות ראש הרשות להגנת הפרטיות ובפיקוחו.

דברי הסבר

סעיפים 26-29: סעיפים אלו שואבים השראה מסעיפים 10(ד) לחוק הגנת הפרטיות הקיים, 41, 41א, 41ב לחוק ההגבלים העסקיים, התשמ"ח–1988, ו-19א-19ג לחוק הגנת הצרכן, התשמ"א–1981. מטרתם להקנות לראש הרשות להגנת הפרטיות כלים שיאפשרו לו וליחידתו חופש פעולה מינהלי ותקציבי שיסייעו בביצוע תפקידיו המורכבים. תקציב הרשות ייקבע בחוק התקציב בסעיף נפרד. ראש הרשות להגנת הפרטיות יהיה הממונה על ביצועו של התקציב, וכך תובטח עצמאותם של הרשות ושל ראש הרשות בניהול הרשות ובהפעלת התקציב שיוקצה לפעולותיה. עובדי הרשות יהיו עובדי מדינה ועל כן יחויבו בנורמות המהותיות והאתיות של עובדי המדינה ויהיו כפופים לחוק שירות המדינה (מינויים), התשי"ט–1959. בד בבד תוקנה לרשות להגנת הפרטיות יכולת ניהול אוטונומית מסוימת.

30. תפקידי הרשות להגנת הפרטיות

(א) תפקידי הרשות יהיו –

(1) לפקח על ביצוע הוראות חוק זה;

(2) לחקור חשד לביצוע עבירה לפי חוק זה ולהביא את העבריין לדין;

(3) לנקוט הליכי אכיפה מינהלית נגד מפר לפי הוראות חוק זה;

(4) לטפח תודעה ציבורית להגנת הפרטיות באמצעות חינוך, הדרכה והסברה, ככל שתפקיד זה אינו מוטל על רשות ציבורית אחרת הפועלת על פי דין;

(5) לטפל בתלונות שיש בהן ממש על הפרת הוראות חוק זה או על פגיעה אחרת בפרטיות נושא מידע;

(6) לערוך וליזום סקרים ומחקרים בענייני הגנת הפרטיות;

(7) לייעץ לממשלה בכל הקשור ביישום מטרות חוק זה;

(8) לטפל בכל עניין אחר הקשור להגנת הפרטיות ואשר לא הוטל בדין על רשות אחרת.

(ב) הגיעה לראש הרשות להגנת הפרטיות תלונה בעניין שבו לפי חיקוק יש לרשות אחרת סמכות לפיקוח ולנקיטת אמצעים בעקבות בירור תלונה, ייוועץ באותה רשות לפני שיטפל בתלונה, ורשאי הוא אף להעביר את התלונה אליה; העביר ראש הרשות להגנת הפרטיות את התלונה כאמור, תודיע הרשות אליה הועברה התלונה לראש הרשות להגנת הפרטיות על תוצאות הטיפול.

(ג) ראה ראש הרשות להגנת הפרטיות כי מטרות החוק לפי סעיף 1 מושפעות, כרוכות או עלולות להיות מושפעות או כרוכות בהליך פלוני שלפני בית משפט, רשאי הוא, לפי ראות עיניו, להתייצב באותו הליך ולהשמיע דברו, או להסמיך במיוחד את נציגו לעשות זאת מטעמו;

דברי הסבר

סעיף 30: עיקרו של הסעיף מבוסס על סעיף 20 לחוק הגנת הצרכן, התשמ"א-1981, מתוך הבנה שיש דמיון רב בין הרשות להגנת הצרכן וסחר הוגן לבין הרשות להגנת הפרטיות. הדמיון בין שתי הרשויות בא לידי ביטוי בקהלי היעד שכל אחת מן הרשויות פועלת מולם, בסוג ההליכים שהן מוסמכות לנהל ובטיפוסי הזכויות שהן אמורות להגן עליהן. בשונה מחוק הגנת הצרכן, הסעיף מעגן את תפקידי הרשות ולא רק את תפקידי ראש הרשות, בדומה לסעיף 18ח לחוק שוויון הזדמנויות בעבודה, התשמ"ח–1988, ולסעיף 5 לחוק הרשות השניה לטלויזיה ורדיו, התש"ן–1990.

ס"ק (א)(7) שואב השראה מסעיף 8 לחוק לעידוד מחקר, פיתוח וחדשנות טכנולוגית בתעשיה, התשמ"ד–1984. מטרתו להעמיק את המתאם בין מדיניות הממשלה לפעילות של הרשות להגנת הפרטיות, הן ברמה הכללית והן ברמה היישומית הפרטנית, באמצעות הסמכת הרשות להגנת הפרטיות לייעץ לממשלה בכל הקשור ליישום של מטרות החוק.

ס"ק (ג) שואב השראה מסעיף 1 לפקודת סדרי הדין (התייצבות היועץ המשפט לממשלה) [נוסח חדש]. מטרתו להבטיח את הצגת האינטרס הציבורי שבהגנה על הזכות לפרטיות על ידי אנשי מקצוע בתחום בהליכים משפטיים, בכלל זה ההליכים המתנהלים נגד הרשות המחוקקת או המבצעת.

31. שיתוף פעולה עם רשות חוץ

(א) מצא ראש הרשות להגנת הפרטיות כי התקיימו כל אלה:

(1) רשות חוץ הגישה לרשות להגנת הפרטיות בקשה לסיוע;

(2) נושא הבקשה לסיוע עשוי להיות הפרה של דיני הגנת הפרטיות שרשות חוץ, שהגישה את הבקשה, מופקדת על ביצועם, אכיפתם ופיקוחם;

רשאי הוא לקבוע כי על הבקשה לסיוע יחולו הוראות סעיף זה.

(ב) לא תיעשה פעולה מכוח הוראות סעיף זה אם היא עלולה, לדעת היועץ המשפטי לממשלה, לפגוע בריבונות מדינת ישראל, בביטחונה, באינטרס החיוני לה, בתקנת הציבור או בחקירה תלויה ועומדת.

(ג) כדי להבטיח מתן סיוע לרשות חוץ, יהיו חוקר, מפקח או עובד מדינה שהוסמך לכך לפי סעיף 33, רשאים להשתמש בסמכויות לפי סעיפים 34 עד 37, שהוסמכו לבצען, לפי העניין, ובסמכויות לפי סעיף 43 לפקודת מעצר וחיפוש וסעיף 3 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007 (בסעיף זה – חוק נתוני תקשורת) בשינויים המחויבים ובלבד שנושא בקשת הסיוע עשוי להיות נתון לחקירה כעבירה פלילית לפי חוק זה, ואם הנושא של הבקשה לסיוע הוא פיקוח – תיעשה הפעלת הסמכויות לפי סעיף 34 בלבד.

(ד) קבע ראש הרשות להגנת הפרטיות כי על הבקשה לסיוע יחולו הוראות סעיף זה, ומידע אישי או מסמך שמבוקשים בבקשה לסיוע מצויים בידי הרשות להגנת הפרטיות, רשאי מי שראש הרשות להגנת הפרטיות הסמיכו לכך בכתב להעביר לרשות החוץ את המידע האישי או המסמך או העתק מאושר או העתק צילומי מאושר שלו.

(ה) לא יועבר מידע אישי או מסמך בהתאם לסעיף קטן (ד) לעיל אלא אם שוכנע ראש הרשות להגנת הפרטיות כי הוא ישמש אך ורק למטרה שלשמה נמסר.

(ו) הועבר מידע אישי או מסמך לפי סעיף קטן (ד) לעיל, רשאי ראש הרשות להגנת הפרטיות לאשר לרשות חוץ להעביר מידע אישי או מסמך לשם ביצוע ואכיפה של דיני הגנת הפרטיות ופיקוח על ביצועם, לרשות ממשלתית אחרת או לרשות שהוקמה מכוח הסכם בין מדינות ורשאי הוא להתנות העברת מידע אישי או מסמך כאמור בתנאים.

(ז) ראש הרשות להגנת הפרטיות רשאי להורות שפעולה לפי סעיף זה לא תיעשה לפי בקשת רשות חוץ, אשר מנועה או נמנעה מביצוע פעולה דומה לבקשת הרשות להגנת הפרטיות.

(ח) על אף האמור בכל דין, מידע אישי, ידיעה או מסמך שנמסרו לרשות על ידי רשות חוץ או שהתקבלו, שנאספו או שנוצרו בעקבות בקשה לסיוע או בקשה לקבלת מידע אישי, ידיעה או מסמך שהוגשה לרשות להגנת הפרטיות על ידי רשות חוץ, לרבות הבקשה עצמה, רשאית הרשות להגנת הפרטיות שלא להעבירם לצד שלישי; אין בהוראה זו כדי למנוע גילוי לפי דרישת היועץ המשפטי לממשלה לצורך משפט פלילי או לפי דרישת בית המשפט.

דברי הסבר

סעיף 31: שואב השראה מסעיפים 50 ל-GDPR ו-54א1–54א9 לחוק ניירות ערך התשכ"ח–1968.

פגיעה בזכות לפרטיות, בעיקר פרטיות במידע, יכולה להיות חוצת גבולות (למשל, בפרשת **קיימברידג' אנליטיקה** נחשף מידע אישי על כ-47 אלף משתמשי פייסבוק מישראל[15]). שיתוף פעולה בין רשויות הגנת פרטיות ברחבי העולם הוא אפוא כורח המציאות – כדי לאפשר אכיפה יעילה של דיני הגנת הפרטיות. הצורך בשיתוף מידע אישי בין רשויות מדינתיות קיבל הכרה בינלאומית בהחלטה מספטמבר 2017,[16] לֶקח מהחקירה המשותפת שניהלו רשויות הגנת הפרטיות של קנדה, של אוסטרליה ושל ארצות הברית בעניין חשיפת מידע אישי ומידע רגיש על משתמשי האתר "אשלי מדיסון".[17]

32. הוועדה המייעצת

(א) שר המשפטים ימנה ועדה מייעצת שתפקידה:

(1) לייעץ לראש הרשות להגנת הפרטיות, לפי דרישתו, בכל עניין הנוגע להגנת הפרטיות, וכן לייעץ לו בהכנת הדין וחשבון השנתי כאמור בסעיף 74 ובהכנת תוכנית העבודה של הרשות;

(2) לדון בנושאים נוספים בנוגע ליישום הוראות חוק זה שיש לדעתה חשיבות בעיסוק הרשות להגנת הפרטיות בהם.

(ב) הוועדה המייעצת תהיה בת חמישה חברים והם:

(1) עובד משרד המשפטים בדרגה ____;

(2) עובד משרד הכלכלה והתעשייה בדרגה שאינה פחותה מדרגת סגן מנהל כללי;

(3) חבר הסגל האקדמי של מוסד מוכר להשכלה גבוהה כמשמעותו בחוק המועצה להשכלה גבוהה, התשי"ח-1958;

(4) שני נציגי ציבור מקרב מוסד, מכון או ארגון, אשר אחד מהם לפחות יהיה נציג מתחום תעשיית הטכנולוגיה והשני יעסוק באחד מהתחומים האלה: צרכנות, משפט, כלכלה או מדיניות ציבורית;

(ג) שר המשפטים ימנה את אחד מחברי הוועדה המייעצת להיות יושב ראש הוועדה.

(ד) חברי הוועדה המייעצת ימונו לתקופה של שלוש שנים וניתן לחזור למנותם, ובלבד שלא יכהנו שלוש תקופות רצופות.

33. הסמכת חוקר או מפקח

(א) ~~10(ה) הרשם יעמוד בראש יחידת הפיקוח, הוא ימנה את המפקחים לצורך ביצוע הפיקוח לפי חוק זה;~~ראש הרשות להגנת הפרטיות רשאי להסמיך חוקר או מפקח, מבין עובדי המדינה, לביצוע סמכויות לפי חוק זה, כולן או חלקן, אם התקיימו בו כל אלה:

(1) משטרת ישראל הודיעה, בתוך שלושה חודשים מפנייתו של ראש הרשות להגנת הפרטיות אליה, כי היא אינה מתנגדת להסמכתו מטעמים של ביטחון הציבור, לרבות בשל עברו הפלילי;

(2) ~~לא יתמנה למפקח אלא מי~~ הוא שקיבל הכשרה ~~מקצועית~~ מתאימה בתחום ~~המחשוב ואבטחת מידע והפעלת סמכויות לפי חוק זה, ומשטרת ישראל לא הביעה התנגדות למינויו מטעמים של שמירה על בטחון הציבור.~~הסמכויות שיהיו נתונות לו לפי חוק זה, כפי שהורה שר המשפטים בהסכמת השר לביטחון הפנים, ולעניין הפעלת סמכויות חדירה לחומר מחשב או העתקתו כאמור בסעיפים 35-36 - הוא בעל תפקיד המיומן לביצוע פעולות כאמור;

(3) הוא עומד בתנאי כשירות נוספים, ככל שהורה שר המשפטים בהסכמת השר לביטחון הפנים.

(ב) הסמכתו של מפקח או חוקר לפי סעיף זה תהיה בתעודה החתומה בידי ראש הרשות להגנת הפרטיות, שמעידה על תפקידו כמפקח או כחוקר ועל סמכויותיו לפי חוק זה.

סימן ב': סמכויות פיקוח

34. סמכויות מפקח

(א) ~~(ה1)לצורך ביצוע תפקידיו~~לשם פיקוח על ביצוע ההוראות לפי פרקים ב', ד', ו-ו', רשאי ראש הרשות להגנת הפרטיות או מפקח שהוסמך על ידו –

(1) לדרוש מכל אדם למסור לו את שמו ומענו ולהציג לפניו תעודת זהות או תעודה רשמית אחרת המזהה אותו;

(2) ~~(1)~~ לדרוש מכל אדם הנוגע בדבר למסור לו כל ידיעה~~ות~~ ומסמך~~כים המתייחסים למאגר המידע~~;

(3) לדרוש מכל אדם הנוגע בדבר להציג לפניו או למסור לו עותק מחומר מחשב הכולל נתוני מערכת או מידע אישי מדגמי; מידע אישי מידגמי לפי סעיף זה לא ייאסף בהיקף העולה על הנדרש למימוש תכליות הפיקוח.

(4) ~~(2)~~ להיכנס למקום שיש לו יסוד סביר להניח ~~כי מופעל בו מאגר מידע, לערוך בו חיפוש ולתפוס חפץ, אם שוכנע כי הדבר דרוש לשם הבטחת ביצוע חוק זה וכדי למנוע עבירה על הוראותיו; על חפץ שנתפס לפי סעיף זה יחולו הוראות פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], תשכ"ט –1969, סדרי כניסה למיתקן צבאי או למיתקן של רשות בטחון כמשמעותה בסעיף 19(ג) ייקבעו על ידי שר המשפטים בהתייעצות עם השר הממונה על רשות הבטחון, לפי העניין; בפסקה זו "חפץ" – לרבות חומר מחשב, ופלט כהגדרתם בחוק המחשבים, תשנ"ה – 1995~~; שנעשה בו עיבוד של מידע אישי, ובלבד ש~~(3) על אף הוראות פסקה (2),~~ לא ייכנס למקום המשמש למגורים ~~בלבד,~~ אלא לפי צו ~~מאת שופט~~ של בית משפט;

(ב) הממונה ימחק מידע אישי מדגמי, שנמסר או שנאסף לפי סעיף זה, כאשר אינו נדרש עוד באופן סביר להמשך הליכי הפיקוח, ולכל היותר בתוך שלוש שנים ממועד מסירתו או איסופו, אלא אם כן המידע האישי המידגמי דרוש לצורך הליכים לפי פרק ג', סימנים ג' או ד'.

דברי הסבר

סעיף 32: שואב השראה מסעיף 22א לחוק הגנת הצרכן, התשמ"ח–1981. הוא בא במקום ההתייחסות ה"כחושה" בסעיף 10א לחוק הגנת הפרטיות הקיים, שהתמקד רק בחובתה הסטטוטורית של המועצה הציבורית להגנת הפרטיות להעיר את הערותיה על דוח רשם מאגרי המידע. מטרת הסעיף לעגן בחוק את הקמת הוועדה המייעצת ולקבוע את סמכויותיה במפורש, מתוך הכרה בסמכותה לדון גם בנושאים נוספים על אלו שידרוש ראש הרשות להגנת הפרטיות, אם לדעתה יש חשיבות לדיון ברשות להגנת הפרטיות ולעיסוק שלה בנושאים אלו. המטרה היא למנוע את האפשרות שראש הרשות להגנת הפרטיות ירוקן את תפקידה של הוועדה המייעצת מתוכן.

סעיף 33: מבוסס על סעיפים 10(ה) להצ"ח תיקון מס' 13 ו-20א(ג) לחוק הגנת הצרכן.

מטרת הסעיף לקבוע שראש הרשות להגנת הפרטיות יהיה רשאי להסמיך חוקר או מפקח, מקרב עובדי המדינה, לביצוע סמכויות האכיפה והפיקוח לפי הצעת החוק, וכן לקבוע תנאי הסמכה הולמים למפקח ולחוקר, בדגש על הכשרה ראויה לצורך הפעלת סמכות חדירה לחומר מחשב. הסעיף אינו מגביל את תוקף הכשרתו של חוקר או מפקח, בדומה לסעיף 20א(ג) בחוק הגנת הצרכן, אלא מסתפק בהסכמת שר המשפטים לקבוע בתקנות תנאי כשירות נוספים, למשל הכשרות עיתיות להבטחת הכשירות של המפקח לביצוע תפקידו, בעיקר לנוכח השינויים הטכנולוגיים התדירים בתחום העיבוד של מידע אישי.

סעיף 34: מבוסס על סעיפים 10(ה1) לחוק הגנת הפרטיות הקיים ו-23י' להצ"ח תיקון מס' 13.

סימן ג': סמכויות בבירור מינהלי

35. צו לחיפוש ולחדירה לחומר מחשב

היה לראש הרשות להגנת הפרטיות או לעובד המדינה שהוא הסמיך לכך בהודעה ברשומות, הכשיר לכהן כשופט של בית משפט מחוזי, יסוד סביר להניח כי בוצעה הפרה של הוראה מההוראות לפי חוק זה כאמור בסעיף 38, רשאי הוא לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב לפי סעיפים 23 עד 24 לפקודת המעצר והחיפוש, ולבצעם בעצמו או באמצעות מפקח.

36. אופן ביצוע חדירה לחומר מחשב

על ביצוע חיפוש, תפיסת חפץ וחדירה לחומר מחשב או העתקתו לפי סימן זה, יחולו הוראות סעיפים 23א, 24(א)(1) ו (ב), 26 עד 28, 31 ו – 45 וכן הוראות הפרק הרביעי, לפקודת המעצר והחיפוש, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות למפקח והסמכויות הנתונות לקצין יהיו נתונות לראש הרשות להגנת הפרטיות ולעובד המדינה שהוא הסמיך כאמור בסעיף 33.

37. סמכויות אכיפה, חקירה, עיכוב ותפיסה

(א) היה לראש הרשות להגנת הפרטיות או לחוקר יסוד סביר לחשד שנעברה עבירה לפי פרקים ב' או ו', או התעורר חשד כי אגב חקירה בעבירה כאמור, נעברה עבירה לפי סעיפים 242, 244, 245, 246, ו-249 לחוק העונשין, התשל"ז-1977 (להלן – חוק העונשין) יהיו נתונות לראש הרשות להגנת הפרטיות ולחוקר כל סמכויות הפיקוח לפי סימן ב', וכן רשאים הם -

(1) לחקור כל אדם הקשור לעבירה כאמור או שעשויות להיות לו ידיעות הנוגעות לעבירה כאמור; על חקירה לפי פסקה זו יחולו הוראות סעיפים 2 ו – 3 לפקודת הפרוצדורה הפלילית (עדות), והוראות חוק סדר הדין הפלילי (חקירת חשודים), התשס"ב–2002, בשינויים המחויבים;

(2) לתפוס כל חפץ שיש לו יסוד סביר להניח שהוא חפץ הקשור לעבירה כאמור;

(3) לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב לפי סעיפים 23 עד 24 לפקודת המעצר והחיפוש, ולבצעו.

(ב) על ביצוע חיפוש, תפיסת חפץ וחדירה לחומר מחשב או העתקתו לפי סעיף זה יחולו סעיפים 23א, 24(א)(1) ו – (ב), 26 עד 28, 31 ו-45 וכן הוראות הפרק הרביעי לפקודת המעצר והחיפוש, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין יהיו נתונות לראש הרשות להגנת הפרטיות ולעובד המדינה שהוא הסמיך כאמור בסעיף 33.

(ג) היה לראש הרשות להגנת הפרטיות או לחוקר יסוד סביר לחשד שאדם עבר עבירה לפי פרקים ב' או ו', או התעורר חשד כי אגב חקירה בעבירה כאמור, נעברה עבירה לפי סעיפים 242, 244, 245, 246, ו-249 לחוק העונשין, רשאי הוא לעכבו כדי לברר את זהותו ומענו או כדי לחוקרו במקום הימצאו; היה הזיהוי בלתי מספיק או שלא ניתן לחקור את אותו אדם במקום הימצאו, רשאי ראש הרשות להגנת הפרטיות או החוקר לדרוש מאותו אדם להתלוות אליו למשרדי ראש הרשות להגנת הפרטיות או לזמנו למשרדי הרשות להגנת הפרטיות למועד אחר שיקבע. מי שזומן למשרדי ראש הרשות להגנת הפרטיות יתייצב במועד שזומן אליו; על עיכוב לפי סעיף קטן זה יחולו הוראות סעיפים 66, 67 ו-72 עד 74 לחוק המעצרים, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין הממונה יהיו נתונות לראש הרשות להגנת הפרטיות.

(ד) היה לראש הרשות להגנת הפרטיות או לחוקר יסוד סביר לחשד שנעברה עבירה לפי פרקים ב' או ו', או התעורר חשד כי אגב חקירה בעבירה כאמור, נעברה עבירה לפי סעיפים 242, 244, 245, 246, ו-249 לחוק העונשין, רשאי הוא לעכב אדם שיכול למסור

לו מידע הנוגע לאותה עבירה, כדי לברר את זהותו ומענו וכדי לחקור אותו במקום הימצאו; וכן רשאי הוא לזמן אותו למשרדי ראש הרשות להגנת הפרטיות למועד סביר אחר שיקבע לצורך ביצוע אותן פעולות; מי שזומן למשרדי ראש הרשות להגנת הפרטיות, יתייצב במועד שזומן אליו; על עיכוב לפי סעיף קטן זה יחולו הוראות סעיפים 68 ו-72 עד 74 לחוק המעצרים, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין הממונה יהיו נתונות לראש הרשות להגנת הפרטיות.

(ה) לעניין סעיפים קטנים (ג) ו – (ד) יראו את משרדי ראש הרשות להגנת הפרטיות שראש הרשות הכריז עליהם בהודעה ברשומות, כ"תחנת משטרה" לעניין הוראות חוק המעצרים.

פרק ד: אמצעי אכיפה מינהליים

סימן א': עיצום כספי

38. עיצום כספי

(א) הפר אדם הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי ראש הרשות להגנת הפרטיות להטיל עליו עיצום כספי בסכום של ___, ואם המפר הוא תאגיד – בסכום של ___:

(1) עיבד מידע אישי מבלי שמילא את חובת מתן הודעה, בניגוד להוראות סעיף 9;

(2) הפר את זכותו של נושא מידע לחזור בו מהסכמתו, בניגוד להוראות סעיף 10;

(3) הפר את זכות מזכויות נושא מידע לעיין במידע אישי על אודותיו, לקבל הסבר, לתקן, לנייד או למחוק מידע אישי על אודותיו, בניגוד להוראת סעיפים 11; 12, 13, 14 ו-15 בהתאמה; או בניגוד להוראות שנקבעו לעניין זה לפי סעיף 16;

(4) סירב לבקשת נושא מידע למימוש זכות מזכויות נושא המידע כאמור בסעיפים 11(ה) עד (ח), 13(ד), 14(ו) או 15(ג), ולא הודיע על כך לנושא המידע כנדרש לפי סעיף 16(ד).

(ב) הפר אדם הוראה מההוראות חוק זה, כמפורט להלן, רשאי ראש הרשות להגנת הפרטיות להטיל עליו עיצום כספי בסכום של ___, ואם המפר הוא תאגיד – בסכום של___:

(1) עיבד מידע אישי שלא למטרה לשמה נמסר, בניגוד להוראות סעיף 7;

(2) לא תיכנן, עיצב או הפעיל את מערכות עיבוד המידע האישי שיבטיחו את התאמתן להוראות חוק זה, בניגוד להוראות סעיף 19;

(3) לא הכין תסקיר השפעה על הפרטיות, בניגוד להוראות סעיף 20;

(4) לא נקט אמצעים סבירים לאבטחת מידע אישי, בניגוד להוראות סעיף 21;

(5) לא תיעד או דיווח על אירועי אבטחה, בניגוד להוראות סעיף 22;

(6) לא מינה ממונה הגנת פרטיות במידע או הסמיכו לבצע את תפקידיו, בניגוד להוראות סעיף 23;

39. הפרה בנסיבות מחמירות

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי הפר אדם הוראה מההוראות לפי חוק זה המפורטות בסעיף 38, בנסיבות מחמירות, רשאי ראש הרשות להגנת הפרטיות להטיל עליו עיצום כספי לפי הוראות פרק זה, ששיעורו פי אחד וחצי מסכום העיצום הכספי שניתן להטיל בשל אותה הפרה לפי סעיף 38.

(ב) בסעיף זה, "נסיבות מחמירות" – הפרה הנוגעת ל 100,000 נושאי מידע לפחות, או הפרה הנוגעת למידע רגיש.

דברי הסבר

__סעיפים 35 ו-36:__ מבוססים על סעיפים 23יא ו– 23יב להצ"ח תיקון מס' 13.

__סעיף 37:__ מבוסס על סעיף 23יג להצ"ח תיקון מס' 13, אך בהשראת סעיף 46 לחוק ההגבלים העסקיים, התשמ"ח–1988, וסעיף 56 לחוק ניירות ערך, התשכ"ח–1968, סמכות האכיפה הנתונה לפי הסעיף לראש הרשות להגנת הפרטיות או לחוקר הורחבה גם לביצוע חקירה בעבירות נלוות לעבירות לפי חוק זה (סעיף 242 (השמדת ראיה), 244 (שיבוש מהלכי משפט), 245 (הדחה בחקירה), 246 (הדחה בעדות), ו-249 (הטרדת עד) לחוק העונשין התשל"ז-1977). הרחבה זו של סמכות האכיפה נועדה למנוע מצב שלא מנוהלת חקירה במכלול השלם של העבירות בנימוק שהעבירה הנלווית אינה חמורה מספיק ולכן אינה מצדיקה חקירת משטרה נפרדת. הסעיף מגדיר אפוא את הרשות להגנת הפרטיות כרשות חקירה עצמאית, בדומה לרשות לניירות ערך ולרשות להגבלים העסקיים, ואף מאפשר לחוקריה לחקור חשדות לשיבוש הליכי חקירה מסוגים שונים כאשר מתעורר חשד שנעשו פעולות לשיבושה. הוראה זו עולה בקנה אחד עם מגמת המחוקק להקשות על שיבוש הליכי משפט.

__סעיף 38:__ מבוסס על הוראת סעיף 23יט להצ"ח תיקון מס' 13 ושואב השראה מהוראות סימן א בפרק ה1 לחוק הגנת הצרכן, התשמ"א–1981, המעגן את המודל העכשווי העדכני ביותר לסמכות אכיפה מינהלית בהקשרים של הגנת הצרכן שהם בעלי דמיון רב מבחינת אופי ומספר ההפרות האפשריות לפגיעות אפשריות בזכות לפרטיות. מודל זה בא במקום המודל המסורבל המוצע בסעיף 23יט להצ"ח תיקון מס' 13.

הסעיף מונה את ההפרות שבגינן יוטל עיצום כספי על פי הוראות הדין המהותי בהצעת החוק. לפיכך הוא אינו מאמץ את סעיפים 23טז(ב), 23יט(ד)(2), 23יט(ג)(7), ו-יט(ג)(9), (10), (11), (12) להצ"ח תיקון מס' 13 העוסקים בהפרת חובות הנוגעות לרישום מאגרי מידע ולדיוור ישיר.

בדומה להבחנה המוצעת גם היום בהצ"ח תיקון מס' 13, סעיף 38 מבחין בין הפרות הקשורות לכיבוד זכויותיו של נושא המידע, המנויות בס"ק (א), לבין הפרות הקשורות לחובות של בעל שליטה במידע ושל מעבד ולדרך עיבוד המידע האישי, לתנאים המקדימים לעיבודו ולהתוויה של אופן עיבוד המידע האישי, המנויים בס"ק (ב).

__סעיף 39:__ מבוסס על סעיף 22ד לחוק הגנת הצרכן ומאפשר הטלת עיצום כספי בסכום גבוה מן הסכום הקבוע להפרה כאשר מדובר בנסיבות מחמירות. בדרך זו אפשר להקשיח את הענישה המינהלית כאשר מדובר במספר גדול של נושאי מידע שעלולים להיפגע או כאשר מדובר במידע רגיש – בלי לאמץ את ההסדר המסורבל המוצע בהצ"ח תיקון מס' 13 באשר לסכום הבסיסי ולכפולותיו.

40. הודעה על כוונת חיוב

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי הפר אדם הוראה מההוראות לפי חוק זה, כאמור בסעיף 38 (בפרק זה – המפר), ובכוונתו להטיל עליו עיצום כספי לפי אותו סעיף או לפי סעיף 39, ימסור למפר הודעה על הכוונה להטיל עליו עיצום כספי (בפרק זה – הודעה על כוונת חיוב).

(ב) בהודעה על כוונת חיוב יציין ראש הרשות להגנת הפרטיות, בין השאר, את אלה:

(1) המעשה או המחדל (בפרק זה – המעשה), המהווה את ההפרה, ומועד ביצועו;

(2) סכום העיצום הכספי והתקופה לתשלומו;

(3) זכותו של המפר לטעון את טענותיו לפני ראש הרשות להגנת הפרטיות לפי הוראות סעיף 41;

(4) שיעור התוספת על העיצום הכספי בהפרה נמשכת או בהפרה חוזרת לפי הוראות סעיף 43.

41. זכות טיעון

(א) מפר שנמסרה לו הודעה על כוונת חיוב לפי הוראות סעיף 40 רשאי לטעון את טענותיו, בכתב או בעל פה, לעניין הכוונה להטיל עליו עיצום כספי ולעניין סכומו, בתוך 45 ימים ממועד מסירת ההודעה.

(ב) ראש הרשות להגנת הפרטיות רשאי, לבקשת המפר, להאריך את התקופה האמורה בסעיף קטן (א) בתקופה נוספת שלא תעלה על 45 ימים.

42. החלטת ראש הרשות להגנת הפרטיות ודרישת תשלום

(א) ראש הרשות להגנת הפרטיות יחליט, לאחר ששקל את הטענות שנטענו לפי סעיף 41, אם להטיל על המפר עיצום כספי, ורשאי הוא להפחית את סכום העיצום הכספי לפי הוראות סעיף 45.

(ב) החליט ראש הרשות לפי סעיף קטן (א) –

(1) להטיל על המפר עיצום כספי – ימסור לו דרישה, בכתב, לשלם את העיצום הכספי (בפרק זה – דרישת תשלום), שבה יציין, בין השאר, את סכום העיצום הכספי המעודכן ואת התקופה לתשלומו כאמור בסעיף 46;

(2) שלא להטיל על המפר עיצום כספי – ימסור לו הודעה על כך, בכתב.

(ג) בדרישת התשלום או בהודעה, לפי סעיף קטן (ב), יפרט ראש הרשות להגנת הפרטות את נימוקי החלטתו.

(ד) לא טען המפר את טענותיו לפי הוראות סעיף 41 בתוך התקופה האמורה באותו סעיף, יראו את ההודעה על כוונת חיוב, בתום אותה תקופה, כדרישת תשלום שנמסרה למפר במועד האמור.

43. הפרה נמשכת והפרה חוזרת

(א) בהפרה נמשכת, יווסף על העיצום הכספי הקבוע לאותה הפרה, החלק החמישים שלו לכל יום שבו נמשכת ההפרה; לעניין זה, "הפרה נמשכת" – הפרת הוראה מההוראות לפי חוק זה, כאמור בסעיף 38, לאחר שנמסרה למפר דרישת תשלום בשל הפרת אותה הוראה או לאחר שנמסרה למפר התראה מינהלית כמשמעותה בסעיף 49, בשל הפרת אותה הוראה וההתראה לא בוטלה כאמור בסעיף 50.

(ב) בהפרה חוזרת יווסף על העיצום הכספי הקבוע לאותה הפרה, סכום השווה לעיצום הכספי כאמור; לעניין זה, "הפרה חוזרת" – הפרת הוראה מההוראות לפי חוק זה, כאמור בסעיף 38(א), בתוך שנתיים מהפרה קודמת של אותה הוראה שבשלה הוטל על המפר עיצום כספי או שבשלה הורשע, ולעניין הפרות לפי סעיף 38(ב) – בתוך תשעה חודשים מהפרה קודמת של הוראות אלה.

44. סכומים מופחתים

(א) ראש הרשות להגנת הפרטיות אינו רשאי להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים בסימן זה, אלא לפי הוראות סעיף קטן (ב).

(ב) שר המשפטים רשאי לקבוע מקרים, נסיבות ושיקולים שבשלהם יהיה ניתן להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים בסימן זה, ובשיעורים שיקבע.

45. סכום מעודכן של הפיצוי הכספי

העיצום הכספי יהיה לפי סכומו המעודכן, לפי סעיף 78, ביום מסירת דרישת התשלום, ולגבי מפר שלא טען את טענותיו לפני ראש הרשות להגנת הפרטיות כאמור בסעיף 42(ד) – ביום מסירת ההודעה על כוונת החיוב; הוגשה עתירה לבית המשפט לעניינים מינהליים או הוגש ערעור על החלטה בעתירה כאמור ועוכב תשלומו של העיצום הכספי בידי ראש הרשות להגנת הפרטיות או בית המשפט – יהיה העיצום הכספי לפי סכומו המעודכן ביום ההחלטה בעתירה או בערעור, לפי העניין.

46. המועד לתשלום העיצום הכספי

המפר ישלם את העיצום הכספי בתוך 45 ימים מיום מסירת דרישת התשלום כאמור בסעיף 42.

47. הפרשי ריבית והצמדה

לא שילם המפר עיצום כספי במועד, ייווספו על העיצום הכספי לתקופת הפיגור, הפרשי הצמדה וריבית כהגדרתם בחוק פסיקת ריבית והצמדה, התשכ"א–1961 (בפרק זה – הפרשי הצמדה וריבית), עד לתשלומו.

48. גבייה

עיצום כספי ייגבה לאוצר המדינה, ועל גבייתו יחול חוק המרכז לגביית קנסות, אגרות והוצאות, התשנ"ה–1995.

דברי הסבר

סעיפים 40-46: מבוססים על סעיפים 23כ-23כה להצ"ח תיקון מס' 13 ומותאמים להוראות סימן א בפרק ה'1 לחוק הגנת הצרכן, התשמ"א–1981, שמציג מתווה מעודכן יותר להטלת עיצום כספי על ידי רשות מינהלית.

סעיפים 46-48: מבוססים על סעיפים 23כו-23כח להצ"ח תיקון מס' 13 ומותאמים להוראות סימן א בפרק ה'1 לחוק הגנת הצרכן, התשמ"א–1981.

סימן ב': התראה מינהלית

49. התראה מינהלית

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 38, והתקיימו נסיבות שקבע ראש הרשות להגנת הפרטיות בנהלים, רשאי הוא, במקום להמציא לו הודעה על כוונת חיוב ולהטיל עליו עיצום כספי, לפי הוראות סימן א', להמציא לו התראה מינהלית לפי הוראות סימן זה.

(ב) בהתראה מינהלית יציין ראש הרשות להגנת הפרטיות מהו המעשה המהווה את ההפרה, יודיע למפר כי עליו להפסיק את ההפרה וכי אם ימשיך בהפרה או יחזור עליה יהיה צפוי לעיצום כספי בשל הפרה נמשכת או הפרה חוזרת, לפי העניין, כאמור בסעיף 43, וכן יציין את זכותו של המפר לבקש את ביטול ההתראה לפי הוראות סעיף 50.

50. בקשה לביטול התראה מינהלית

(א) נמסרה למפר התראה מינהלית כאמור בסעיף 49 רשאי הוא לפנות לראש הרשות להגנת הפרטיות, בכתב או בעל פה, בתוך 45 ימים, בבקשה לבטל את ההתראה בשל כל אחד מטעמים אלה:

(1) המפר לא ביצע את ההפרה;

(2) המעשה שביצע המפר, המפורט בהתראה, אינו מהווה הפרה.

(ב) קיבל ראש הרשות להגנת הפרטיות בקשה לביטול התראה מינהלית, לפי הוראות סעיף קטן (א), רשאי הוא לבטל את ההתראה או לדחות את הבקשה ולהותיר את ההתראה על כנה; החלטת ראש הרשות להגנת הפרטיות תינתן בכתב ותימסר למפר בצירוף נימוקים.

51. הפרה נמשכת והפרה חוזרת לאחר התראה

(א) נמסרה למפר התראה מינהלית לפי הוראות סימן זה והמפר המשיך להפר את ההוראה שבשלה נמסרה לו ההתראה, ימסור לו ראש הרשות להגנת הפרטיות דרישת תשלום בשל הפרה נמשכת כאמור בסעיף 43(א); דרישת תשלום אינה גורעת מזכותו של המפר לטעון כאמור בסעיף 41 לעניין סכום העיצום הכספי ולעניין הימשכות ההפרה, וייחולו הוראות סעיפים 41 ו-42, בשינויים המחויבים.

(ב) נמסרה למפר התראה מינהלית לפי הוראות סימן זה והמפר חזר והפר את ההוראה שבשלה נמסרה לו ההתראה, בתוך שנתיים מיום מסירת ההתראה, יראו את ההפרה הנוספת כאמור כהפרה חוזרת לעניין סעיף 43(ב), וראש הרשות להגנת הפרטיות ימסור למפר הודעה על כוונת חיוב לפי הוראות סעיף 40 בשל ההפרה החוזרת.

דברי הסבר

סעיף 49: מבוסס על הוראת סעיפים 23כט להצ"ח תיקון מס' 13 ו-22יג לחוק הגנת הצרכן, לעניין ההסדר לאישור הנהלים שיקבעו על ידי ראש הרשות להגנת הפרטיות ובאישור היועץ המשפטי לממשלה.

סעיף 50: מבוסס על סעיפים 23ל ו-22יד לחוק הגנת הצרכן.

סעיף 51: מבוסס על סעיפים 23לא להצ"ח תיקון מס' 13 ו-22טו לחוק הגנת הצרכן.

סימן ג': התחייבות להימנע מהפרה

52. התחייבות להימנע מהפרה והפקדת עירבון

(א) היה לראש הרשות להגנת הפרטיות יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 38, והתקיימו נסיבות המנויות בנהלים שקבע ראש הרשות להגנת הפרטיות, רשאי הוא להציע למפר, בהודעה בכתב, להגיש לו כתב התחייבות ועירבון מסוג שייקבע בנהלים, לפי הוראות סימן זה, במקום שיוטל עליו עיצום כספי לפי הוראות סימן א'.

(ב) בכתב ההתחייבות יתחייב המפר להפסיק את הפרת ההוראה כאמור בסעיף קטן (א), ולהימנע מהפרה נוספת של אותה הוראה בתוך תקופה שיקבע ראש הרשות להגנת הפרטיות, שתחילתה ביום מסירת ההודעה כאמור באותו סעיף קטן, ובלבד שהתקופה האמורה לא תעלה על שנתיים (בסימן זה – תקופת ההתחייבות).

(ג) ראש הרשות להגנת הפרטיות רשאי לדרוש כי המפר יכלול בכתב ההתחייבות תנאים נוספים שעליו לעמוד בהם בתקופת ההתחייבות לשם הקטנת הנזק שנגרם מההפרה או מניעת הישנותה.

(ד) נוסף על כתב ההתחייבות יפקיד המפר בידי ראש הרשות להגנת הפרטיות עירבון בסכום העיצום הכספי שראש הרשות להגנת הפרטיות היה רשאי להטיל על המפר בשל אותה הפרה, בהתחשב בקיומן של מקרים, נסיבות ושיקולים שנקבעו לפי סעיף 44.

53. תוצאות הגשת כתב התחייבות ועירבון או אי הגשתם

(א) הגיש המפר לראש הרשות להגנת הפרטיות כתב התחייבות ועירבון לפי סימן זה, בתוך 45 ימים מיום מסירת ההודעה כאמור בסעיף 52, לא יוטל עליו עיצום כספי בשל אותה הפרה.

(ב) לא הגיש המפר לראש הרשות להגנת הפרטיות כתב התחייבות ועירבון בתוך 45 ימים מיום מסירת ההודעה כאמור בסעיף 52, ימציא לו ראש הרשות להגנת הפרטיות הודעה על כוונת חיוב בשל אותה הפרה, לפי סעיף 40.

54. הפרת התחייבות

(א) הגיש המפר כתב התחייבות ועירבון לפי סימן זה והפר תנאי מתנאי ההתחייבות, כמפורט להלן, יחולו הוראות אלה, לפי העניין:

(1) המשיך המפר, במהלך תקופת ההתחייבות, להפר את ההוראה שבשל הפרתה נתן את כתב ההתחייבות – יחלט ראש הרשות להגנת הפרטיות את העירבון וימציא למפר דרישת תשלום בשל ההפרה הנמשכת כאמור בסעיף 43(א);

(2) חזר המפר והפר, במהלך תקופת ההתחייבות, את ההוראה שבשל הפרתה נתן את כתב ההתחייבות – יחלט ראש הרשות להגנת הפרטיות את העירבון ויראו את ההפרה הנוספת כאמור כהפרה חוזרת לעניין סעיף 43(ב); ראש הרשות להגנת הפרטיות ימציא למפר הודעה על כוונת חיוב בשל ההפרה החוזרת;

(3) הפר המפר תנאי מהתנאים הנוספים שנקבעו בכתב ההתחייבות כאמור בסעיף 52 – יודיע ראש הרשות להגנת הפרטיות למפר על כוונתו לחלט את העירבון; המפר רשאי לטעון את טענותיו לעניין זה, בכתב או בעל פה, כפי שיורה ראש הרשות להגנת הפרטיות, בתוך 45 ימים מיום הודעת ראש הרשות להגנת הפרטיות, וראש הרשות להגנת הפרטיות רשאי, לבקשת המפר, להאריך תקופה זו בתקופה נוספת שלא תעלה על 45 ימים.

(ב) לעניין פרק זה, יראו בחילוט העירבון לפי הוראות סעיף זה, כהטלת עיצום כספי על המפר בשל ההפרה שלגביה ניתן העירבון.

(ג) הופר תנאי מתנאי ההתחייבות כאמור בסעיף זה, והפר המפר פעם נוספת את ההוראה שבשל הפרתה נתן את כתב ההתחייבות, לא יאפשר לו ראש הרשות להגנת הפרטיות להגיש כתב התחייבות נוסף לפי הוראות סימן זה, בשל אותה הפרה.

55. השבת העירבון

עמד המפר בתנאי כתב ההתחייבות שמסר לפי סימן זה, יוחזר לו, בתום תקופת ההתחייבות, העירבון שהפקיד; העירבון, למעט אם היה ערבות בנקאית, יוחזר בתוספת הפרשי הצמדה וריבית מיום הפקדתו עד יום החזרתו.

סימן ד': הוראות כלליות

56. עיצום כספי בשל הפרה לפי חוק זה ולפי חוק אחר

על מעשה אחד המהווה הפרה של הוראה מהוראות לפי חוק זה המנויות בסעיף 38 ושל הוראה מההוראות לפי חוק אחר, לא יוטל יותר מעיצום כספי אחד.

57. פרסום לעניין הטלת עיצום כספי

(א) הטיל ראש הרשות להגנת הפרטיות עיצום כספי לפי פרק זה, יפרסם באתר האינטרנט של הרשות להגנת הפרטיות את הפרטים שלהלן, באופן שיבטיח שקיפות לגבי הפעלת שיקול דעתו בקבלת ההחלטה להטיל עיצום כספי:

(1) דבר הטלת העיצום הכספי;

(2) מהות ההפרה שבשלה הוטל העיצום הכספי ונסיבות ההפרה, לרבות מספר נושאי המידע שמידע אישי על אודותיהם נחשף או עלול להיחשף עקב ההפרה;

(3) סכום העיצום הכספי שהוטל;

(4) אם הופחת העיצום הכספי – הנסיבות שבשלהן הופחת סכום העיצום ושיעורי ההפחתה;

(5) פרטים על אודות המפר, הנוגעים לעניין;

(6) שמו של המפר – ככל שהמפר הוא תאגיד.

(ב) הוגשה עתירה לבית המשפט לעניינים מינהליים או הוגש ערעור על החלטה בעתירה כאמור, יפרסם ראש הרשות להגנת הפרטיות, בפרסום לפי סעיף קטן (א), גם את דבר הגשת העתירה או הערעור ואת תוצאותיהם.

(ג) על אף הוראות סעיף קטן (א)(6), רשאי ראש הרשות להגנת הפרטיות לפרסם את שמו של מפר שהוא יחיד, אם סבר שהדבר נחוץ לצורך אזהרת הציבור.

(ד) פרסום לפי סעיף זה בעניין עיצום כספי שהוטל על תאגיד יהיה לתקופה של ארבע שנים, ובעניין עיצום כספי שהוטל על יחיד – לתקופה של שנתיים.

58. שמירת אחריות פלילית

(א) תשלום עיצום כספי, המצאת התראה מינהלית או מתן כתב התחייבות ועירבון, לפי פרק זה, לא יגרעו מאחריותו הפלילית של אדם בשל הפרת הוראה מההוראות לפי חוק זה המפורטות בסעיף 38, שהיא עבירה על חוק זה.

(ב) על אף האמור בסעיף קטן (א), נמסרה למפר הודעה על כוונת חיוב, או התראה מינהלית או הגיש המפר כתב התחייבות ועירבון, בשל הפרה כאמור באותו סעיף קטן, לא יוגש נגדו כתב אישום בשל אותו מעשה, אלא אם כן התגלו עובדות או ראיות חדשות, המצדיקות זאת.

(ג) שילם המפר עיצום כספי או הפקיד עירבון והוגש נגדו כתב אישום בנסיבות האמורות בסעיף קטן (ב), יוחזר לו הסכום ששילם או העירבון; הסכום ששילם המפר כאמור או עירבון, למעט ערבות בנקאית, יוחזר בתוספת הפרשי הצמדה וריבית מיום תשלומו או הפקדתו עד יום החזרתו.

(ד) הוגש נגד אדם כתב אישום בשל הפרה המהווה עבירה כאמור בסעיף קטן (א), לא ינקוט נגדו ראש הרשות להגנת הפרטיות הליכים לפי פרק זה בשל אותה הפרה.

59. אישור נהלים ופרסומם

נהלי ראש הרשות להגנת הפרטיות לפי סעיפים 49 ו-52 טעונים אישור היועץ המשפטי לממשלה או משנה ליועץ המשפטי שהוא הסמיך לכך, והם יפורסמו באתר האינטרנט של הרשות להגנת הפרטיות.

60. אצילת סמכויות

ראש הרשות להגנת הפרטיות רשאי לאצול את סמכויותיו לפי פרק זה, למעט קביעת נהלים לפי סעיפים 49(א) ו-52(א), לסגנו או לעובד הרשות להגנת הפרטיות האחראי לנושא העיצומים הכספיים.

דברי הסבר

סעיף 52: מבוסס על סעיפים 23לב ו-23לג להצ"ח תיקון מס' 13 ו-22טז, 22יז לחוק הגנת הצרכן.

סעיפים 53-56: מבוססים על סעיפים 23לד–23לז בהצ"ח תיקון מס' 13 ו-22יז–22יט, ו-22כג לחוק הגנת הצרכן.

סעיף 23לח להצ"ח תיקון מס' 13 העוסק בעיכוב הביצוע של החלטת ראש הרשות להגנת הפרטיות לעניין הטלת עיצום כספי והחזר עיצום כספי ששולם או עירבון שהופקד במקרה של ערעור על החלטת ראש הרשות להגנת הפרטיות להפעיל את סמכותו המינהלית לפי פרק זה לא אומץ בהצעת החוק, שכן הנושא צריך להיות מטופל במסגרת הדינים הכלליים, ובמקרה שלנו – חוק בתי המשפט לעניינים מינהלים, התש"ס–2000.

סעיף 57: מבוסס על סעיפים 23לט להצ"ח תיקון מס' 13 ו-22כא לחוק הגנת הצרכן.

בס"ק (א) הועדף ההסדר שבסעיף 22כא לחוק הגנת הצרכן. כמו כן נקבע בו שהפרסום יעשה באתר האינטרנט של הרשות להגנת הפרטיות ולא יפורסם באתר האינטרנט של משרד המשפטים או בדרך אחרת על פי החלטת ראש הרשות להגנת הפרטיות.

ס"ק (א)(2) מבהיר שמספר נושאי המידע, שמידע אישי עליהם נחשף או עלול להיחשף עקב ההפרה, הוא מידע שרלוונטי לבחינה של שיקול הדעת של ראש הרשות בהטלת העיצום הכספי, ולכן יש לפרסמו כחלק מנסיבות ההפרה.

סעיף 23לט(ו) להצ"ח תיקון מס' 13 לא אומץ בהצעת החוק משום שיש בו משום התערבות יתר ופגיעה בגמישות סמכויות העזר הנתונות בידי השר האחראי או ראש הרשות להגנת הפרטיות. בחוק ההגבלים העסקיים ובחוק ניירות ערך, למשל, אין הוראה דומה לדרכי פרסום נוספות של דבר הטלת עיצום כספי.

ס"ק (ד) מגביל את פרסום דבר הטלת עיצום כספי לתקופה של 4 שנים כאשר העיצום הכספי הוטל על תאגיד, ולשנתיים כאשר העיצום הכספי הוטל על אדם יחיד. הסעיף מחייב בכך את ראש הרשות להגנת הפרטיות למחוק את הפרסום מאתר האינטרנט בתום התקופה האמורה.

סעיף 58: מבוסס על סעיפים 23מ להצ"ח תיקון מס' 13 ו-22כב לחוק הגנת הצרכן. במקרים של אי התאמה הועדף הנוסח הקבוע בחוק הגנת הצרכן מתוך הנחה שהוא העדכני ביותר. הסעיף משקף את הצורך הממשי באכיפה פלילית לצד זו המינהלית. המטרה היא לצמצם את מספר ההפרות ה"משתלמות כלכלית" באמצעות ה"שוט" שלא האחריות הפלילית. עם זאת, כדי להפיג את חוסר הוודאות הנלווה לחשש מסיכון כפול, כלומר ממצב בו המפר חשוף לאכיפה מינהלית ואינו זוכה לסופיות הדיון כי עדיין חשוף לסנקציה פלילית, יש לקבוע בנהלים קריטריונים ברורים לאכיפה פלילית ואכיפה מינהלית.

סעיף 59: מבוסס על סעיף 22כד לחוק הגנת הצרכן ומטרתו ליצור סעיף סל לאישור הנהלים שקובע ראש הרשות להגנת הפרטיות כחלופה לאיזכור הצורך באישור בכל סעיף חוק רלוונטי כפי שנעשה בהצ"ח תיקון מס' 13 בסעיפים 23כט(א) ו-23לב.

סעיף 60: מבוסס על סעיף 22כה לחוק הגנת הצרכן.

פרק ~~ד~~ה: מסירת מידע או ידיעות מאת גופים ציבוריים

~~23. הגדרות בפרק זה –~~
~~"גוף ציבורי" –~~ ההגדרה הועברה לסעיף 2 המוצע.

הנושא מצריך מחקר נפרד, שאינו בליבת עבודתנו הנוכחית לגיבוש הצעה לחוק הגנת פרטיות חדש ומעודכן.

23א. תחולה על ידיעות

הוראות פרק זה יחולו על ידיעות על ענייניו הפרטיים של אדם, אף שאינן בגדר מידע, כשם שהן חלות על מידע.

23ב. איסור על מסירת מידע

(א) מסירת מידע מאת גוף ציבורי אסורה, זולת אם המידע פורסם לרבים על פי סמכות כדין, או הועמד לעיון הרבים על פי סמכות כדין, או שהאדם אשר המידע מתייחס אליו נתן הסכמתו למסירה.

(ב) אין בהוראות סעיף זה כדי למנוע מרשות בטחון כמשמעותה בסעיף 19 לקבל או למסור מידע לשם מילוי תפקידה, ובלבד שהמסירה או הקבלה לא נאסרה בחיקוק.

23ג. סייג לאיסור

מסירת המידע מותרת, על אף האמור בסעיף 23ב, אם לא נאסרה בחיקוק או בעקרונות של אתיקה מקצועית –

(1) בין גופים ציבוריים, אם נתקיים אחד מאלה:

(א) מסירת המידע היא במסגרת הסמכויות או התפקידים של מוסר המידע והיא דרושה למטרת ביצוע חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו;

(ב) מסירת המידע היא לגוף ציבורי הרשאי לדרוש אותו מידע על פי דין מכל מקור אחר;

(2) מגוף ציבורי למשרד ממשלתי או למוסד מדינה אחר, או בין משרדים או מוסדות כאמור, אם מסירת המידע דרושה למטרת ביצוע כל חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו;

אולם לא יימסר מידע כאמור שניתן בתנאי שלא יימסר לאחר.

23ד. חובותיו של גוף ציבורי

(א) גוף ציבורי המוסר דרך קבע מידע בהתאם לסעיף 23ג יפרט עובדה זו על כל דרישת מידע בהתאם לחוק.

(ב) גוף ציבורי המוסר מידע בהתאם לסעיף 23ג יקיים רישום של המידע שנמסר.

(ג) גוף ציבורי המקבל דרך קבע מידע בהתאם לסעיף 23ג, והמידע נאגר במאגר מידע, יודיע על כך לרשם ועובדה זו תיכלל בפרטי רשימת מאגרי המידע לפי סעיף 12.

(ד) גוף ציבורי שקיבל מידע בהתאם לסעיף 23ג לא יעשה בו שימוש אלא במסגרת הסמכויות או התפקידים שלו.

(ה) לענין חובת השמירה על סודיות לפי כל דין, מידע שנמסר לגוף ציבורי מכוח חוק זה, כמוהו כמידע שאותו גוף השיג מכל מקור אחר, ובנוסף יחולו על הגוף המקבל גם כל ההוראות החלות על הגוף המוסר.

23ה. מידע עודף

(א) מקום שמידע שמותר למסרו לפי סעיפים 23ב או 23ג מצוי על גבי אותו קובץ עם מידע אחר (להלן - מידע עודף), רשאי הגוף המוסר את המידע למסור לגוף המקבל את המידע המבוקש עם המידע העודף.

(ב) מסירת מידע עודף לפי סעיף קטן (א) מותנית בקביעת נוהלים שיבטיחו מניעת שימוש כלשהו במידע עודף שנתקבל; נוהלים כאמור ייקבעו בתקנות וכל עוד לא נקבעו בתקנות, יקבע הגוף המבקש נוהלים כאמור בכתב, וימציא לגוף המוסר עותק מהם, לפי דרישתו.

23ו. מסירה מותרת אינה פגיעה בפרטיות

מסירת מידע המותרת לפי חוק זה לא תהווה פגיעה בפרטיות ולא יחולו עליה הוראות סעיפים 2 ו-8.

23ז. תקנות לענין מסירת מידע

שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, רשאי להתקין תקנות בדבר סדרי מסירת מידע מאת גופים ציבוריים.

23ח. (בוטל).

פרק ו: עוולה אזרחית ועונשין

61. ~~4.~~ פגיעה בפרטיות – עוולה אזרחית

הפרת הוראה מההוראות לפי סעיפים 4, 9, 11, 13 עד 15, או הוראה שנקבעה לפי סעיף 16 לעניין האופן והתנאים למימוש זכות לפי סעיפים 11, 13, 14 או 15, ~~פגיעה בפרטיות~~ היא עוולה אזרחית, והוראות פקודת הנזיקין [נוסח חדש], יחולו עליה בכפוף להוראות חוק זה.

62. ~~5.~~ פגיעה בפרטיות - עבירה

הפוגע ~~במזיד~~ בפרטיות זולתו, באחת הדרכים האמורות בסעיף 4 ~~2(1), (3) עד (7) ו-(9) עד (11)~~, דינו - מאסר 5 שנים; נעברה העבירה או היתה מכוונת כלפי קשישים, חסרי ישע או קטינים, או כלפי ציבור של נושאי מידע הנתונים במצב של חולשה שכלית, נפשית או גופנית– דינו של עובר העבירה מאסר שבע שנים.

דברי הסבר

סעיף 61: מחליף את סעיף 31ב לחוק הגנת הפרטיות הקיים ומבוסס על סעיף 4 לחוק הגנת הפרטיות הקיים, אך מרחיב אותו לכל פגיעה בפרטיות ולכל פגיעה בזכות מזכויות נושא המידע.

סעיף 62: מבוסס על סעיף 5 לחוק הגנת הפרטיות הקיים וגם בא במקום סעיף 16 לחוק הגנת הפרטיות הקיים.

בנוסף, הסעיף שואב השראה מסעיף 23א לחוק הגנת הצרכן ומחמיר את הענישה כאשר העבירה נעברה כלפי אוכלוסיות חלשות כגון קטינים, קשישים וחסרי ישע, מתוך הבנה שאוכלוסיות אלו, ולא רק קטינים כמוצע בהצ"ח פרטיות קטינים, עלולות להיתקל בקשיים בהתמודדות עם השימוש בשירותים מקוונים.

סעיפים 23מא עד 23מה להצ"ח תיקון מס' 13 לא אומצו בהצעת החוק מאחר שמקצתם מכוסה גם כך בהוראת סעיף 62, מקצתם נוגעים להוראות בדין המהותי שאינן מופיעות בהצעת החוק, כמו, למשל חובת רישום מאגר מידע, ומקצתם רחבים מידי.

63. ~~29א.~~ פיצוי ללא הוכחת נזק

(א) הורשע אדם בעבירה לפי סעיף ~~5~~62, רשאי בית המשפט לחייבו לשלם לנפגע פיצוי שלא יעלה על 50,000 שקלים חדשים, בלא הוכחת נזק; הורשע אדם בעבירה לפי סעיף 62 לעניין קטין, קשיש, חסר ישע או ציבור של נושאי מידע הנתונים במצב של חולשה שכלית, נפשית או גופנית, רשאי בית המשפט לחייב את הפוגע לשלם לנפגע פיצוי שלא יעלה על כפל הסכום האמור, בלא הוכחת נזק. חיוב בפיצוי לפי סעיף קטן זה הוא כפסק דין של אותו בית משפט שניתן בתובענה אזרחית של הזכאי נגד החייב בו.

(ב)

(1) במשפט בשל עוולה אזרחית לפי סעיף ~~4~~61 עקב הפרת הוראת סעיף 4(8), רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על 50,000 שקלים חדשים, בלא הוכחת נזק.

(2) במשפט כאמור בפסקה (1) שבו הוכח כי הפגיעה בפרטיות נעשתה בכוונה לפגוע, רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על כפל הסכום כאמור באותה פסקה, בלא הוכחת נזק.

(3) במשפט כאמור בפסקה (1) שבו הוכח כי הפגיעה בפרטיות נעשתה או היתה מכוונת כלפי קשישים, חסרי ישע או קטינים, או כלפי ציבור של נושאי מידע הנתונים במצב של חולשה שכלית, נפשית או גופנית, רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על כפל הסכום כאמור באותה פסקה, בלא הוכחת נזק.

(ג) לא יקבל אדם פיצוי בלא הוכחת נזק לפי סעיף זה, בשל אותה פגיעה בפרטיות, יותר מפעם אחת.

~~הסכומים האמורים בסעיף זה יעודכנו ב-16 בכל חודש, בהתאם לשיעור השינוי במדד החדש לעומת המדד הבסיסי; לעניין זה –~~

~~"מדד" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה;~~

~~"המדד החדש" – מדד החודש שקדם לחודש העדכון;~~

~~"המדד הבסיסי" – מדד חודש מאי 2007.~~

64. ~~22.~~ ~~הקלות~~שיקולים בגזירת הדין או גובה הפיצוי

בבואו לגזור את הדין או לפסוק פיצויים רשאי בית המשפט להתחשב, לטובת הנאשם, ~~או~~ הנתבע או הצד להליך מינהלי, גם באלה:

(1) חומרת הפגיעה בפרטיות ~~לא היתה אלא חזרה על מה שכבר נאמר, והוא נקב את המקור שעליו הסתמך~~;

(2) ~~הוא לא התכוון לפגוע~~היקף הפגיעה בפרטיות;

(3) משך הזמן שבו בוצעה הפגיעה בפרטיות;~~אם היתה הפגיעה בדרך של פרסום - הוא התנצל על הפרסום ונקט צעדים להפסקת מכירתו או הפצתו של עותק הפרסום המכיל את הפגיעה, ובלבד שההתנצלות פורסמה במקום, במידה ובדרך שבהם פורסמה הפגיעה ולא היתה מסויגת.~~

(4) הנזק הממשי שנגרם לנפגע בעבירה או לתובע, לפי העניין, להערכת בית המשפט;

(5) הרווח שצמח לנאשם או לנתבע, לפי העניין, בשל הפגיעה בפרטיות, להערכת בית המשפט;

(6) מאפייני הפעילות של הנאשם או הנתבע, לפי העניין;

(7) טיב היחסים בין הנפגע בעבירה לבין הנאשם, או הנתבע לתובע, לפי העניין;

(8) תום ליבו של הנאשם או הנתבע;

~~(3)~~(9) טיב תהליך עיצוב לפרטיות שהתבצע לפי סעיף 19.

פרק ~~ג~~ז: הגנות

65. ~~18.~~ הגנות מה הן

(א) בכל הליך משפטי או משמעתי לפי חוק זה~~ב משפט פלילי או אזרחי בשל פגיעה בפרטיות~~ תהא זו הגנה טובה אם נתקיימה אחת מאלה:

(1) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי סעיף 13 לחוק איסור לשון הרע, תשכ"ה-1965;

(2) עיבוד של המידע האישי נדרש לשם מילוי חובה על פי דין המוטלת על בעל השליטה במידע או המעבד;

(3)~~(2)~~ הנתבע, ~~או~~ הנאשם או צד להליך מינהלי עשה את הפגיעה בתום לב באחת הנסיבות האלה:

(א) הוא לא ידע ולא היה עליו לדעת על אפשרות הפגיעה בפרטיות;

(ב) הפגיעה נעשתה בנסיבות שבהן היתה מוטלת על הפוגע חובה חוקית~~,~~ ~~מוסרית, חברתית~~ או מקצועית לעשותה; לענין פסקה זו, "חובה מקצועית" – חובה לפי עקרונות או כללים של אתיקה מקצועית, החלים עליו מכוח דין או המקובלים על אנשי המקצוע שהוא נמנה עמהם;

(ג) הפגיעה נעשתה לשם הגנה על ענין אישי כשר של הפוגע;

(ד) הפגיעה נעשתה תוך ביצוע עיסוקו של הפוגע כדין ובמהלך עבודתו הרגיל, ובלבד שלא נעשתה דרך פרסום ברבים;

(ה) הפגיעה היתה בדרך של צילום, או בדרך של פרסום תצלום או של תוצר של תיעוד על אודות אדם, שנעשה ברשות הרבים ודמות הנפגע מופיעה בו באקראי;

(ו) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי פסקאות (4) עד (11) לסעיף 15 לחוק איסור לשון הרע, תשכ"ה-1965;

~~(ה)~~(ז) הפגיעה היתה נחוצה כדי להגן על חיין, חירותו, בריאותו או שלמות גופו של הנפגע או של אדם אחר;

(4) בפגיעה היה ענין ציבורי המצדיק אותה בנסיבות הענין, ובלבד שאם היתה הפגיעה בדרך של פרסום - הפרסום לא היה כוזב.

(5) הנפגע הוא קשיש, חסר ישע או קטין או שהיה קטין בעת הפגיעה בפרטיותו, והפגיעה נעשתה על ידי הורהו או אפוטרופסו שנתמנה לו כדין, לשם הגנה על עניין אישי כשר שלו.

(ב) ~~20(ב)~~ חזקה על הנאשם, ~~או~~ הנתבע או צד להליך מינהלי שעשה את הפגיעה בפרטיות שלא בתום לב אם התקיים אחד מאלה:

(1) הוא פגע ביודעין במידה העולה על הנדרש ~~גדולה משהיתה נחוצה באופן סביר~~ לצורך העניינים שניתנה להם הגנה ~~בסעיף 18(2)~~;

~~(א)~~(2) נושא המידע שנפגע דרש ממנו לתקן את המידע האישי על אודותיו לפי סעיף 13 והוא סירב שלא כדין לעשות כן.

66. ~~19.~~ פטור

~~(א)~~ לא ישא אדם באחריות לפי חוק זה על מעשה שהוסמך לעשותו על פי דין.

~~(ב) רשות בטחון, או מי שנמנה עם עובדיה או פועל מטעמה, לא ישאו באחריות לפי חוק זה על פגיעה שנעשתה באופן סביר במסגרת תפקידם ולשם מילויו.~~

~~(ג) "רשות בטחון", לענין סעיף זה - כל אחד מאלה:~~

~~(1) משטרת ישראל;~~

~~(2) אגף המודיעין במטה הכללי והמשטרה הצבאית של צבא-הגנה לישראל;~~

~~(3) שירות בטחון כללי;~~

~~(4) המוסד למודיעין ולתפקידים מיוחדים;~~

~~(5) הרשות להגנה על עדים.~~

67. ~~21.~~ הפרכה של טענות הגנה

הביא הנאשם, ~~או~~ הנתבע או צד להליך מינהלי ראיה, או העיד בעצמו כדי להוכיח אחת ההגנות הניתנות בחוק זה, רשאי התובע או הצד שכנגד להביא ראיות סותרות; אין בהוראה זו כדי לגרוע מסמכות בית המשפט לפי כל דין להתיר הבאת ראיות בידי בעלי הדין.

פרק ~~ה~~ח: הוראות שונות

68. ~~24.~~ דין המדינה

חוק זה חל על המדינה.

69. ~~25.~~ מות הנפגע

(א) אדם שנפגע בפרטיותו ותוך ששה חדשים לאחר הפגיעה מת בלי שהגיש תובענה או קובלנה בשל אותה פגיעה, רשאים בן-זוגו, ילדו או הורהו, ואם לא השאיר בן-זוג, ילדים או הורים – אחיו או אחותו, להגיש, תוך ששה חדשים לאחר מותו, תובענה או קובלנה בשל אותה פגיעה.

(ב) אדם שהגיש תובענה או קובלנה בשל פגיעה בפרטיות ומת לפני סיום ההליך, רשאים בן-זוגו, ילדו או הורהו, ואם לא השאיר בן-זוג, ילדים או הורים - אחיו או אחותו, להודיע לבית המשפט, תוך ששה חדשים לאחר מותו, על רצונם להמשיך בתובענה או בקובלנה, ומשהודיע כאמור יבואו הם במקום התובע או הקובל.

~~**26. התיישנות**~~

~~תקופת ההתיישנות של תביעה אזרחית לפי חוק זה היא שנתיים.~~

דברי הסבר

סעיף 63: מבוסס על סעיף 29א בחוק הגנת הפרטיות הקיים בשילוב התיקונים המוצעים בעניין החמרת הענישה כאשר הפגיעה היא בפרטיותם של נושאי מידע מאוכלוסיות חלשות.

ס"ק (ב) מגביל את מתן הפיצויים ללא הוכחת נזק בשל עוולה אזרחית רק להפרת הוראת סעיף 4(8) להצעת החוק הנוגעת לעיבוד מידע אישי. המטרה היא להגביר את ההרתעה מפני עיבוד מידע אישי בניגוד להוראת הצעת חוק זו.

סעיף 64: מבוסס על סעיף 56(ב) לחוק זכויות יוצרים, התשס"ח-2007 ומחליף את סעיף 22 לחוק הגנת הפרטיות הקיים, שלא מציג מכניזם ברור דיו לבית המשפט בקובעו את סכום הפיצוי בגין פגיעה בפרטיות.

סעיף 65: ס"ק (א) מבוסס על סעיף 18 בחוק הגנת הפרטיות הקיים, אך ההגנות הורחבו לכל הליך משפטי או משמעתי, כדי שיכלול גם הליכי אכיפה מינהלית והליכים אחרים שאינם פליליים או אזרחיים.

ס"ק (א)(1) זהה לסעיף 18(1) בחוק הגנת הפרטיות הקיים.

ס"ק (א)(2) מבוסס על סעיף 6(1)(c) ל-GDPR, אך הוסף כהגנה, ולא כבסיס לגיטימי לעיבוד מידע אישי כפי שקבוע ב-GDPR. המטרה היא שלא להטיל על נושא המידע את הנטל שבהוכחת תנאיו של ס"ק (א)(2).

ס"ק (א)(3)(א) מבוסס על סעיף 18(2)(א) בחוק הגנת הפרטיות הקיים, אבל מאחר שהרחבנו את ההגנות לכל הליך משפטי או משמעתי בחרנו לא להתייחס רק ל"נתבע או נאשם", אלא גם לצד בהליך מינהלי.

ס"ק (א)(3)(ב) מבוסס על סעיף 18(2)(ב) בחוק הגנת הפרטיות הקיים, אך הוא מחדד את ההבנה מהי חובה מקצועית ומסיר את ההתייחסות לחובה חברתית ומוסרית שמשמעותן והיקפן אינן ברורות. המטרה היא להימנע מפסיקות מרחיבות המתירות פגיעה בפרטיות בכסות של חובה מוסרית או חברתית.

ס"ק (א)(3)(ג) זהה לסעיף 18(2)(ג) לחוק הגנת הפרטיות הקיים.

ס"ק (א)(3)(ד) מבוסס על סעיף 18(2)(ד) לחוק הגנת הפרטיות הקיים.

ס"ק (א)(3)(ה) מבוסס על סעיף 18(2)(ה) לחוק הגנת הפרטיות הקיים. עם זה, לפעולת ה"צילום" הוספה פעולת "תיעוד", כדי להרחיב את ההגנה גם לקליטה אקראית של מידע אישי על הנפגע באמצעות חיישנים המוצבים במרחב הציבורי. לדוגמה: עיבוד בחיישני קול ובמפות חום במרחב הציבורי לצרכיי מעקב ומניעת פשיעה.

ס"ק (א)(3)(ו) זהה לסעיף 18(2)(ו) לחוק הגנת הפרטיות הקיים.

ס"ק (א)(3)(ז) שאב השראה מסעיפים 6(1)(d), 9(2)(c) ו-9(2)(i) ל-GDPR, אך הוסף כהגנה ולא כבסיס לגיטימי לעיבוד מידע אישי כפי שקבוע ב-GDPR. המטרה היא שלא להטיל על נושא המידע את הנטל שבהוכחת תנאי הסעיף.

ס"ק (א)(4) זהה לסעיף 18(3) לחוק הגנת הפרטיות הקיים.

ס"ק (א)(5) מבוסס על החמרת הענישה כאשר העבירה או הפגיעה היא בנושאי מידע מאוכלוסיות חלשות כמוצע בסעיף 62 להצעת החוק ובסעיף 1א להצ"ח פרטיות קטינים.

ס"ק (ב) מבוסס על סעיף 20 לחוק הגנת הפרטיות הקיים. הכללת חזקת תום הלב בסעיף ההגנות נועדה להצביע על כך שיש לפרשה בצמצום ואך ורק בהקשר של ההגנות המפורטות בסעיף קטן (א).

ס"ק (ב)(1) מבוסס על סעיף 20(ב) לחוק הגנת הפרטיות הקיים.

ס"ק (ב)(2) מבוסס על סעיף 17(א) לחוק איסור לשון הרע העוסק בשלילת הגנת תום הלב. מטרתו לתת בידי נושא המידע כלי נוסף שיבטיח שבקשתו לתיקון מידע אישי עליו לפי סעיף 13 תישקל במלוא תשומת הלב וכראוי.

<u>**סעיף 66:**</u> מבוסס על סעיף 19(א) לחוק הגנת הפרטיות הקיים.

סעיף 19(ב) לחוק הגנת הפרטיות הקיים לא אומץ בהצעת החוק. מאז חקיקת סעיף 19(ב) בשנת 1981 התרחשה המהפכה החוקתית והזכות לפרטיות עוגנה כאחת מזכויות היסוד החוקתיות בחוק-יסוד: כבוד האדם וחירותו. כתוצאה מכך, אין להתיר היום פגיעה בחוק בזכות לפרטיות באופן שאינו עומד בדרישות פסקת ההגבלה. בנוסף, סמכות מעקב ופגיעה גורפת בפרטיות לרשויות ביטחון יכולה להיות אבן נגף בפני הכרה אירופית (adequacy) שרמת הגנת הפרטיות בדין בישראל תואמת את זו האירופית.[18] יש צורך לקבוע הסמכה מפורשת ומידתית בחוק ייעודי שתעסוק בשימוש בטכנולוגיות לשם מעקב ומניעת פשיעה.

<u>**סעיף 67:**</u> זהה לסעיף 21 בחוק הגנת הפרטיות הקיים, אך לאור הרחבת ההגנות לכל הליך משפטי או משמעתי הוספנו גם את המילים "צד להליך מינהלי".

<u>**סעיף 68:**</u> זהה לסעיף 24 לחוק הגנת הפרטיות הקיים.

<u>**סעיף 69:**</u> זהה לסעיף 25 לחוק הגנת הפרטיות הקיים.

סעיף 26 לחוק הגנת הפרטיות הקיים המגביל את תקופת ההתיישנות של תביעה אזרחית לשנתיים, לא אומץ בהצעת החוק. לנוכח חשיבותה של הזכות לפרטיות כזכות יסוד חוקתית מוצע להשוות את תקופת ההתיישנות הקבועה בהצעת החוק לזו הנהוגה ביחס לעוולות אזרחיות אחרות. ככל שמדובר בתקופת התיישנות שאינה חורגת מהקבוע בחוק ההתיישנות, התשי"ח-1958, אין צורך בקביעה מיוחדת בחוק הפרטני, ולכן אין הצדקה לקביעת הוראה בנוגע להתיישנות בהצעת החוק.

~~3.~~70. ~~27.~~ סייג לפרסום הליכים ~~החלת הוראות מחוק איסור לשון הרע~~

~~על הליכים משפטיים בשל פגיעה בפרטיות יחולו הוראות סעיפים 21, 23 ו-24 לחוק איסור לשון הרע, תשכ"ה-1965, בשינויים המחוייבים לפי הענין.~~ במשפט פלילי או אזרחי בשל פגיעה בפרטיות רשאי בית המשפט מיוזמתו או לבקשת בעל דין, לאסור או לעכב זמנית, מנימוקים שירשמו, פרסום ברבים של הליכי בית המשפט – לרבות כתבי טענות, כתבי בי-דין אחרים, כתב אישום ודבר הגשתם של אלה ולרבות פסק דין כל עוד אינו חלוט – במידה שראה צורך בכך לשם הגנה על פרטיותו של אדם הנוגע במשפט; העובר על האיסור לפי סעיף זה, דינו – מאסר ששה חודשים או קנס ____.

71. דין שני משפטים

על הליכים משפטיים בשל פגיעה בפרטיות יחולו הוראות סעיף 77 לחוק בתי המשפט [נוסח משולב], התשמ"ד–1984.

~~**28. ראיות על שם רע, אופי או עבר של אדם**~~

~~במשפט פלילי או אזרחי בשל פגיעה בפרטיות אין להביא ראיה או לחקור עד בדבר שמו הרע של הנפגע או בדבר אפיו, עברו, מעשיו או דעותיו.~~

72. ~~29.~~ צוויים נוספים

הוראת סעיף 29 בחוק הגנת הפרטיות הקיים לא נדונה בקבוצת המומחים.

(א) בנוסף לכל עונש וסעד אחר רשאי בית המשפט, במשפט פלילי או אזרחי בשל הפרה של הוראה מהוראות חוק זה, לצוות כמפורט להלן, לפי הענין:

(1) על איסור הפצה של עתקי החומר הפוגע או על החרמתו; צו החרמה לפי פסקה זו כוחו יפה כלפי כל אדם שברשותו נמצא חומר כזה לשם מכירה, הפצה או החסנה, גם אם אותו אדם לא היה צד למשפט; ציווה בית המשפט על החרמה, יורה מה ייעשה בעתקים שהוחרמו;

(2) על פרסום פסק הדין, כולו או מקצתו; הפרסום ייעשה על חשבון הנאשם או הנתבע, במקום, במידה ובדרך שקבע בית המשפט;

(3) על מסירת החומר הפוגע לנפגע;

(4) על השמדת מידע שנתקבל שלא כדין, או לאסור על שימוש במידע כאמור או במידע עודף כהגדרתו בסעיף 23ה, או להורות לגבי המידע כל הוראה אחרת.

(ב) אין בהוראות סעיף זה כדי למנוע החזקת עותק של פרסום בספריות ציבוריות, בארכיונים וכיוצא באלה, זולת אם הטיל בית המשפט, בצו החרמה על פי סעיף קטן (א)(1), הגבלה גם על החזקה כזאת, ואין בהן כדי למנוע החזקת עותק של פרסום בידי הפרט.

~~29א. פיצוי בלא הוכחת נזק~~ סעיף 29א הועבר לסעיף 63 המוצע.

~~**30. אחריות בשל פרסום בעתון**~~

~~(א) פורסמה פגיעה בפרטיות בעתון, ישאו באחריות פלילית ואזרחית בשל הפגיעה האדם שהביא את הדבר לעתון וגרם בכך לפרסומו, עורך העתון ומי שהחליט בפועל על פרסום אותה פגיעה בעתון, ובאחריות אזרחית ישא גם המוציא לאור של העתון.~~

~~(ב) באישום פלילי לפי סעיף זה תהא זאת הגנה טובה לעורך העתון שנקט אמצעים סבירים כדי למנוע פרסום אותה פגיעה ושלא ידע על פרסומה.~~

~~(ג) בסעיף זה, "עורך עתון" – לרבות עורך בפועל.~~

~~**31. אחריות של מדפיס ומפיץ**~~

~~פורסמה פגיעה בפרטיות בדפוס, למעט בעתון בעל תדירות הופעה של ארבעים ימים או~~

~~פחות, ישאו באחריות פלילית ואזרחית בשל הפגיעה גם מחזיק בית הדפוס שבו הודפס הפרסום, ומי שמוכר את הפרסום או מפיץ אותו בדרך אחרת, ובלבד שלא ישאו באחריות אלא אם ידעו או חייבים היו לדעת שהפרסום מכיל פגיעה בפרטיות.~~

~~31א. עונשין בעבירות של אחריות קפידה~~

~~(א) העושה אחד מאלה, דינו - מאסר שנה:~~

~~(1) מנהל, מחזיק או משתמש במאגר מידע בניגוד להוראות סעיף 8;~~

~~(2) מוסר פרטים לא נכונים בבקשה לרישום מאגר מידע כנדרש בסעיף 9;~~

~~(3) אינו מוסר פרטים או מוסר פרטים לא נכונים בהודעה המלווה בקשה לקבלת מידע לפי סעיף 11;~~

~~(4) אינו מקיים את הוראות סעיפים 13 ו-13א לענין זכות העיון במידע המוחזק במאגר מידע, או אינו מתקן מידע על פי הוראות סעיף 14;~~

~~(5) מאפשר גישה למאגר מידע בניגוד להוראות סעיף 17א(א) או אינו מוסר לרשם מסמכים או תצהיר בהתאם להוראות סעיף 17א(ב);~~

~~(6) אינו ממנה ממונה על אבטחת מידע בהתאם להוראות סעיף 17ב;~~

~~(7) מנהל או מחזיק מאגר המשמש לשירותי דיוור ישיר, בניגוד להוראות סעיפים 17ד עד 17ו;~~

~~(8) מוסר מידע בניגוד לסעיפים 23ב עד 23ה.~~

~~(ב) עבירה לפי סעיף זה אינה טעונה הוכחת מחשבה פלילית או רשלנות.~~

~~31ב. עוולה בנזיקין~~

~~מעשה או מחדל בניגוד להוראות פרקים ב' או ד' או בניגוד לתקנות שהותקנו לפי חוק זה יהווה עוולה לפי פקודת הנזיקין [נוסח חדש].~~

דברי הסבר

<u>**סעיפים 70 - 71**</u>: מחליפים את סעיף 27 בחוק הגנת הפרטיות הקיים המפנה לסעיפים 21, 23-24 בחוק איסור לשון הרע, התשכ"ה–1965. במקום ההפניה לסעיף 21 לחוק איסור לשון הרע, התשכ"ה–1965 הוספה לשון הסעיף במלואה, למעט ההוראה הקובעת שבית המשפט אינו יכול לעכב או לאסור פרסום דבר פתיחתו של הליך פלילי אם הנפגע התנגד לכך. הוראה זו מתאימה לדיני איסור לשון הרע ואין מקומה בהצעת חוק העוסקת בפגיעה בפרטיות. סעיף 23 בחוק איסור לשון הרע אינו רלוונטי לעולם דיגיטלי, ויש להחיל במקומו את דיני הראיות הרגילים. במקום ההפניה לסעיף 24 לחוק איסור לשון הרע הוספה בסעיף 71 להצעת החוק הפניה לסעיף 77 לחוק בתי המשפט [נוסח משולב], התשמ"ד – 1984, שהיא עדכנית וברורה יותר.

<u>**סעיפים 30 ו-31 בחוק הגנת הפרטיות הקיים**</u>, שעוסקים באחריות עורך עיתון, מפרסם בעיתון ומפיץ, לא אומצו בהצעת החוק. הוראות סעיפים אלו עוסקות באמצעי תקשורת קונקרטיים ואילו בהצעת החוק ביקשנו ליצור הוראות ניטרליות לטכנולוגיה. נוסיף עוד שפרסום נכלל בעיבוד מידע אישי לפי הגדרת "עיבוד" בסעיף 2 להצעת החוק, ועל כן המפרסם מידע אישי ממילא יישא באחריות לפי הצעת החוק אם פועל שלא לפי הוראות הצעת החוק. משום כך הוראות סעיפים 30 ו-31 לחוק הגנת הפרטיות הקיים מיותרות.

<u>**סעיף 31א לחוק הגנת הפרטיות הקיים**</u> המגדיר את עבירות האחריות קפידה, לא אומץ בהצעת החוק. הותרת הוראה בעניין אחריות קפידה מגבירה את הסיכון הכפול שבשמירת האחריות הפלילית לפי סעיף 58 המוצע. נוסיף גם כי אין הוראה דומה בדברי חקיקה אחרים, ששילבו בעשור האחרון הוראות לאכיפה מינהלית, למשל התיקון משנת 2012 לחוק ההגבלים העסקיים[19] והתיקון משנת 2014 לחוק הגנת הצרכן.[20]

<u>**סעיף 31ב לחוק הגנת הפרטיות הקיים**</u> שמגדיר מהי עוולה בנזיקין, לא אומץ בהצעת החוק. אין לו הצדקה לאור סעיף 61 המוצע.

73. ~~32.~~ חומר פסול לראיה

חומר שהושג תוך פגיעה בפרטיות יהיה פסול לשמש ראיה בבית משפט, ללא הסכמת הנפגע, זולת אם בית המשפט התיר מטעמים שיירשמו להשתמש בחומר, או אם היו לפוגע, שהיה צד להליך, הגנה או פטור לפי חוק זה.

74. ~~10א.~~ דו"ח הגנה על הפרטיות

לא יאוחר מ-1 באפריל בכל שנה יגיש ראש הרשות להגנת הפרטיות ~~תגיש המועצה להגנת הפרטיות~~ לועדת החוקה חוק ומשפט של הכנסת דין וחשבון ~~שיכין הרשם~~ על פעולותיה של הרשות, ובכלל זה פעולות האכיפה והפיקוח בשנה שקדמה להגשת הדו"ח, לרבות מספר העיצומים הכספיים שהוטלו, סכומם, בשל אילו הפרות הוטלו ומספר ההפרות החוזרות שבוצעו מתוך כלל ההפרות בשנה שקדמה למועד הדיווח~~בצירוף הערותיה של המועצה~~.

75. תיקון חוק בתי משפט לענינים מינהליים

בחוק בתי המשפט לענינים מינהליים, התש"ס–2000, בתוספת הראשונה, במקום פרט 28 יבוא:

" 28. החלטה של הרשות להגנת הפרטיות לפי חוק הגנת הפרטיות, התשע"ט-2019."

~~33. תיקון פקודת הנזיקין~~

~~בפקודת הנזיקין [נוסח חדש], סעיף 34א - בטל.~~

~~34. תיקון חוק סדר הדין הפלילי~~

~~בתוספת לחוק סדר הדין הפלילי, תשכ"ה-1965, אחרי פסקה (12) יבוא:~~

~~"(13) עבירות על חוק הגנת הפרטיות, תשמ"א-1981".~~

76. ~~35.~~ שמירת דינים

הוראות חוק זה לא יגרעו מהוראות כל דין אחר שהיה קיים ערב תחילתו של חוק זה.

77. ~~36.~~ ביצוע ותקנות

שר המשפטים ממונה על ביצוע חוק זה והוא רשאי, באישור ועדת החוקה חוק ומשפט של הכנסת, להתקין תקנות~~, באישור ועדת החוקה חוק ומשפט של הכנסת,~~ בכל ענין הנוגע לביצועו, ובין השאר –

(1) תנאי החזקת מידע אישי ושמירתו ~~במאגרי מידע~~;

(2) תנאים להעברה של מידע אישי אל ~~מאגרי מידע ש~~מחוץ לגבולות המדינה ~~או מהם~~;

(3) תנאי אבטחת מידע אישי~~כללי התנהגות ואתיקה לבעלים, למחזיקים או למנהלים של מאגרי מידע ולעובדיהם~~;

(4) הוראות לענין ביעור מידע אישי עם הפסקת עיבודו~~פעולתו של מאגר מידע~~.

78. התאמה למדד

(א) הסכום לתשלום בגין מימוש זכות מזכויות נושא המידע לפי סעיף 16(ב) וסכום הפיצוי בלא הוכחת נזק לפי סעיף 63 יעודכנו ב-16 בכל חודש, בהתאם לשיעורי השינוי במדד החדש לעומת המדד הבסיסי, לעניין זה –

"המדד" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה;

"המדד החדש" – מדד החודש שקדם לחודש העדכון;

"המדד הבסיסי" – מדד חודש דצמבר 2018.

(ב) סכומי העיצום הכספי כאמור בסעיף 38 וסכום הקנס כאמור בסעיף 70 יעודכנו ב-1 בינואר בכל שנה (בסעיף קטן זה – "יום העדכון"), בהתאם לשיעור שינוי המדד הידוע ביום העדכון לעומת המדד שהיה ידוע ב-1 בינואר של השנה הקודמת; הסכום האמור

יעוגל לסכום הקרוב שהוא מכפלה של 10 שקלים חדשים; לעניין זה, "מדד" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה. שר המשפטים יפרסם בהודעה ברשומות את סכום הקנס המעודכן לפי סעיף קטן זה. ראש הרשות להגנת הפרטיות יפרסם ברשומות הודעה על סכומי העיצום הכספי המעודכנים לפי סעיף קטן זה.

36א.אגרות

(א) שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, רשאי לקבוע –

(1) אגרות בעבור רישום מאגר מידע ועיון בו לפי חוק זה;

(2) אגרה, לתקופה שיקבע, בעבור מאגר מידע הרשום בפנקס (להלן – אגרה תקופתית), למעט מאגר מידע שבבעלות המדינה, ורשאי הוא לקבוע שיעורים שונים של אגרות תקופתיות לפי סוגים של מאגרים, וכן את מועדי התשלום של האגרה התקופתית, ותוספת אגרה לאגרה תקופתית שלא שולמה במועדה.

(ב) כספי אגרות שנגבו לפי סעיף זה ייועדו לרשם וליחידת הפיקוח לצורך פעולתם לפי חוק זה.

(ג) לא שולמה האגרה התקופתית או תוספת האגרה לאגרה התקופתית, לפי הענין, בתוך שישה חודשים מהמועד שנקבע בתקנות לתשלום תוספת האגרה, יותלה רישומו של המאגר בפנקס עד לתשלום.

37.תחילה

תחילתו של פרק ב' ששה חדשים מיום פרסומו של חוק זה.

דברי הסבר

סעיף 73: זהה לסעיף 32 לחוק הגנת הפרטיות הקיים.

סעיף 74: מבוסס על סעיפים 10א בחוק הגנת הפרטיות הקיים ו-22כו לחוק הגנת הצרכן, לעניין דיווח על אכיפה מינהלית.

סעיף 75: מבהיר שכל החלטה של הרשות להגנת הפרטיות היא החלטה מינהלית שמותר לעתור בגינה לבית המשפט לעניינים מינהליים.

סעיף 76: מבוסס על סעיפים 35 בחוק הגנת הפרטיות הקיים ו-10 בחוק-יסוד: כבוד האדם וחירותו – מתוך הבנת חשיבותה ומרכזיותה של הזכות לפרטיות כזכות יסוד חוקתית.

סעיף 77: מבוסס על סעיף 36 לחוק הגנת הפרטיות הקיים ומותאם לנושאים ששר המשפטים מוסמך להתקין בעניינם תקנות לפי הצעת החוק.

סעיף 78: מבוסס על תקנה 6 לתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי דין בערעור על סירוב לבקשת עיון), התשמ"א–1981 ועל סעיף 23כה(ב) להצ"ח תיקון מס' 13. סעיף 78 הוא סעיף סל שמאגד את כל ההוראות הנוגעות לעדכון סכום כספי לפי הצעת החוק: תשלום בעבור מימוש זכות מזכויות נושא המידע לפי סעיף 16, פיצוי בלא הוכחת נזק לפי סעיף 63, עיצום כספי לפי סעיף 38 וקנס לפי סעיף 70.

סעיף 36א לחוק הגנת הפרטיות הקיים שעוסק בסמכות שר המשפטים לקבוע אגרות , לא אומץ בהצעת החוק. תשלום אגרות בעבור רישום מאגרי מידע ואגרות תקופתיות בוטל באוגוסט 2017 בתקנות הגנת הפרטיות (אגרות) (ביטול), התשע"ז–2017, ולכן אין הצדקה להסמכת שר המשפטים לקבוע אגרות בהצעת החוק.

1 חוק-יסוד: כבוד האדם וחירות, ס"ח התשנ"ב 1391.

2 ראו בג"ץ 6650/04 **פלונית נ' בית הדין הרבני האזורי נתניה**, פ"ד סא(1) 581 (2006).

3 הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח–2018 [להלן: "**הצ"ח תיקון מס' 13**"].

4 הצוות לבחינת החקיקה בתחום מאגרי המידע, דין וחשבון (ינואר 2007), עמ' 19-23 [להלן: "**ועדת שופמן**"].

5 הצעת חוק הגנת הפרטיות (תיקון – הגנה על פרטיות של קטינים), התשע"ז–2017 (להלן: "**הצ"ח פרטיות קטינים**").

6 אסף הרדוף, "צילום חכם: האם צילום מחשב ללא רשות ראוי להוות עברה פלילית", **משפטים** על אתר (2018).

7 ועדת שופמן, ה"ש 4 לעיל, עמ' 24.

8 תזכיר חוק הגנת הפרטיות (לצמצום חובת הרישום וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולתיעודם במסמכים), התשע"ב-2012.

9 Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/56/EC, 844/14/EN WP 217 (2014) Article 29

10 סעיף 6 לחוק הכשרות המשפטית והאפוטרופסות, התשכ"ו-1962 קובע כי: "פעולה משפטית של קטין שדרכם של קטינים בגילו לעשות כמוה, וכן פעולה משפטית בין קטין לבין אדם שלא ידע ולא היה עליו לדעת שהוא קטין ,אינה ניתנת לביטול כאמור בסעיף 5, אף שנעשתה שלא בהסכמת נציגו, אלא אם היה בה משום נזק של ממש לקטין או לרכושו".

11 ועדת שופמן, ה"ש 4 לעיל, עמ' 42-47.

12 סעיף 3(ד)(7) לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007: "פרטי הזיהוי של המנוי או מיתקן הבזק שנתוני התקשורת מתבקשים לגביהם, אם הם ידועים מראש, לרבות היות המנוי האמור מי שחל לגביו חיסיון מקצועי לפי כל דין (בחוק זה – בעל מקצוע); בפסקה זו, 'דין' – לרבות הלכה פסוקה;"

13 תקנה 5(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017, קובעת כך:

"5. (ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר סיכוני אבטחת מידע (להלן - סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשרה חודשים לפחות."

14 privacy Amendment (Notifiable Data Breaches) Act 2017 No. 12, 2017

15 שגיא כהן, "פייסבוק: מידע על 47 אלף ישראלים נחשף בפרשת קיימברידג' אנליטיקה", **Ynet** (10 באפריל 2018).

16 39th International Conference of Data Protection and Privacy Commissioners Hong Kong, Sep. 25-29, 2017, Resolution on exploring future options for International Enforcement Cooperation (2017);

17 FTC Earns Prestigious International Award for AshleyMadison.com Data Breach Investigation, FTC (Sep. 27, 2017);

18 סמכות המעקב והפגיעה הגורפת בפרטיות על ידי ה-NSA בארה"ב, כפי שנתגלה מהמסמכים שחשף סנאודן, היתה הסיבה העיקרית לביטול ה-safe harbor – בארה"ב *Maximillian Schrems v Data Protection*) *Commissioner*, Case C–362/14, 6 October 2015, ECLI:EU:C:2015:650), ודיונים בנוגע להכרה בתאימות הדין ביפן ובאנגליה ל-GDPR עסקו בנושא סמכות המעקב הניתנת לרשויות הביטחון בכל אחת מהמדינות. ראו Andrew D. Murray, *Data Transfers between the EU and UK Post Brexit?*, 7(3) INTERNATIONAL Claude Moraes, ;DATA PRIVACY LAW 149 (2017) Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection of personal data .afforded by Japan (2018q2979 (RSP))

19 חוק ההגבלים העסקיים (תיקון מס' 13), התשע"ב–2012.

20 חוק הגנת הצרכן (תיקון מס' 39), התשע"ד–2014.

עו"ד רחל ארידור הרשקוביץ היא חוקרת בתוכנית "דמוקרטיה בעידן המידע" שבמרכז לערכים ולמוסדות דמוקרטיים במכון הישראלי לדמוקרטיה. בעלת תואר ראשון ושני במשפטים. עבודת הדוקטור שלה בפקולטה למשפטים באוניברסיטת חיפה עוסקת בנושא מסגרות לשיתופי פעולה בין הממשל לתעשייה לשם הגברת ההגנה על מרחב הסייבר.

ד"ר תהילה שוורץ אלטשולר היא עמיתה בכירה במכון הישראלי לדמוקרטיה, עומדת בראש התוכניות "רפורמות במדיה" ו"דמוקרטיה בעידן המידע". עמיתת מחקר בכירה במרכז פדרמן למשפט וסייבר באוניברסיטה העברית בירושלים ומשמשת נציגת ציבור בנשיאות מועצת העיתונות. מומחית לאסדרת תקשורת ולממשק שבין טכנולוגיה, משפט ומדיניות.

מסת"ב:
978-965-519-265-0

המכון הישראלי
לדמוקרטיה

www.idi.org.il