

סקירה כללית של תיקון מס' 13 לחוק הגנת הפרטיות

עו"ד רבקי דב"ש
עמיתה בכירה במכון הישראלי למדיניות טכנולוגיה

אוקטובר/2024

1 - רקע	2
2 - עיקרי התיקון הישראלי לחוק הפרטיות	3
3 - שינוי הגדרות של מונחי מפתח, כגון "נתונים אישיים" או "נתונים ביומטריים"	3
4 - צמצום היקף דרישת הרישום	8
5 - פיצוי ללא הוכחת נזק (פיצויים לדוגמא)	9
6 - התיקון מחייב מינוי קציני הגנת מידע במקרים ספציפיים	9
7 - הסמכויות של הרשות להגנת הפרטיות השתנו באופן משמעותי	10
7.1 - הגדרת הרשות להגנת הפרטיות ותפקידה	10
7.2 - סמכויות הרשות	11
7.3 - אמצעי אכיפה מנהליים	13
7.4 - הוראות פרוצדורליות לעניין הטלת עיצומים כספיים	14
8 - התיקונים מציגים עבירות פליליות הקשורות לעיבוד נתונים אישיים	15
9 - תיקונים שונים: משינוי הגבלת המטרה, להרחבת דרישת ההודעה	16
9.1 - הגבלת מטרה	16
9.2 - הודעה	17
9.3 - התיישנות	18
9.4 - אחריות קפידה	18
9.5 - ביטול ההסמכה לקבוע אגרות	18
10 - סיכום	18
נספח	19

סקירה כללית של תיקון מס' 13 לחוק הגנת הפרטיות

עו"ד רבקי דב"ש, עמיתה בכירה, FPF ישראל

מסמך זה מבקש לסקור את עיקריו של תיקון מס' 13 לחוק הגנת הפרטיות, שנחקק באוגוסט 2024. נציין כי לדברי נציגי משרד המשפטים, תיקון נוסף לחוק הגנת הפרטיות, שצפוי לכלול תיקונים מהותיים להוראות החוק, נמצא בשלבי ניסוח מתקדמים ומתוכנן להתפרסם בתקופה הקרובה. הניתוח יבחן גם השוואה של היבטים מרכזיים (גם אם לא באופן מקיף) עם שתי חקיקות מובילות בתחום זה ברחבי העולם: התקנה הכללית להגנה על נתונים (GDPR) (EU) וחוק פרטיות הצרכן בקליפורניה (CCPA) (קליפורניה).

נקודה משמעותית שיש לזכור ביחס להשוואה כזו היא שיש הבדל גדול מכיוון שהתקנות של האיחוד האירופי וקליפורניה הן אקס-טריטוריאליות. במילים אחרות, כאשר בעל שליטה מעבד נתונים על תושבי האיחוד האירופי או קליפורניה ועומד בהגדרות ההסדר הנורמטיבי, הדין באותו אזור יחול עליהם גם אם העסק אינו ממוקם בתחום השיפוט הרלוונטי, בניגוד לחוק הישראלי ולתקנות החלות רק על ישויות בתחום השיפוט של ישראל.

מטעמי נוחות, ההשוואה לדין הזר תסומן ברקע כחול.

1 – רקע

ביום 5.8.2024 אישרה מליאת הכנסת את **הצעת חוק הגנת הפרטיות** (תיקון מס' 13), התשפ"ד-2024 (להלן: התיקון), אשר ייכנס לתוקף ביום 14.8.2025.

על פי דברי ההסבר, התיקון החקיקתי נובע מהקמת הרשות להגנת הפרטיות בשנת 2006 ומההמלצות בדו"ח שופמן שהוגש בשנת 2007, אשר עסק בתיקונים הנדרשים באותה עת בנוגע להסדר הנוגע להגנת המידע. הצעת החוק שביקשה לקדם את סמכויות האכיפה של הרשות הוגשה לראשונה בשנת 2011 ולאחר מכן בשנת 2018, ולא קודמה בשל חוסר יציבות פוליטית בישראל.

למרות חלוף הזמן, התיקונים נותרו להתמקד בסמכויות האכיפה של הרשות, ואילו התיקון המיוחל הנוגע להוראות מהותיות בחוק, לרבות בסיסים משפטיים נוספים לעיבוד נתונים והרחבת זכויותיהם של נושאי מידע, נותר מחוץ לחקיקה. חריג היה הסדר שנקבע בתקנות לפי חוק הפרטיות ביחס למאגר מידע שאליו מועברים נתונים מהאזור הכלכלי האירופי, כמפורט להלן:

בשנת 2023, ועל מנת לשמור על ההכרה בעמידה של הדין הישראלי ב-GDPR, אישרה הכנסת את **תקנות הגנת הפרטיות** (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023 (להלן – תקנות הגישור). תקנות אלו הקנו זכויות יתר לנושאי מידע שמידע אודותם מצוי במאגר מידע הכולל גם מידע שמקורו מהאיזור הכלכלי האירופי (אזור EEA). יודגש, כי ההבחנה אינה על פי זהותו או **לאומיותו** של נושא הנתונים, אלא **על פי המקור** ממנו התקבלו הנתונים. במילים אחרות, תקנות הגישור יצרו שני רובדי זכויות של נושאי המידע: הראשון, הזכויות המוגבלות הקיימות בדין הישראלי החלות על כלל מאגרי המידע בישראל, והשני, המרחיב משמעותית את זכויות נושאי המידע בהשוואה לאלו הקבועות בדין הישראלי והחלה על מאגרי מידע המכילים נתונים שהגיעו מאזור EEA – בעוד שהזכויות יחולו על כל נושאי המידע במאגר, ללא קשר למקור שממנו הגיעו הנתונים.

גם אם ההסדר בתקנות הגישור הוא חלקי ואינו כולל את כל היתרות ב-GDPR, הוא יצר חובות מוגברות לגבי מידע אישי המעובד בחלק ממאגרי המידע בישראל.

למידע נוסף על תקנות הגישור קראו את [סקירת המכון הישראלי למדיניות טכנולוגיה](#) בנושא (אפריל 2023).

2 - עיקרי התיקון הישראלי לחוק הפרטיות

התיקון כולל מספר נושאים עיקריים:

- שינוי הגדרות חקיקתיות (ראו סעיף 3 להלן);
 - צמצום חובות הרישום (סעיף 4);
 - הוספת האפשרות לדרוש פיצוי ללא הוכחת נזק (בלשון החוק: פיצוי לדוגמא) - אופציה שניתנה עד כה רק בגין פגיעה בפרטיות (Privacy) ולא בגין הפרת הוראות הנוגעות להגנת מידע אישי (Data Protection) (סעיף 5);
 - חובת מינוי ממונה על הפרטיות (סעיף 6);
 - הסדרת מעמדה של הרשות וסמכויות האכיפה שלה (סעיף 7);
 - קביעת סנקציות בגין הפרה מינהלית (סעיף 7);
 - הגדרת עבירות פליליות ביחס להפרות הגנת מידע אישי (סעיף 8).
- כמו כן, ישנם תיקונים נוספים הקשורים לנושאים שונים. אלה כוללים שינוי הנוסח הנוגע לחובת בעל המאגר לעבד את הנתונים רק בהתאם למטרת המאגר, הוספת חובות להודעה שנמסרה בעת איסוף הנתונים, הסרת ההגבלה להגשת תביעה אזרחית תוך שנתיים (התיישבות) לפי חוק הפרטיות, שעמדה בעבר על שנתיים ועוד. תיקונים אלה יטופלו גם בסקירה (סעיף 9).

3 - שינוי הגדרות של מונחי מפתח, כגון "נתונים אישיים" או "נתונים ביומטריים"

ההגדרות בחוק הגנת הפרטיות, התשמ"א-1981 (להלן: החוק) מתפרסות על פני מספר סעיפים, לרבות סעיפים 3, 7 ו-17א. התיקון העביר את ההגדרות החלות על החוק כולו לסעיף 3, תוך עדכון והוספת ההגדרות הנדרשות.

להלן נתייחס לחלק מההגדרות העיקריות המעודכנות ונשווה אותן לגרסאות הקיימות של ההסדרים האירופי והקליפורני. יש לציין כי בכלל, ההגדרות לא הועתקו מילה במילה (כאשר הועתקו כאמור, הניסוח מצוין במרכאות). ההתייחסות להסדרים בחו"ל נועדה להציג פערים משמעותיים, אם בכלל, בין ההגדרה בישראל לבין ההגדרה באותו מקום, ולא דווקא להציג את ההגדרה כולה.

הגדרה	ההסדר הישראלי	GDPR	CCPA
מידע אישי	"נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי". "אדם הניתן לזיהוי" – פירושו אדם שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזוהה או באמצעות נתון אחד או יותר הנוגע אליו.	ההגדרה הישראלית דומה להגדרה האירופאית בהבדל אחד – ה-GDPR אינו משתמש במונח "סבירות" ביחס ליכולת לזהות אדם, ובכך הופך אותו למחמיר יותר	ההגדרה בקליפורניה שונה במספר מובנים – א. היא מתייחסת גם לנתונים המשויכים למשק בית. ב. ההגדרה מפרטת דוגמאות למידע אישי

הגדרה	ההסדר הישראלי	GDPR	CCPA
		מההגדרה החדשה בישראל (Art 4).	(אם כי הרשימה אינה סגורה). ג. ההגדרה מחריגה מידע שפורסם לרבים כדין או שיש אינטרס ציבורי בחשיפתו. ד. ההגדרה מחריגה מידע לא מזוהה או נתונים מצטברים (אגרגטיביים) (v)1798.140)
מידע בעל רגישות מיוחדת	ההגדרה רלוונטית לעניין חובת הודעה, מינוי ממונה על פרטיות (ככל שמתקיימים התנאים הנוספים) והעלאת גובה העיצום הכספי. יצוין כי בתוספת הראשונה לתקנות אבטחת המידע קיימת רשימה של סוגי מידע שעיודם מעלה את המאגר לרמת אבטחה בינונית, תוך הבנה כי קטגוריות אלו הן של מידע רגיש יותר. <u>אין</u> התאמה בין שתי הרשימות, דבר היוצר חוסר אחידות בתפיסה הנורמטיבית ועלול להטעות.	ההבדל המהותי בין שני החוקים הוא שההתייחסות למונח "קטגוריות מיוחדות של מידע אישי" (special categories of personal data), נועדה ברגולציה האירופית להגביל את העיבוד המותר בקטגוריות אלו תוך החרפת הנסיבות שבהן ניתן לעבד את המידע המכוסה תחת אחת הקטגוריות (art. 9).	ההבדל המהותי בין ההסדרים הוא שההתייחסות ל"מידע אישי רגיש" נועדה להוסיף הוראות מיוחדות לגביהם, ובין היתר ביחס לחובות ההודעה (1798.100) ולזכותו של נושא המידע להגביל את השימוש במידע כאמור או את גילוי (1798.121).
	מידע בעל רגישות מיוחדת – א. צנעת חייו של אדם ונטייתו המינית; ב. מצב בריאותו של אדם; ג. מידע גנטי; ד. "מזהה ביומטרי המשמש או המיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב"; ה. מוצאו של אדם; ו. עבר פלילי; ז. דעות פוליטיות, אמונות דתיות אדם והשקפת עולם; ח. הערכת אישיות שנערכה מטעם גורם מקצועי; ט. נתוני מיקום ונתוני תעבורה שנוצרו על ידי ספק מורשה, ונתונים על מיקומו של אדם שיש בהם כדי ללמד על מידע לפי	סוג המידע הכלול בקטגוריה זו מצומצם יותר וחופף רק לקטגוריות המנויות בס"ק (1)-(4), ו- (7) להגדרה בישראל, ומתווספת חברות באיגוד עובדים.	קטגוריות המידע האישי הרגיש, שונות במקצת מאלה שבבישראל. בנוסף להגדרות דומות לקטגוריות המנויות בס"ק (1)-(7), קיימות גם הקטגוריות הבאות: א. מפתח זיהוי (כגון מספר ת.ז, מספר דרכון); ב. נתונים המאפשרים כניסה לחשבון של צרכן; ג. מיקום גיאוגרפי מדויק; ד. תוכן דואר והודעות, למעט אם העסק הוא הנמען; ה. חברות באיגודים מקצועיים.

הגדרה	ההסדר הישראלי	GDPR	CCPA
	פסקאות (1)-(7) ו-(10)-(11) להגדרה; י. נתוני שכר ופעילות פיננסית; יא. מידע אישי שלגביו קיימת חובת סודיות בדיון; יב. מידע נוסף שקבע השר בתוספת השנייה, אשר הגיע מחוץ לישראל ושבמדינה ממנה הגיע, חלים על סוג מידע כאמור הוראות דין מיוחדות.		עם זאת הזכות להגביל את השימוש או הגילוי של מידע אישי רגיש מוגבלת רק למידע המשמש להסיק מאפיינים אל אדם.
מזהה ביומטרי	"נתון ביומטרי המשמש לזיהוי אדם או לאימות זהותו, או אמצעי ביומטרי שניתן להפיק ממנו נתון כאמור" " 'ביומטרי' – מאפיין אנושי, פיזיולוגי או התנהגותי, ייחודי, הניתן למדידה ממוחשבת."	ההגדרה הישראלית דומה להגדרה האירופאית (Art 4) אם כי ההגדרה ב-GDPR מבחינה בין הנתונים עצמם לבין הנתונים המיועדים לזיהוי אדם. השפה בה נעשה שימוש מתייחסת לאפשרות הזיהוי ולא דווקא ליכולת לעשות זאת, כפי שניתן ללמוד מהלשון של ההגדרה בישראל.	ההגדרות דומות, אלא שההסדר בקליפורניה כולל מזהה ביומטרי המשמש או מיועד לשמש לזיהוי בשילוב עם נתונים נוספים (ולא רק מזהה כשלעצמו). (1798.140(c))
מאגר מידע (מסד נתונים)	"אוסף פרטי מידע אישי המעובד באמצעי דיגיטלי, למעט" – א. אוסף לשימוש אישי שאינו למטרות עסק; ב. אוסף הנוגע לפחות מ-100,000 איש, ויש בו רק שם, מען ודרכי התקשרות, שאין לגבי הרשימה מאפיין אישי נוסף, ואין בידי בעל השליטה אוסף הכולל מידע נוסף על אנשים אלו.	החוק האירופי חל על כל עיבוד של נתונים אישיים הנעשה באמצעים אוטומטיים, בין אם נתונים אלה הם חלק ממערכת תיוק (filing system) ובין אם לאו. ה-GDPR חל גם על עיבוד לא אוטומטי (ידני) של נתונים אישיים רק כל עוד הוא נעשה במערכת תיוק, המוגדרת בסעיף 4(6) ככל קבוצה מובנית של נתונים אישיים הנגישים על פי קריטריונים ספציפיים, בין אם הם מרוכזים, מבוזרים על בסיס פונקציונלי או גיאוגרפי.	החוק בקליפורניה הוא למעשה חוק צרכני. לפיכך הגורם הרלוונטי היחיד לעניין נשיאה באחריות הוא אם העסק עונה על לפחות אחד משלושת הבאים – א. בעל הכנסה שנתי (ברוטו) מעל \$25M; ב. מדי שנה קונה, מוכר או משתף במידע האישי של 100,000 או יותר מתושבי קליפורניה או משקי בית; ג. 50% או יותר מההכנסה השנתית, מקורה ממכירת מידע אישי על תושבי קליפורניה.

הגדרה	ההסדר הישראלי	GDPR	CCPA
עיבוד, שימוש	כל פעולה שמבוצעת במידע אישי.	קיימת שונות מסוימת (הגדרת ה-GDPR (סעיף 4(2)) מתייחסת במפורש גם למערך נתונים ועיבוד באמצעים אוטומטיים), אך נראה כי ההגדרה הישראלית היא רחבה יותר ומכילה גם את אלו בתוכה.	ההגדרה בקליפורניה דומה ל-GDPR של האיחוד האירופי.
בעל השליטה במאגר מידע	"מי שקובע, לבדו או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע או גוף שהוא או בעל תפקיד בו הוסמך בחיקוק לעבד מידע במאגר מידע."	ההגדרה הישראלית מקבילה להגדרה האירופאית (סעיף 4(7)).	המקבילה בקליפורניה היא "עסקים" (ראו הגדרה לעיל).
מחזיק	"גורם חיצוני לבעל השליטה במאגר המידע המעבד בעבורו מידע."	ההגדרה של "מחזיק" בחוק הישראלי מעורפלת בהשוואה למושגים של ה-GDPR של "Processor" ו"third party", אך היא קרובה יותר לראשונה. על פי ה-GDPR "מעבדים" הם כל אישיות טבעית או משפטית המעבדת נתונים אישיים בשם (on behalf) בעל השליטה במידע, בעוד שצד שלישי הוא כל אישיות טבעית או משפטית שאינה נושא המידע, מעבד או כל אדם אחר המעבד מידע אישי תחת סמכותו של בעל השליטה (כך שהם גורמים חיצוניים).	ההגדרה המקבילה היא "Contractor" והיא כוללת מגבלות על סוג ההתקשרות שעסק יכול לעשות עם מי שפועל מטעמו. (1798.140(j))
אבטחת מידע	"הגנה על שלמות המידע האישי או הגנה על המידע האישי מפני עיבוד, ללא רשות כדין".	ה-GDPR אינו מגדיר את המונח, אך החובה עצמה מוגדרת בצורה הוליסטית יותר מאשר בהסדר הישראלי, תוך התייחסות למרכיבים שונים שיש לקחת בחשבון בנקיטת אמצעי הביטחון המתאימים (סעיף 32). חובת אבטחת המידע ב-GDPR לוקחת בחשבון את "מצב האמנות, עלויות היישום והאופי, ההיקף,	ההגדרה מתייחסת לאבטחה (Security and integrity) וכוללת שלושה היבטים – א. קיומן של רשתות או מערכות מידע לאיתור אירועי אבטחה המסכנים את הזמינות, האותנטיות, השלמות והסודיות של המידע האישי המאוחסן או המועבר.

הגדרה	ההסדר הישראלי	GDPR	CCPA
		ההקשר ומטרות העיבוד, כמו גם את הסיכון של סבירות וחומרה משתנות לזכויות וחירויות של אנשים טבעיים". לפיכך, יינקטו "אמצעים טכניים וארגוניים מתאימים להבטחת רמת אבטחה המתאימה לסיכון" מוזכרים מספר אמצעים, שאינם מהווים רשימה ממצה - א. פסאודונימיזציה והצפנה; ב. הבטחת סודיות, שלמות, זמינות וחוסן של מערכות ושירותים; ג. היכולת לשחזר זמינות וגישה באירוע פיזי או טכני; ד. תהליך בדיקה מתמשך להערכת אמצעים טכניים וארגוניים להבטחת האבטחה.	ב. היכולת לזהות אירועי אבטחה, להתנגד לפעולות זדוניות, מטעות, הונאה או בלתי חוקיות ולסייע בהעמדה לדין של האחראים. ג. היכולת להבטיח בטיחות פיזית לאנשים. ((ac)1798.140)
דיוור (שיווק) ישיר	"פנייה אישית לאדם, בהתבסס על השתייכותו לקבוצת אוכלוסין, שנקבעה על פי אפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע".	אין הגדרה של המונח. קיימת התייחסות לזכות להתנגד לעיבוד אובייקטים למטרות שיווק ישיר (direct marketing) כולל יצירת פרופילים, בין אם ביחס לעיבוד ראשוני או נוסף, בכל עת וללא תשלום (סעיף 21).	"פרסום התנהגותי חוצה הקשרים" (Cross-context behavioral advertising) פירוש מיקוד הפרסום לצרכן בהתבסס על המידע האישי של הצרכן המתקבל מפעילות הצרכן בין עסקים, אתרי אינטרנט, יישומים או שירותים בעלי מיתוג מובהק, למעט העסק, אתר האינטרנט, היישום או השירות הממותגים באופן מובהק שעמם הצרכן מקיים אינטראקציה במכוון.

הגדרה	ההסדר הישראלי	GDPR	CCPA
שירותי דיוור ישיר	"מתן שירותי דיוור ישיר לאחרים בדרך של העברת רשימות, מדבקות או נתונים בכל אמצעי שהוא".	אין התייחסות ייחודית לשירותי דיוור ישיר.	Data Broker (מתווך מידע) נדרש להירשם לפי החוק בקליפורניה. ההגדרה של מתווך מידע היא: "עסק האוסף ומוכר ביודעין לצדדים שלישיים מידע אישי של צרכן שאין לעסק קשר ישיר עמו." (1798.99.82(c)). קיימים חריגים להגדרה לגופים שחויבו על פי דין לפעול באופן האמור (כגון חברות דירוגי אשראי).

4 - צמצום היקף דרישת הרישום

התיקון מבקש לצמצם את דרישת הרישום הקיימת לשני מקרים (סעיף 8א(א)(1)) –

- סוחרים במידע, ככל שיש במאגר המידע יותר מ-10,000 אנשים במאגר.
- רשות ציבורית, ביחס לכל מאגר מידע שברשותה, אלא אם כן המידע נוגע לעובדי רשות ציבורית בלבד.

התפיסה המיושנת הקיימת בחוק, המשקפת מצב שבו קודם יש רישום, ורק אחר כך השימוש חוקי, נשמרת גם היא בתיקון. עם זאת, התיקון צמצם את הזמן בין רישום מאגר המידע לבין האפשרות להקמתו ל-60 יום (במקום 90) (סעיף 8א(א)(2)).

בעידן שבו מאגר מידע נתונים מוקם בשבריר שנייה, הוראה זו אינה ישימה במקרים רבים. לדוגמה, נניח שרשות ממשלתית מארגנת יום מודעות לאוכלוסייה בעלת צרכים מיוחדים, שאינם עובדי מדינה. עובד המדינה האחראי על ארגון היום מבקש למלא את פרטי המשתתפים (שאינם עובדי הגוף הציבורי) בטבלת אקסל. על פי הוראות התיקון, אם לא הגיש בקשה לרישום וחלפו 60 יום או אם לא ניתנה לו הרשאה להקים את מאגר המידע (טבלת אקסל), הוא אינו רשאי לערוך את הרשימה משום שמדובר במאגר שבעל השליטה בו הוא רשות ציבורית, והנתונים אינם על עובדיו.

בנוסף לחובת הרישום, חלה חובת הודעה על כל מאגר מידע המכיל מידע בעל רגישות מיוחדות שיש בו מידע על מעל 100,000 אנשים. מאגר כאמור נדרש לשלוח הודעה לרשם בתוך 30 ימים מיום שהתקיים התנאי שבשלו הוא חייב להודיע על כך לרשות (סעיף 8א(א)(ב)).

ל-GDPR אין דרישת רישום כלל. ב-CPPA, קיימת דרישה לרישום עסקים הפועלים כסוחר נתונים. ההסדר קובע כי סוחר נתונים יירשמו עד 31 בינואר של השנה שבה הפכו למתווכים ברשות הגנת הפרטיות של קליפורניה (סעיף 1798.99.82). יש לציין כי הסדר זה אינו כרוך ברישום מלבתיחילה כתנאי להקמת מאגר המידע, כפי שהוא נשמר בהסדר הישראלי.

למידע נוסף על הסדרי רישום בעולם, ראו [מחקר](#) שנערך במכון בנושא השוואת הסדרים בחקיקת הגנת הפרטיות (ינואר 2022).

5 - פיצוי ללא הוכחת נזק (פיצויים לדוגמא)

על פי הדין הקיים, ניתן להגיש תביעה אזרחית ולתבוע פיצויים ללא הוכחת נזק (סעיף 29א(ב)) בגין ביצוע עוולה אזרחית של פגיעה בפרטיות. עוולות אלו מתייחסות לפגיעה בפרטיות על פי אחד המקרים המתוארים בסעיף 2 לחוק, אשר כולם נוגעים לפגיעה ב"פרטיות הקלאסית" (privacy) ולא להפרה של הוראות החוק הנוגעות להגנת המידע. על פי סקירת המכון הישראלי למדיניות טכנולוגיה לגבי [על עשור של פסקי דין אזרחיים בנושא הגנת הפרטיות האזרחית](#) (ינואר 2023), מתוך 293 פסקי דין שניתנו בגין עוולה של פגיעה בפרטיות, כל התובעים למעט אחד תבעו פיצויים ללא הוכחת נזק. לפיכך, ניתן להניח כי התיקון צפוי לעודד הגשת תביעות אזרחיות בגין הפרת הוראות הגנת המידע.

התיקון מאפשר תביעות פיצויים בהליך אזרחי, ללא הוכחת נזק, בסכום שלא יעלה על 10,000 ₪ לכל הפרה (סעיף 15א). סוג ההפרות בגין ניתן להגיש תביעה כזו כולל:

- א. אי רישום מאגר מידע, ובלבד שהתובע פנה לבעל השליטה בדרישה לרשום את המאגר וחלפו 90 יום והמאגר לא נרשם;
- ב. אי מתן הודעה כנדרש (יש לתת לבעל השליטה את האפשרות לתקן תוך 30 יום);
- ג. אי מימוש זכות העיון או התיקון;
- ד. אי יידוע ראש הרשות על קבלת מידע דרך קבע בין גופים ציבוריים (יש לתת התראה של 30 יום מראש לפני הגשת התביעה).

בחוקים האירופי והקליפורני, פיצוי אינו אפשרי ללא הוכחת נזק.

6 - התיקון מחייב מינוי קציני הגנת מידע במקרים ספציפיים

התיקון מחייב מינוי ממונה הגנת מידע (DPO) במקרים מסוימים (סעיף 17ב1). החובה חלה על הגורמים הבאים:

- א. חייבים ברישום (סוחר מידע וגופים ציבוריים);
- ב. מאגרי מידע שדרך פעילותם הוא ניטור ומעקב, כגון חברות סלולר;
- ג. מאגרי מידע שעיסוקם העיקרי הוא עיבוד מידע בעל רגישות מיוחדת, כגון קופות חולים;

תפקידו של הממונה על הפרטיות לפעול ל"הבטחת קיום הוראות החוק". פעילות זו חייבת להיעשות על ידי הפיכתו לסמכות מקצועית ומרכז ידע. בנוסף, על הממונה לפעול לביצוע הדרכות בארגון, לקבוע תכנית בקרה, לתת הצעות לתיקון ליקויים בשטח ולוודא את קיומו של נוהל אבטחת מידע ומסמך הגדרות מאגר המידע הנדרש על פי [תקנות הפרטיות](#) (אבטחת המידע), תשע"ז-2017 (להלן – תקנות אבטחת המידע), לפעול בארגון למימוש זכויות נושאי מידע, ולהיות איש הקשר של הארגון עם הרשות.

על הממונה להיות כפוף למנכ"ל או למי מטעמו, ועל הארגון לוודא כי לממונה יהיו המשאבים והמעורבות בארגון הנדרשים למילוי תפקידו.

כפי שצוין, תפקיד של ממונה על הגנת הפרטיות, קיים גם ב-GDPR הקובע חובת מינוי DPO - Data Protection Officer בשורה של ארגונים, בדומה לחובה הקיימת בתיקון (למעט ביחס לסוחרים במידע).

עם זאת, ישנם מספר שינויים מהותיים בין ההסדרים –

שדרות רוטשילד 74-76, תל אביב-יפו, 6521401

משרדים: +972 50 6217710

www.techpolicy.org.il | rdvash@techpolicy.org.il

1. ההסדר האירופי קובע עצמאות מקצועית של ה-DPO וכי לא יקבל כל הוראות ביחס למילוי משימותיו. כמו כן נקבע כי חל איסור על פיטוריו או ענישתו בשל ביצוע תפקידו (סעיף 38(3));
 2. הממונה גם מיעץ בתסקיר ההשפעה על הפרטיות בעת הכנסת רכיבים חדשים שיש בהם לפגוע בפרטיות, ומפקח על ביצוע תסקיר הפרטיות (סעיף 39(1)(c)). בישראל אין עדיין חובה לבצע הערכה כאמור, אולם השונות מחדדת את ההבדל בין ממונה על פרטיות המסייע ביישום הוראות חוק שיש בהן הוראות מהותיות המגדירות את המסגרת המקצועית, לבין ממונה שהתוכן המקצועי בסופו של דבר מאוד מצומצם (הסכמה, מתן הודעה, רישום ככל שרלוונטי, ומתן זכות עיון ותיקון);
 3. בהסדר האירופי הממונה אינו רק איש קשר עם הרשות, אלא מחויב לשתף עמה פעולה (סעיף 39(1)(d)).
- בהסדר הקליפורני אין בעל תפקיד דומה להגנת הפרטיות.

7 - הסמכויות של הרשות להגנת הפרטיות השתנו באופן משמעותי

7.1 - הגדרת הרשות להגנת הפרטיות ותפקידיה

הרשות להגנת הפרטיות הוקמה בהחלטת ממשלה בינואר 2006, בה נקבע כי תוקם רשות משפטית לטכנולוגית מידע והגנת הפרטיות, שתאחד¹ את רשם מאגרי המידע, רשם נתוני אשראי² ורשם חתימה אלקטרונית תחת גוף אחד. כן נקבע דרך המינוי של ראש הרשות שיהיה אחראי לניהול מערך הרישום, הפיקוח והאכיפה המנהלית של שלושת הרשמים (החלטה 4660).

כחלק מניסיונה של ישראל לשמר את מעמד התאימות האירופאית, ולאחר שהבטחותיה לאיחוד האירופי לעגן את מעמד הרשות בחקיקה לא התקיימו, הוחלט להסדיר את מעמד הרשות בהחלטת ממשלה מאוקטובר 2022 (החלטה מספר 1890).

בהחלטה זו נקבע כי הרשות תהיה עצמאית במילוי תפקידיה וכי תקציב הרשות ינוהל בנפרד במסגרת תקציב משרד המשפטים (סעיף 1(ב) להחלטת הממשלה). בנוסף, נקבעו תנאי כשירות למי שעשוי להיות ראש הרשות, שאינם כרוכים בניסיון או השכלה קונקרטיים בתחום הפרטיות, הגנת המידע או הטכנולוגיה (סעיף 3 להחלטת הממשלה).

ההחלטה קובעת כי תפקידי הרשות יכללו את אלה (סעיף 2 להחלטת הממשלה):

- א. פיקוח על קיום הוראות החוק ביחס למאגרי מידע;
- ב. חקירת חשדות לביצוע עבירות לפי החוק ביחס למאגרי מידע בהתאם לסמכויות הרשות;
- ג. העלאת המודעות באמצעות חינוך, הדרכה והסברה;
- ד. טיפול בפניות הציבור;
- ה. פיתוח ויישום "תכניות מקצועיות והכשרות בתחומי פעילותה";
- ו. קידום קשרים במישור הבינלאומי עם גופים מקבילים;
- ז. ביצוע סמכויות רשם הגורמים המאשרים לפי חוק חתימה אלקטרונית.

¹ מאז שונה שם הרשות פעמיים בהחלטות ממשלה עד לשמה הנוכחי "הרשות להגנת הפרטיות". החלטה 4820 מיוני 2012, והחלטה 3019 מספטמבר 2017.

² מאז החלטת הממשלה האמורה הועבר תחום זה בחקיקה לפיקוח בנק ישראל.

נוסח הצעת החוק, כפי שהוגש על ידי הממשלה, לא הציע להסדיר את מעמדה של הרשות אלא רק לשנות את שם הרגולטור. הרצון להסדיר את הגדרת הרשות ותפקידה עלה במהלך הדיונים על ההצעה. נקבע כי הגדרת הרשות תתייחס לארבע החלטות הממשלה הרלוונטיות כאשר נוסח ההחלטה 1890 הוצג בנספח הראשון.

זוהי דרך ניסוח שאינה מקובלת בדרך כלל בחקיקה הישראלית, הן משום שבהסדרת מעמדה של רשות ציבורית נהוג להגדיר אותה בחוק, והן משום שלא נהוג להעתיק החלטות ממשלה כלשונן לחוק. במישור המהותי נוצר מצב שבו לכאורה החוק מסתמך על החלטת ממשלה (פעולה ביצועית), אך בפועל, אם הממשלה תבקש לשנות את ההחלטה, יידרש תיקון חקיקה מקביל, וכל עוד לא יתקן, החוק יגבר.

7.2 - סמכויות הרשות

עיקרו של החוק עוסק בסמכויות המוקנות לרשות למלא את תפקידה. סמכויות אלה כוללות את אלה:

א. **חוות דעת מקדמית** – אפשרות של בעל שליטה או מחזיק לבקש חוות דעת מקדמית (pre-ruling). הרשות רשאית לפרסם חוות דעת אלה המזהות את הגורם המבקש בשמו (בהסכמת המבקש) או בעילום שם (ללא הסכמתו) (סעיף 217ט);

ב. **פיקוח רוחבי** – הרשות רשאית לבצע פיקוח רוחבי באמצעות שליחת שאלונים לגורמים הרלוונטיים. בביצוע פיקוח רוחבי, אדם שאינו עובד מדינה ("מומחה חיצוני") יכול לסייע, אך שיקול הדעת יישאר רק בידי עובד מדינה (סעיף 23ז). המומחה החיצוני רשאי לדרוש גם מסמכים וידיעות ובלבד שניתן אישור מראש של מפקח (סעיף 23ח(ו)).

ג. **סמכויות פיקוח** (סעיף 23י) – על פי התיקון, הסמכויות מחייבות את הגוף המפוקח להזדהות בפני הממונה, למסור למפקח כל מסמך או מידע מבוקש, לאפשר את כניסתו של המפקח לכל מקום שאינו בית פרטי, להעביר למפקח נתוני מערכת (כגון לוגים) ומידע אישי מדגמי. ביחס לשני הנתונים האחרונים, על הרשות למחוק אותם ברגע שאינם נדרשים, ולא יאוחר משבע שנים עבור נתוני המערכת ושלוש שנים עבור מידע אישי מדגמי, אלא אם כן הם נדרשים לניהול הליכים.

ד. **בירור מינהלי** (סעיף 23יב) – מקום בו קיים חשד לביצוע הפרה לפי החוק שראש הרשות רשאי להורות על הפסקתם, ניתנות למפקח סמכויות נוספות, לרבות אפשרות לבקש צו חיפוש, תפיסה וצו חדירה למחשב (סעיף 23יד).

ה. **סמכויות חקירה** – ראש הרשות רשאי להסמיך עובדי מדינה כחוקרי עבירות פליליות מטעם הרשות. לחוקרים תהיה סמכות לחקור אנשים רלוונטיים, לתפוס חפץ הקשור לעבירה, לבקש צו בית משפט לתפוס ולחדור לחומר מחשב, לעכב אדם, לדרוש ממנו להתלוות לחוקר, או לזמן אותו לחקירה במשרדי הרשות (סעיפים 23נ-23נא).

למרות סמכויות הפיקוח הנרחבות של הרשות, ישנם מספר מקרים חריגים הנוגעים לאופן ביצוע הפיקוח על ידי הרשות:

א. הפיקוח על גופים הכפופים להנחיות בטחון של מערך הסייבר ייעשה בהתאם לנוהל שיגובש בין הרשות לבין מערך הסייבר הלאומי (סעיף 23ט);

ב. לגבי רשויות ייעודיות לביטחון, כמו המשטרה, צה"ל, השב"כ, המוסד ועוד כמה רשויות ביטחון המפורטות בסעיף, שיטת הפיקוח תהיה שונה. בסמכויות אלה ימונה ממונה פרטיות מבין העובדים, אשר ידווח לראש רשות הביטחון ויונחה על ידי ראש הרשות לפרטיות (סעיף 23בא). המפקח באותה רשות יבצע פעולות על פי תכנית שנתית שתאושר על ידי ראש הגוף הביטחוני וראש הרשות ויהיו לו אותן סמכויות כמו למפקח על הרשות להגנת הפרטיות (סעיפים 23בב-23כג). ראש הרשות להגנת הפרטיות רשאי להורות לממונה לבצע פעולות מטעמו, או להפעיל אמצעי אכיפה מינהליים או פליליים במקום שעלו חשדות להפרה או עבירה (סעיף 23כד);

ג. הסדר מיוחד לתקופת בחירות – הפעלת סמכויות הרשות ביחס למאגרי מידע של מפלגות או של מועמדים לבחירות ברשויות המקומיות בתקופת בחירות יכולה להיעשות רק אם התקבל אישור מוקדם מיו"ר ועדת הבחירות המרכזית או האזורית, לפי העניין (סעיף 23נט).

בנוסף לסמכויות הרשות, עליה להגיש דו"ח שנתי לוועדת החוקה, חוק ומשפט (סעיף 17ט3). החוק מפרט את תוכן הדו"ח ומחייב כי הדו"ח יכלול פילוח לפי גופים ממשלתיים, ציבוריים ופרטיים. לגבי כל אחד מהם על הרשות לדווח אודות: מס' חוזר מקדמיות; רישום, הודעות, תלונות, פעולות פיקוח, בירורים מנהליים, צווי חיפוש ותפיסה, תלונות על מומחה חיצוני, הוראות להפסקת הפרה, התראות מינהליות, כתב התחייבות או ערבון שנדרשו, עיצומים, מימוש זכות הטיעון, הודעה על חיוב ללא עיצום, הפחתת עיצום, הפרות חוזרות, הפרות נמשכות, ערעורים על ראש הרשות להטלת עיצום כספי, הליכי אכיפה פלילית, בקשה לחקירת מפלגות, ונתוני תיקים לפיצוי ללא הוכחת נזק.

ה-GDPR דורש כי הרשות המפקחת ("supervisory authority"), תהיה ישות עצמאית (סעיף 4(21)) וסעיף 52). מעניין לציין כי החקיקה האירופית מדגישה כי תפקידה של הרשות המפקחת הוא לאכוף את הוראות החקיקה הן כדי להגן על זכויותיהם של נושאי המידע, והן כדי לאפשר זרימה חופשית של מידע (סעיף 51(1)). הצורך ביצירת משטר משפטי המאפשר זרימה חופשית של נתונים תוך שמירה על זכויות יסוד שזור בחקיקה האירופית והיעדרו בולט בתיקון הישראלי. משמעות הדבר היא שגם ביישום כלי האכיפה הנתונים בידי הרשות הישראלית, היא אינה מחויבת לאיזון שבו רשות אירופית מחויבת לאפשר זרימה חופשית של מידע אישי כערך שיש להגן עליו, כל עוד הוא מתקיים במסגרות שנקבעו.

החוק האירופי מונה את המשימות המוטלות על הרשות המפקחת (סעיף 57) ואת סמכויותיה (סעיף 58). ראוי לציין כי התפקידים הבאים שהוקצו לרשות המפקחת ב-GDPR נעדרים מתיקון 13:

- א. להיות גוף מייצג לממשלה ולמוסדות ציבוריים אחרים ביחס לחקיקה ולהחלטות מנהליות בתחום הגנת המידע האישי;
- ב. לספק מידע לכל נושאי המידע, לפי בקשה, על זכויותיהם;
- ג. לעקוב אחר התפתחויות רלוונטיות, במיוחד בנושאים של פיתוח טכנולוגיות מידע ותקשורת, ופרקטיקות מסחריות;
- ד. לעודד ניסוח קודי התנהגות בהתאם לתקנה האירופית (סעיף 40), ולבחון קודים כאלה תוך מתן חוות דעת עליהם.

באשר לסמכויות המוקנות לרשויות הפיקוח האירופיות בהשוואה לאלה של הרשות הישראלית, יש לציין כי הסמכות לנהל הליכים פליליים נעדרת מה-GDPR. בהקשר זה יש לציין כי ה-GDPR אינו קובע עבירות בהסדר ומותיר את קביעתן למדינות (סעיף 84). בנוסף, החוק הישראלי חסר פירוט של הסמכויות המוקנות לרשות המפקחת לסייע לבעלי השליטה לקיים את הוראות החוק (לא כענישה אלא כפעולות עזר מקדימות), כגון ניסוח כללי אתיקה, סעיפים מקובלים בחוזים אחידים וכיו"ב (סעיף 58(3)).

הסוכנות להגנת מידע אישי בקליפורניה (להלן – הסוכנות) הוקמה על ידי תיקון לחוק בקליפורניה בשנת 2020. הסוכנות מנוהלת על ידי מועצת מנהלים בת 5 חברים. חברי הדירקטוריון חייבים להיות בעלי מומחיות בפרטיות, טכנולוגיה והגנת הצרכן (סעיף 1798.199.10) וממונים על ידי ארבעה גופים שונים (אחד ממנה שני נציגים, והשאר ממנים נציג אחד כל אחד). תפקידי הסוכנות דומים לאלה של רשויות הפיקוח באיחוד האירופי, עם שינויים קלים, בתוספת חובה להתקין תקנות הנדרשות בחקיקה (סעיף 1798.199.40), וכן סקירה וחלוקה של מענקים מקרן ייעודית שהוקמה להגנת מידע אישי החוק (סעיף 1798.199.40(k)). הסוכנות גם אינה יכולה לנהל חקירות פליליות. התובע הכללי של קליפורניה מוסמך בנפרד לאכוף את החוק.

7.3 - אמצעי אכיפה מנהליים

החוק פירט מספר אמצעי אכיפה מנהליים שניתנו לראש הרשות או למי שהוסמך מטעמו, שניתן להטיל על גוף שהפר את הוראות החוק בתחום הגנת המידע האישי (מאגרי מידע).

הערה מקדמית לגבי הפרקטיקה החקיקתית שיצר התיקון: הרגולציה מחייבת קביעה נורמטיבית של התנהגות ראויה על מנת להסדיר את ההתנהגות הרצויה. המחוקק נוהג להצמיד ענישה (מנהלית או פלילית) להוראות מסוימות או לאפשר הגשת תביעה אזרחית בגין הפרתן. כלומר, לאחר שהחובה בסעיף נוסחה באופן ברור, יציין המחוקק כי הפרת הוראות מאותו סעיף עלולה להוביל לסנקציות מינהליות או פליליות. אין זה נוהג שכיח במשפט הישראלי לקבוע הפרות בסעיף נפרד אחר.

בתיקון זה, ובשונה מהמקובל, החליט המחוקק למנות מחדש את כל ההפרות. מעבר לסרבול ולקושי בהבנת הוראות החוק, הדבר עלול ליצור פערים בין הנוסחים השונים במיוחד במקום בו יהיו תיקוני חקיקה עתידיים, ולא תהיה הקפדה על תיקון כל המקומות הנדרשים בחוק. יש לציין כי כבר כיום קיימים פערים בין הוראות מסוימות לבין ההפרות שהוגדרו מחדש. כך למשל, תקנות אבטחת המידע מחייבות שמירת לוגים למשך שנתיים (תקנה 17), אך ההפרה המוגדרת בפרט (25) לתוספת השלישית מאפשרת הטלת עיצום כספי אם הלוגים לא נשמרים למשך שנה בלבד. כלומר, מי ששמר לוגים ל-18 חודשים הפר את הוראת התקנות אך לא ניתן יהיה להטיל עליו עיצום כספי, דבר המעודד את בעלי השליטה להתכנס לשנת שימור. אם המחוקק סבור כי הדרישה המהותית שגויה, מומלץ להציע תיקון להוראת הוודאות המשפטית.

להלן אמצעי האכיפה שהוענקו לרשות להגנת הפרטיות -

א. **הפסקת הפרה** – הודעה של ראש הרשות, לאחר שימוע, כי בוצעה הפרה וכי יש לתקנה. ההפרות שבגינן ניתן לקבוע הפסקת הפרה נוגעות להפרות הבאות: שימוש במידע שלא למטרה לשמה נמסר, עיבוד מידע בניגוד לדין, עיבוד שלא בהתאם לתקנות הגישור וליקויים במינורי או בתפקוד הממונה על הגנת הפרטיות (סעיף 23(כה)).

ב. **עיצומים כספיים** – ראש הרשות או מי מטעמו רשאי להורות על הטלת עיצומים כספיים בהחלטה מינהלית בשל הפרת הוראות החוק (סעיף 23כו). בניגוד להצעת החוק הממשלתית, שקבעה רמת ענישה סכמתית מסוימת לגבי גודל המאגר, מידת רגישות הנתונים וסוג ההפרה, החוק שאישרה הכנסת יצר חלוקה לתשעה חישובים שונים לגבי גובה העיצום הכספי. לפירוט החלוקה האמורה לתשעת החישובים השונים ראו נספח למסמך.

ג. **התראה מינהלית** - ראש הרשות רשאי למסור התראה מינהלית במקום עיצום כספי. על ההתראה לציין את מהות ההפרה ולהזהיר כי אי תיקונה עלול להוביל להטלת עיצום כספי בגין הפרה חוזרת או נמשכת (סעיף 23לז). בקשה לביטול ההתראה ניתן להגיש בתוך 45 יום (סעיף 23לח).

ד. **התחייבות להמנע מהפרה** - ראש הרשות רשאי לדרוש כתב התחייבות להימנע מההפרה המזוהה, כחלופה לעיצום כספי. המפר יפקיד עירבון ויתחייב שלא לבצע את ההפרה בתוך תקופה שתיקבע, שלא תעלה על שנתיים. ראש הרשות רשאי להוסיף תנאים נוספים לתקופת ההתחייבות כדי להקטין את הנזק שנגרם כתוצאה מההפרה או למנוע את הישנותה (סעיף 23לט-23מ). הפרת התחייבות תיחשב כהפרה חוזרת או נמשכת (סעיף 23מב).

ה. **צו הפסקה שיפוטי (סעיף 23מט)** - ראש הרשות רשאי לפנות לבית המשפט לעניינים צו להפסקת עיבוד מידע או למחיקת מידע כאשר קיים יסוד סביר להניח כי בוצעה הפרה או כי עומדת להתבצע הפרה באחד מהמקרים הבאים:

1. שימוש במידע שלא למטרה לשמה נמסר;
2. שימוש במידע שלא למטרות החוקיות של המאגר או חריגה מהרשאות של בעל השליטה במידע;
3. כשל אבטחת מידע;
4. מסירת מידע מגוף ציבורי שלא על פי דין.

כדי לתת את הצו, על בית המשפט להשתכנע כי –

- א. הפרה מבוצעת או עומדת להתבצע והיא בעלת חומרה מספקת המצדיקה מתן צו;
- ב. אין אמצעי לפגיעה פחותה כדי למנוע את ההפרה;
- ג. הנזק שעלול להיגרם כתוצאה מההפרה גדול מהנזק שעלול להיגרם עקב מתן הצו השיפוטי.

ככל שהצו יינתן במעמד צד אחד, הוא לא יעלה על 48 שעות ולא יכלול צו למחיקת המידע.

7.4 - הוראות פרוצדורליות לעניין הטלת עיצומים כספיים

התיקון מסדיר גם את הליך הטלת העיצום הכספי. בין היתר נקבע כי:

א. ראש הרשות נדרש להודיע על כוונת חיוב (סעיף 23כז), ולתת זכות טיעון טרם הטלת העיצום (סעיף 23כח).

ב. ראש הרשות רשאי להפחית את סכום העיצום (סעיף 23כט) מטעמים המפורטים בתוספת החמישית (כגון אי קיומן של הפרות קודמות, נקיטת פעולות לאי השנות ההפרה שנית, מינוי ממונה פרטיות

היכן שנדרש, נסיבות אישיות וכיו"ב) וסכום ההפחתה לא יעלה על 70% אלא אם סכום העיצום עולה על 5% ממחזור העסקאות. בכל מקרה, החלטת ראש הרשות תינתן בכתב ובאופן מנומק.

ג. בהפרה נמשכת תתווסף מאית מהסכום שהוטל עבור כל יום נוסף שמבוצעת ההפרה. בהפרה חוזרת שבוצעה תוך שנתיים מההפרה הראשונה, יוכפל הסכום (סעיף 23ל).

התיקון מתייחס גם לעדכון סכומי העיצום (סעיף 23לב); תשלום העיצום בתוך 45 ימים ממועד מסירת דרישת התשלום (סעיף 23לג); תשלום ריבית נוספת ודמי פיגורים (סעיף 23לד); ודרך גביית החובות (סעיף 23לה).

בנוסף, נקבעו ההוראות הבאות -

- א. אסור להטיל יותר מעיצום כספי אחד על פעולה אחת (סעיף 23מד).
- ב. ערעור על הליכי אכיפה ניתן להגיש לבית משפט השלום בתוך 45 ימים (סעיף 23מה).
- ג. על ראש הרשות לפרסם, לאחר שאיפשר למפר להציג את טענותיו, את העיצום הכספי שהוטל ופרטים הנוגעים אליו (לרבות שם המפר). הפרסום באתר האינטרנט של הרשות יישאר שנתיים ליחיד וארבע שנים לתאגיד (סעיף 23מו).

ה-GDPR מצוין כי לכל רשות פיקוח חייבת להיות הסמכות, הקבועה בחקיקה הלאומית, להטיל עיצומים כספיים. סנקציות אלה מוגבלות בהפרות מסוימות המנויות בתקנה ל-10 מיליון אירו או 2% מהמחזור הכולל של שנת הכספים הקודמת ובעבירות אחרות ל-20 מיליון אירו או 4% מהמחזור הכולל של שנת הכספים הקודמת (הגבוה מבניהם) (סעיף 83). ההוראה לסנקציה על הפרות בדין הישראלי בשיעור של 5% מהמחזור אינה מבדילה לפי סוג ההפרה ועולה על התקרה האירופית המקסימלית.

החוק בקליפורניה קובע קנס מנהלי של 2,500 דולר על כל הפרה. אם ההפרה בוצעה בכוונת זדון או מעורבים בה קטינים מזוהים, העונש עולה ל-7,500 דולר (סעיף 1798.155). כספים אלה מועברים לקרן פרטיות הצרכן כדי לחזק את ההגנה על הפרטיות. הרשות שוקלת את רמת שיתוף הפעולה המתקבלת מהמפר בעת קביעת סכום הסנקציה (סעיף 1798.199.100).

8 - התיקונים מציגים עבירות פליליות הקשורות לעיבוד נתונים אישיים

התיקון קובע כי פעולות מסוימות יוגדרו כעבירות פליליות, שהרשות תהיה מוסמכת לחקור. העבירות החדשות בתיקון כוללות את אלה:

- א. הפרעה לראש הרשות, לחוקר או למפקח מטעמים במילוי תפקידם (שישה חודשי מאסר) (סעיף 23נג).
- ב. מסירת פרטים לא נכונים בבקשה לרישום מאגר מידע, בהודעה על שינוי פרטים, או בתגובה למפקח ולמומחה חיצוני מטעם הרשות, וזאת בכוונה להטעות אותם (מאסר שנתיים) (סעיף 23נד).
- ג. עיבוד מידע ללא הרשאה מבעל השליטה (סעיף 23נה).
- ד. מסירת נתונים לא נכונים בהודעה לפי סעיף 11 כדי להטעות את האדם בנוגע למסירת המידע האישי (3 שנים) (סעיף 23נו).

ה. גילוי בלתי חוקי של מידע אישי מרשות ציבורית לצד אחר (3 שנים) (סעיף 23נז).

שדרות רוטשילד 74-76, תל אביב-יפו, 6521401

משרדים: + 972 50 6217710

www.techpolicy.org.il | rdvash@techpolicy.org.il

כאמור, התקנות האירופיות הקליפורניות אינן כוללות הוראות פליליות, אם כי ב-GDPR יש ציפייה שכל מדינה תגדיר עבירות בחקיקה המקומית.

9 - תיקונים שונים: משינוי הגבלת המטרה, להרחבת דרישת ההודעה

9.1 - הגבלת מטרה

התיקון ביקש "להקשיח" את הוראות החוק המחייבות שימוש במידע רק למטרה שלשמה נמסרה המידע. הנוסח המתוקן קובע כי "לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין" (סעיף 8(ב)). החוק אינו מפרט היכן מתקבלת קביעה כזו ומי קובע את הדין הרלוונטי כאשר העוגן המשפטי היחיד לשימוש במידע הוא הסכמה.

בנוסף, מובהר כי לא יעבד אדם מידע אישי ללא הרשאה מבעל השליטה ויש לפעול על פיה (סעיף 8(ג)), וכן שלא ניתן לעבד מידע שהתקבל בניגוד להוראות החוק או כל דין אחר (סעיף 8(ד)(1)).

הרגולציה האירופית שונה מהחוק הישראלי. ה-GDPR קובע בסיסים משפטיים לעיבוד מידע (סעיף 6), המפרטים מספר חלופות, כולל הסכמה, צורך לקיים חוזה, חובה משפטית, אינטרס ציבורי ועוד. לפיכך, החוק בנוגע למטרות עיבוד נתונים חוקיות ברור יותר ב-GDPR. בנוסף, העקרונות הכלליים של עיבוד מידע המנויים בסעיף 5 של GDPR קובעים, בין היתר, כי יש לאסוף את המידע "למטרות מוגדרות, מפורשות ולגיטימיות" ועיבוד המידע צריך שיהיה תואם למטרות אלה, אלא אם העיבוד מתבצע למטרות "ארכיון למען האינטרס הציבורי, למטרות מחקר מדעי או היסטורי או למטרות סטטיסטיות".

במילים אחרות, בניגוד לניסוח המעורפל שנבחר בתיקון, הרגולציה של האיחוד האירופי מפרטת את המסגרת המשפטית לסוג המטרות שלשמן ניתן להתיר עיבוד מידע, מגדירה כי יש לקבוע במפורש את המטרות ולפעול לפיהן, ואף מפרטת מקרים בהם מותר לעבד מידע שלא במסגרת המטרות. יצוין כי ה-GDPR קובע כי על חקיקת המדינה להתייחס למספר סוגיות ולקבוע את המסגרות הברורות יותר לגביהן, ביניהן ביחס למגבלת התכלית (סעיף 6(3)(b)).

CCPA דורש שכל עסק יקבע את מטרתו העסקית ("Business purpose") (סעיף 1798.140(e)). החוק קובע כי השימוש במידע האישי צריך להיות הכרחי ומידתי באופן סביר כדי להשיג את המטרות שלשמן המידע האישי נאסף או עובד, או למטרה גלויה אחרת התואמת את ההקשר שבו נאסף המידע האישי. החוק בקליפורניה קובע מטרות עסקיות המאפשרות עיבוד מידע אישי, כולל ביקורת אינטראקציות עם צרכנים, אבטחה, איתור באגים וכו'. תקנות הסוכנות יצרו דרישות מזעור נתונים מוגברות, וקבעו כי איסוף הנתונים והשימוש בהם צריכים לעלות בקנה אחד עם "הציפיות הסבירות" של המשתמשים (תקנות CCPA, סעיף 7002).

העובדה שבמשפט הישראלי העוגן היחיד לעיבוד מידע נותר הסכמה, ללא הגדרת תכליות משפטיות לעיבוד מידע, עלולה ליצור קשיים מעשיים לעיבוד כדין של נתונים אישיים לצורך אינטרסים לגיטימיים, כמו הבטחת אבטחת מערכות או מאבק בהונאות, שכן הוא אינו רואה בעיבוד לגיטימי כמקובל במשטרים משפטיים אחרים. נכון למועד זה, התיקון לא הקנה סמכות להטיל סנקציה מינהלית בגין הפרה על סעיף 8(ב) שעניינו הגבלת מטרה, אלא רק כאשר קיימת חריגה מההרשאה שניתנה או כאשר הנתונים משמשים למטרה אחרת מזו שלשמה נמסרו (הכוונה לפגיעה בסעיף 2(9) שעניינו הגבלת התכלית בדבר פגיעה בפרטיות "הקלאסית").

הדרישה החוקית הנוכחית להודיע לאנשים כאשר הנתונים שלהם נאספים (סעיף 11) תורחב כך שתכלול את החובה למסור את הפרטים הבאים לאדם שממנו מתבקשים הנתונים:

- א. ההשלכות של סירוב לספק מידע;
- ב. שם בעל השליטה ודרכי ההתקשורת איתו;
- ג. קיומה של זכות העיון והמחיקה. בהקשר זה ראוי לציין כי התיקון לא דרש מבעל השליטה לפרט את כל זכויותיו של נושא המידע, דבר שהיה מבטיח כי נושא המידע יקבל מידע על הזכויות העומדות לו גם מכח תקנות הגישור. נושא זה חשוב שבעתיים משום שנושאי המידע אינם יכולים לדעת האם מאגר מידע כפוף לתקנות הגישור, ולכן יכולתם לממש את זכויותיהם פוחתת.

נוסח החוק הישראלי אינו מבחין בין הודעה שנמסרה לאדם שלגביו מתבקשים נתונים לבין אדם שממנו מתבקשים נתונים.³

התקנות האירופיות עושות הבחנה בין פנייה ישירה לאדם (סעיף 13) לבין איסוף נתונים מצד שלישי. כאשר נתונים נאספים מצד אחר, יש להודיע לנושא הנתונים על איסוף הנתונים שלו (סעיף 14). בנוסף למידע הנדרש על פי החוק הישראלי להימסר בהודעה לנושא המידע לפי סעיף 13 של GDPR (מקביל לחוק הישראלי), יש לספק גם את הפרטים הבאים:

- א. פרטי הקשר של הממונה;
- ב. האינטרסים הלגיטימיים של בעל השליטה ככל שהמידע נדרש למימושם;
- ג. נמענים שאליהם מועבר מידע או קטגוריות של נמען כזה, אם ישנם;
- ד. האם המידע מיועד להעברה למדינה שלישית או לארגון בינלאומי ואיזה מנגנון מאפשר העברה כזו;
- ה. תקופת השמירה של המידע או הקריטריונים שלפיהם נקבעת תקופת השמירה;
- ו. שימוש בקבלת החלטות אוטומטית, המשמעות וההשלכות של שימוש כזה.

בנוסף, בעל השליטה נדרש לתת הודעה מוקדמת לפני עיבוד המידע למטרה אחרת, בעוד שעל פי החוק הישראלי, ההודעה ניתנת רק עם איסוף המידע הראשוני.

דרישת ההודעה של CCPA דורשת שהעסק יודיע לנושא הנתונים בעת איסוף המידע האישי או לפניו. במילים אחרות, ההנחה היא כי לא ניתן לאסוף נתונים מהאדם ישירות או מגורם אחר ללא מתן הודעה (סעיף 1798.100). על העסק לכלול בהודעה את המידע הבא:

- א. קטגוריות הנתונים הנאספים (רגילים או רגישים);
- ב. מטרת איסוף הקטגוריות הללו;
- ג. האם הנתונים נמכרים או מועברים לצד שלישי;
- ד. משך הזמן שבו הנתונים יישמרו ובהיעדר זמן מוגדר, הנסיבות שבהן הנתונים עדיין יישמרו.

לכן, למרות הרחבת החוק הישראלי כך שיכלול מידע נוסף שנוסף למתן הודעה, משטרים משפטיים אחרים עדיין יוצרים שקיפות רבה יותר עבור נושא ההודעה. בנוסף, הן GDPR והן CCPA לוקחים בחשבון את המציאות הנוכחית שבה המידע לעתים קרובות לא נאסף מנושא המידע. במסגרת הגנת המידע הישראלית, המבוססת כולה על הסכמה, מצב כזה יוצר פרדוקס: כיצד ניתן לקבל הסכמה אם האדם הנוגע בדבר אינו מודע לכך

³ קיימת עמדה של הרשות (לא הנחייה) בנושא "חובת יידוע במסגרת איסוף ושימוש במידע אישי" קושרת בין סעיף 11 להסכמה, ועל כן רואה את הפנייה ככזו הנעשית לנושא המידע.

שהנתונים שלו נאספים? עם זאת, ברור כי במציאות, מצבים כאלה שבהם עיבוד נתונים אישיים מתרחש ללא הסכמת נושא המידע קיימים (למשל, משוב עמיתים בעבודה או דיווח של מורה על התנהגות תלמידים במערכת ממוחשבת).

9.3 - התיישנות

התיקון מבטל את הכלל המיוחד שקבע את תקופת ההתיישנות על עוולות שנגרמו בשל הפרה של חוק הפרטיות על שנתיים (סעיף 26). במקום זאת, תחול תקופת ההתיישנות הרגילה במשפט הישראלי, העומדת כיום על 7 שנים.

9.4 - אחריות קפידה

התיקון מבטל את העבירות הפליליות הקבועות בסעיף 31א לחוק, שאינן טעונות הוכחת יסוד נפשי ("אחריות קפידה").

9.5 - ביטול ההסמכה לקבוע אגרות

התיקון מבטל את ההוראות בחוק המסמיכות את השר להסדיר את האגרות הכרוכות ברישום מאגר מידע (סעיף 36א). יש לציין כי בפועל לא נגבו אגרות כאלה מאז שנת 2017, אז בוטלו תקנות הגנת הפרטיות (אגרות). התיקון נועד להתאים את ההסדר בחקיקה הראשית למדיניות שנקטה הרשות עם ביטול התקנות האמורות.

הרישום אינו נדרש ב-GDPR, ותשלום של \$400 נגבה ב-CCPA עבור רישום סוחרי נתונים, שנועד לממן את עלות הפעלת מסד הנתונים של מתוכי מידע כאמור.

10 – סיכום

תיקון החקיקה המקיף, שהתקבל ב-5 באוגוסט 2024 וייכנס לתוקף בעוד שנה לאחר פרסומו (ב-14 באוגוסט), הגדיל משמעותית את הסיכון של בעלי שליטה לעשות שימוש במאגר מידע שלא בהתאם לחוק הגנת הפרטיות. בהתחשב בפערים בין החקיקה הישראלית לבין מסגרות משפטיות מובילות אחרות בתחום הפרטיות והגנת המידע בעולם, נראה כי גם מי שהנהיג תוכניות ציות לכללים הנוקשים של ה-GDPR עלול למצוא את עצמו בסיכון לאי ציות לחוק הפרטיות הישראלי החדש.

ברמה המהותית, בשל העוגן המשפטי היחיד של הסכמה לעיבוד חוקי של מידע אישי, לרשות להגנת הפרטיות יש לכאורה מרחב נרחב להדרכה ולפרשנות משפטית כאשר היא מיישמת את החוק. הדבר יוצר מידה מסוימת של אי-ודאות משפטית ומעלה שאלה לגבי האפקטיביות של הגברת הציות לחוק. ניתן להניח כי לפחות בכל הנוגע להטלת העיצומים הכספיים הגבוהים, ובהתחשב בכך שהדין המהותי נותר ברובו כפי שנכתב במקור בשנות השמונים, בתי המשפט ידרשו לספק הבהרות.

נספח

להלן פירוט הרמות השונות של עיצומים כספיים שניתן להטיל בגין ההפרות השונות על פי חוק. הפירוט הוא לפי הסכום הנמוך לגבוה יותר ולא לפי הסדר שבו מופיעות הסנקציות בחקיקה.

א. מכפלה של 2 ש"ח לכל אדם במאגר, ואם במאגר בעל רגישות מיוחדת – 4 ש"ח. אם הסכום נמוך מ-20,000 ש"ח ובמאגר מידע רגיש במיוחד של 40,000 ש"ח ניתן להגדיל את הסכום עד לסכום זה (סעיף 23ב(ד)). להלן פירוט ההפרות בגין ניתן להטיל סנקציה זו:

1. פנייה בלתי מסוימת לקבוצה ללא מתן הודעה לפי סעיף 11;
2. אי מינוי ממונה על אבטחת מידע;
3. אי מינוי ממונה על הגנת הפרטיות;
4. עיבוד מידע אישי במאגר לצורך שירותי דיוור ישיר ללא רישום מקור הנתונים, מועד קבלתו ורישום למי נמסר אוסף הנתונים;
5. רשות ציבורית שלא עורכת רישום על מידע שהועבר על ידה במסגרת ההסדר להעברת מידע בין גופים ציבוריים (סעיף 23ג);
6. בעל השליטה במאגר החייב ברישום שלא תיקן הפרה רלוונטית עליה הורה ראש הרשות. שר המשפטים רשאי להרחיב בצו את האפשרות להטיל עיצום כספי בנסיבות כאמור גם על גופים נוספים המחויבים במינוי ממונה על הפרטיות,

ב. מכפלה של 4 ש"ח לכל אדם הנמצא במאגר, ואם במאגר בעל רגישות מיוחדת – 8 ש"ח. אם הסכום נמוך מ-200,000 ש"ח, ניתן להגדיל את הסכום עד לסכום זה (סעיף 23ב(ה)). להלן פירוט ההפרות בגין ניתן להטיל סנקציה זו:

1. לא הפסיק לבצע הפרה שראש הרשות הכריז עליה של עיבוד מידע שלא כדין, או שלא למטרה שלשמה המידע נמסר;
2. עיבוד מידע אישי במאגר מידע למטרה שאינה כדין;
3. עיבוד מידע ללא הרשאה מבעל השליטה;
4. מסירת מידע מגוף ציבורי שלא במסגרת ההסדר שבפרק ד' להעברת מידע בין גופים ציבוריים.

ג. מכפלה של 50 ש"ח לכל אדם שאליו נעשתה הפנייה או הדרישה, ואם המידע בעל רגישות מיוחדת – 100 ש"ח. אם הסכום נמוך מ-30,000 ש"ח ניתן להגדילו עד לסכום זה (סעיף 23ב(ג)). להלן פירוט ההפרות בגין ניתן להטיל סנקציה זו:

1. אי מתן הודעה לפי סעיף 11 (בקשה לקבלת מידע);
2. אי מתן הודעה בעת פנייה בדיוור ישיר בהתאם להוראות סעיף 17(א);
3. גוף ציבורי שלא הודיע כי הוא מוסר מידע דרך קבע.

ד. עיבוד מידע שלא בהתאם למטרות המאגר עלול להוות הפרה שהעיצום בצידה בין 2,000 ש"ח ל-160,000 ש"ח בהתאם לסיווג רמות האבטחה של המאגר הקבועים בתקנות אבטחת המידע (הערה: לא ברור מה הקשר בין ההפרה לבין הסיווג הקבוע בתקנות האבטחה) (סעיף 23ב(ו)).

ה. ניתן להטיל עיצום כספי בסך 15,000 ש"ח בגין ההפרות הבאות (סעיף 23ב(ב)) –

1. אי מימוש זכות העיון;
2. תיקון מידע ללא הודעה לכל מי שקיבל מבעל השליטה מידע;

3. אי מתן הודעה על אי תיקון מידע;
 4. אי תיקון מידע;
 5. אי מחיקה ממאגר מידע המשמש לדיוור ישיר (הערה: מדובר בהוראה בעייתית משום שמקור הנתונים עשוי לשמש לעסק לגיטימי והשיווק הישיר בוצע כחלק מניהול העסק. ההפרה הייתה צריכה להיות מוגדרת ככזו אם נושא המידע ביקש להמחק מרשימת הדיוור הישיר, אולם נעשתה אליו פנייה נוספת על בסיס רשימת הדיוור);
 6. בעל מאגר לשירותי דיוור ישיר אשר לא נענה לדרישת נושא מידע שלא להעביר מידע אודותיו לאחר.
- ו. ניתן להטיל עיצום כספי בסך 150,000 ש"ח, ואם במאגר מעל מיליון איש העיצום יעמוד על 300,000 ש"ח, בגין ההפרות הבאות (סעיף 23ב(א)) –
1. אי רישום (רק אם סוחר במידע);
 2. כלל פרטים לא נכונים בבקשה או לא הודיע על שינוי בפרטים. ההפרה חלה לכאורה גם על גוף ציבורי;
 3. אי מסירת הודעה על ידי בעל שליטה המחויב בהודעה מכח סעיף 8א(ב) או חוסר עדכון שינוי הפרטים בהודעה כאמור;
 4. עיבד מידע אישי לשירותי דיוור ישיר מבלי שאחת המטרות תיכתב ככזו;
 5. גוף ציבורי שלא הודיע לראש הרשות כי הוא מקבל נתונים באופן שוטף מגוף אחר.
- ז. אי מסירת מידע, מסמכים או חומר מחשב למפקח, עלולה לגרור הטלת עיצום כספי בסך 300,000 ש"ח (סעיף 23ב(ז)). יש לציין כי מדובר באחד מהעיצומים הגבוהים והמחמירים, ללא קשר לגודל המאגר, רגישות המידע שבו או נסיבות רלוונטיות אחרות.
- ח. בגין הפרת הוראות תקנות אבטחת המידע ניתן להטיל עיצומים כספיים הנעים בין 1,000 ש"ח ל- 640,000 ש"ח, בהתאם לרמת האבטחה הנדרשת במאגר כמפורט בתקנות אבטחת המידע (תוספת שלישית לחוק).
- ט. בגין הפרת הוראות תקנות הגישור ניתן להטיל עיצומים כספיים בסכומים משתנים (סעיף 23ב(ט)). סכומים אלה תואמים את הפגיעה בזכויות לפי החוק והמדגים שנקבעו בסעיפים הקטנים של סעיף 23ב לחוק (תוספת רביעית לחוק).



Washington, DC | Brussels | Singapore | Tel Aviv

info@fpf.org

FPF.org