GOLDMAN
גולדמן משרד עורכי דין
סייבר | פרטיות | מערכות מידע

13 באוגוסט 2025

3162-71-2025

<u>מזכר 2025/2: כניסת תיקון 13 לחוק הפרטיות לתוקף: מדריך ללקוחות</u>

מחר (14.8.2025) תיקון 13 לחוק הגנת הפרטיות נכנס לתוקף.

תיקון 13 משנה באופן משמעותי את החובות החלים בניהול מערכות מידע. התיקון מטיל עיצומים גבוהים (עד מיליוני שקלים) על הפרת חוק בניהול מערכות מידע, ומעניק לרשות להגנת הפרטיות סמכויות פיקוח, חקירה ואכיפה נרחבות.

המסמך הבא מסביר בקצרה את חוקי הגנת פרטיות, אבטחת מידע וסייבר, בדגש על חובות מעשיות. המסמך אינו ממצה את הדין ואינו מהווה ייעוץ, אלא מדריך לעיקרי הדין.

לייעוץ פרטני ניתן להיכנס לאתר : https://israelgoldman.co.il

או לפנות במייל : israel@israelgoldman.co.il

בטלפון : 03-5533799 **או נייד** : 052-6400720 **ובפקס** : 077-4703857

כללי

החובות והעיצומים שנקבעו בחוק מחלקים את הגופים לארבע רמות, הרמות נגזרות מרמת רגישות הנתונים, כמות הנתונים, מספר העובדים ועוד.

ניתן להתרשם מהי רמת המאגר החלה על הארגון שלכם, במחשבון באתר המשרד.

כדי לסדר את הוראות הדין בצורה נוחה להתמצא, המזכר יסודר לפי סדר זרימת הנתונים:

כניסת המידע >> אחזקת המידע >> יציאת המידע

פרק א' איסוף מידע

אסור לאסוף מידע אישי על בני אדם, למעט במקרים הבאים:

כאשר חלה חובה חוקית לאסוף מידע אישי: למשל, בלא מעט מקצועות מוטלת חובה לאסוף צילומי תעודות זהות, למניעת הלבנת הון[1].

בהסכמת בעל המידע: הסכמה יכולה שתהיה מפורשת או משתמעת, אך ההסכמה צריכה להיות מודעת ומרצון חופשי[2].

[1] סעיף 3(א) לצו איסור הלבנת הון (חובת זיהוי, ניהול רישומים של נותן שירות עסקי למניעת הלבנת הון ומימון טרור), תשע"ה-2014. כמו כן, גילוי הדעת של הרשות "איסוף מספרי תעודות זהות וצילום תעודות זהות" מיום 17.03.2024.

[2] עמדת הרשות ב"טיוטת גילוי דעת בנושא הסכמה בדיני הגנת הפרטיות" (להלן – **"טיוטת גילוי דעת הסכמה"**).

גם כאשר מותר לאסוף מידע, קיימת חובת יידוע:

יש להודיע למוסר המידע: האם העברת המידע מחויבת בחוק; מה מטרת העברת המידע; מה תהיה תוצאת סירוב העברת מידע; למי יועבר המידע ולאיזו מטרה; שם בעל השליטה במאגר המידע; ועדכונו על זכותו העיון במידע האישי אודותיו וזכותו לבקש את תיקון המידע[3].

כמו כן:

- מותר לאסוף מידע שפורסם ברשתות חברתיות (למשל, פוסט ציבורי)[4], אך אין לעבד אותו בבינה מלאכותית[5].
- ניתן להשיג מידע מחוקרים פרטיים אך הוא חייב לעמוד בהגנות הקבועות בחוק (המידע נאסף מכוח חובה חוקית, מוסרית או חברתית)[6].
- יש לנסח מסמך "הסכמה ויידוע" ומומלץ לנסח "מדיניות הפרטיות".

עיצומים על איסוף מידע בלא לקיים את חובת היידוע:

ההפרה	סכום העיצום		פיצויים לדוגמה
איסוף מידע אישי בלא קיום חובת היידוע	**מידע אישי** – 50 ש"ח על כל אדם **מידע רגיש מאוד** – 100 ש"ח על כל אדם	ניתן להטיל מינימום של 30,000 ש"ח	ניתן לתבוע פיצויים של 10,000 ש"ח
פניה לאיסוף מידע אישי בלא לקיים את חובת היידוע, המופנית לקבוצה בלתי מסוימת של אנשים	**מידע אישי** – 2 ש"ח על כל אדם **מידע רגיש מאוד** – 4 ש"ח על כל אדם	ניתן להטיל מינימום: **על מידע אישי** – 20,000 ש"ח **על מידע רגיש מאוד** – 40,000 ש"ח	כל אחד יכול לתבוע פיצויים של 10,000 ש"ח

פרק ב' אחזקת מידע

החובות הבסיסיים באחזקת מידע:

1. **צמידות מטרה:** ניתן להשתמש במידע רק למטרה שלשמה נאסף.
2. **זכויות בעל המידע:** לבעל המידע זכות לעיין במידע עליו ולדרוש לתקנו.
3. **אבטחת מידע:** לוודא שהמידע מוגן ולא נחשף לגורמים לא מורשים.

---

[3] סעיף 11 לחוק הפרטיות.
[4] הערת מס' 2 "חובת יידוע במסגרת איסוף ושימוש במידע אישי" מיום 18.7.2022.
אך לא כאשר המידע נשלח למטרה ספציפית, למשל אתר היכרויות. ראה הערה 25 ל[טיוטת הנחיית הרשות להגנת הפרטיות: תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית](#) מיום 28.4.2025 (להלן – **"טיוטת הנחיה בינה מלאכותית"**)
[5] סעיף 6.3.5. לטיוטת הנחיה בינה מלאכותית.
[6] יש ליישם הגנות אלו בצמצום, בתום לב ובסבירות, רע"פ 4742/20 **מרדכי לייבל נ' מדינת ישראל** (נבו 21.7.22).

1 | צמידות מטרה

אין להשתמש או לעבד מידע אלא למטרה שלשמה נאסף המידע ("עיקרון צמידות המטרה").

חובה לבחון אחת לשנה, האם אין במאגרים מידע עודף שאינו נדרש עוד.

- דיוור ישיר: ניתן להשתמש בנתונים שנמסרו לצורך דיוור ישיר בנושאי העסק, ובלבד שתתאפשר הסרה מהדיוור הישיר[7].
- חשוב לציין בטופס ההסכמה כל מטרה הנצפית לשימוש במידע.
- חשוב למחוק מידע רגיש (למשל, צילום תעודות זהות או הקלטות ממצלמות אבטחה) כשאינו נדרש עוד.

עיצומים אי קיום בדיקה שנתית על קיום מידע עודף:

ההפרה	סכום העיצום לפי רמת מאגר			
	יחיד	בסיסית	בינונית	גבוהה
אי קיום בדיקה שנתית על קיום מידע עודף	2,000 ש"ח	2,000 ש"ח	40,000 ש"ח	160,000 ש"ח

2 | זכויות במידע

לבעל המידע מוקנות הזכויות הבאות:

- **יידוע:** יש לעדכן על איסוף המידע ומטרתו.
- **עיון:** בעל המידע זכאי לדרוש לדעת איזה מידע מוחזק אודותיו.
- **תיקון:** בעל המידע זכאי לדרוש תיקון מידע שגוי, וחובה לעדכנו שהמידע תוקן (אם מוחזק מידע אודות אזרחי אירופה, יש להפעיל מנגנון לדיוק המידע וליזום תיקון מידע שגוי).
- **לאירופאים (על מידע שהגיע מאירופה):** גם זכות לדרוש מחיקת המידע בסיום השימוש "הזכות להשכח" (ויש להפעיל מנגנון לנטר מידע מיותר ולמחוק אותו) וחובה לעדכן אותו בהעברת המידע לצד ג'.

[7] סעיף 11 ל[הנחיית רשם מאגרי המידע 2/2017].

עיצומים על אי־מתן זכויות:

ההפרה	סכום העיצום		פיצויים לדוגמה
אי מתן זכות עיון, אי מענה לבקשת תיקון, או אי תיקון או אי מתן הודעה על תיקון	קנס של 15,000 ש״ח		ניתן לתבוע פיצויים של 10,000 ש״ח
אי מחיקת מידע על אזרח האיחוד האירופי	קנס של 15,000 ש״ח		
אי הפעלת מנגנון לתיקון מידע או למחיקת מידע מיותר על אזרחי האיחוד האירופי. וכן, אי תיקון מידע שגוי שהתגלה	**מידע אישי** – 2 ש״ח על כל אדם **מידע רגיש מאוד** – 4 ש״ח על כל אדם	ניתן להטיל מינימום: **על מידע אישי** – 20,000 ש״ח **על מידע רגיש מאוד** – 40,000 ש״ח	

3 | אבטחת המידע והגנתו

חובה לאבטח את המידע מפני הסיכונים לדליפתו. מקורות הסיכונים הם:

(1) **הנהלה**: הנהלה חסרת מודעות או רשלנית;
(2) **עובדים**: עובדים חסרי הכשרה או לא מתאימים;
(3) **ספקים:** ספקים לא מתאימים;
(4) **טכנולוגיה:** מערכות טכנולוגיה לא עדכניות או לא מובטחות;

חובות החלות על ההנהלה

חובות ההנהלה:

- **הכרת מאגרי המידע**: יש לתעד את תשתיות המחשוב (חומרה, תקשורת, תוכנה, רכיבי אבטחת מידע ותרשים של מבנה המערכת) במסמך "**מבנה המאגר**" מעודכן.
- **הכרת נתוני הארגון:** חובה לתעד את סוג המידע, מטרות השימוש בו, הסיכונים לאבטחתו ודרכי הגנה במסמך "**הגדרות המאגר**" מעודכן.
- **נהלי אבטחת מידע:** חובה לקבוע נהלים לאבטחת מידע, לרבות התייחסות להרשאות גישה, הגנה טכנולוגית, ניהול סיכונים והתמודדות עם אירועי סייבר.
- **הודעה לרשות**: חובה להודיע לרשות על מאגר עם מידע בעל רגישות מיוחדת על יותר מ-100,000 איש.

- **דיונים**: חובה לקיים דיונים בהנהלה בסוגיית אבטחת מידע, ממצאי ביקורת ומבדק חדירה. תדירות הדיונים משתנה מסוגיה לסוגיה ובהתאם לגודל המאגר.
- **מינויים:** יש למנות בחלק מהארגונים, ממונה אבטחת מידע (CISO) וממונה הגנת הפרטיות (DPO).

הרשות דוחה את אכיפת מינוי ממונה הגנת פרטיות לסוף אוקטובר 2025!

עיצומים על הנהלה שאינה מקיימת את המוטל עליה:

ההפרה	סכום העיצום לפי רמת מאגר			
	יחיד	בסיסית	בינונית	גבוהה
אי קיום מסמך "מבנה המאגר"		1,000 ש"ח	20,000 ש"ח	80,000 ש"ח
אי קיום מסמך "הגדרת המאגר" מעודכן	2,000 ש"ח	2,000 ש"ח	40,000 ש"ח	160,000 ש"ח
אי קיום מסמך "נוהל אבטחה"		2,000 ש"ח	40,000 ש"ח	160,000 ש"ח
אי קיום דיון באבטחת מידע או בממצאי ביקורת			40,000 ש"ח	160,000 ש"ח
אי קיום דיון בממצאי מבדק חדירה				320,000 ש"ח
אי מתן הודעה לרשות				150,000 ש"ח
	סכום העיצום (ללא תלות בסוג המאגר)			
אי מינוי ממונה אבטחת מידע (CISO) או ממונה הגנת פרטיות (DPO)	**מידע אישי** – 2 ש"ח על כל אדם **מידע רגיש מאוד** – 4 ש"ח על כל אדם		ניתן להטיל מינימום: **על מידע אישי** – 20,000 ש"ח **על מידע רגיש מאוד** – 40,000 ש"ח	

חובות החלות בהקשר של עובדים

עובדי ארגון עלולים להיות מקור לדליפת מידע, לכן נקבעו החובות הבאים:

- **מיון:** לפני מתן הרשאת גישה למאגר מידע, יש לבחון את התאמת העובדים בתהליך מיון.
- **הדרכה:** יש לערוך הדרכת אבטחת מידע לפני מתן הרשאת גישה למאגר המידע, ובחלק מהמאגרים, גם אחת לשנתיים.
- **הרשאות גישה:** יש לערוך נוהל הרשאות גישה[8], לכלול פירוט תפקידים וזהות מורשים, ולהבטיח גישה רק למורשים, בחלק ממאגרי המידע, יש להשתמש באמצעי זיהוי פיזי[9].
- **פרטיות העובדים:** יש לשמור על פרטיות העובדים ולהימנע ממעקב בלתי מידתי אחריהם. מעקב חייב לעמוד בעקרונות של לגיטימיות, רלוונטיות, מידתיות, הליך הוגן, הסכמה ושקיפות[10].
- **סיום העסקה:** בסיום העסקת עובד, יש לבטל מיד את כל הרשאות הגישה ולשנות סיסמאות למאגרים.

עיצומים על הפרת חובות הקשורים לעובדים:

ההפרה	סכום העיצום לפי רמת מאגר			
	יחיד	בסיסית	בינונית	גבוהה
אי קיום מיון או הדרכה		1,000 ש"ח	20,000 ש"ח	80,000 ש"ח
אי קיום נוהל הרשאות ויישומו		2,000 ש"ח	40,000 ש"ח	160,000 ש"ח

חובות בהקשר של ספקים

ספקים עלולים להיות נקודת תורפה בהגנה על מידע, לכן נקבעו החובות הבאים:

- **בחינת ספקים**: לפני התקשרות עם ספק יש לבדוק את רמתו ואיכותו ולשלוח לו שאלונים למילוי.
- **חוזה עם הספק**: יש לערוך חוזה או נספח לחוזה המכתיב סטנדרט אבטחת מידע ומגבלות גישה לנתוני הארגון[11].

---

[8] ולשמור אותו למשך שנתיים.

[9] במסמך דגשים למנהלים ועובדים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית מיום 24.3.2020 הרשות ממליצה לכלול בנוהל אבטחת מידע התייחסות ספציפית לעבודה מרחוק, לרבות ניטור מוגבל, הדרכה למניעת דיוג, אבטחה כפולה והמנעות מכלים מאובטחים.
גם מערך הסייבר הלאומי פרסם מסמך עם רשימת אלגוריתמים ופרוטוקולים של ארשת וירטואלית פרטית (VPN) מומלצת לשימוש.

[10] ע"ע 41179-01-24 **ד"ר מרק פרידמן בע"מ ואח' נ' רויטל אלקנר**.
הרשות פרסמה (ראה סעיף 9 "היבטי פרטיות במעקב אחר עובדים בעבודה מרחוק" מיום 17.10.2023) רשימת פרקטיות בלישה אסורים.

[11] תקנה 15(א)(2) לתקנות אבטחת מידע מפרטת 8 סוגיות שעליהם להיות מוסדרות בחוזה עם ספק.

- **ביקורת ספקים**: יש לערוך בדיקות תקופתיות לוודא את עמידת הספק בדרישות ולשמור תיעוד הביקורת[12].

עיצומים על הפרת החובות החלים על התקשרות עם ספקים:

ההפרה	סכום העיצום לפי רמת מאגר			
	יחיד	בסיסית	בינונית	גבוהה
אי קיום בדיקה, הסדרה חוזית וביקורת על ספקים		4,000 ש"ח	80,000 ש"ח	320,000 ש"ח

חובות בהקשר של טכנולוגיה

לצורך הגנה על מידע במערכות המחשוב, נקבעו החובות הבאים:

- **תיעוד מצאי:** יש להחזיק מסמך עדכני של רשימת אמצעי חומרה, תוכנה ותקשורת.
- **אבטחה פיזית:** חובה לאחסן ציוד מחשוב ותקשורת במקום מוגן. בחלק ממאגרי המידע יש לנהל תיעוד של הגישה לציוד.
- **אבטחה טכנולוגית:** יש להתקין אמצעי הצפנה ואבטחה (כגון EDR/XDR, חומת אש, אנטי וירוס, אנטי מיילור, מניעת גישה לאתרים זדוניים בסטנדרט הנוהג בענף הפעילות.
- **עדכונים:** יש להשתמש רק בציוד מחשוב ותקשורת ובתוכנות מורשים ונתמכים בעדכוני אבטחה למערכות.
- **בקרה ותיעוד גישה:** הגישה למערכות תהיה באמצעות סיסמאות חזקות[13], או באמצעות אימות דו-שלבי, ובחלק מהמאגרים רצוי שהגישה תהיה באמצעים פיזית (טוקן או כרטיס). בחלק ממאגרי המידע חובה להתקין לוגים לתיעוד כניסות וניסיונות כניסה למערכות המידע, ולבדוק אותם באופן שוטף, לעדכן את בעלי ההרשאה על קיומם, לערוך דיווח על תקלות ולשמור את תיעוד הלוגים וגיבויים[14].
- **ניתוק והפרדה:** יש לנתק מחשבים שאינם בשימוש, ולהפריד בין מחשבים ותוכנות עם גישה למאגר מידע לאלו ללא גישה.
- **ביקורת וסקר סיכונים:** בחלק מהארגונים יש לערוך ביקורת אבטחה, סקר סיכונים ומבדק חדירות.

---

[12] למשך שנתיים (ראה: תקנה 17(א) לתקנות אבטחת מידע). במאגרי מידע ברמה בינונית או גבוהה, יהיה לביקורת גיבוי ויכולת שזור, ובמאגר ברמה הגבוהה ישמר גם עותק הגיבוי.
[13] הרשות ומערכת הסייבר פרסמו (הרשות כאן ומערך הסייבר כאן) כללים בסיסיים לסטנדרט של איכות של סיסמה.
[14] תקנות 10 ו-17 לתקנות אבטחת מידע. עם זאת עמדת הרשות כי שמירת הלוגים למשך שנתיים נדרשת רק בלוגים על מערכת ההפעלה, מאגר המידע, אקטיב דיירקטורי, EDR, NAC וחומת אש. הלוגים על יתר המערכות נדרשים לשמירה של חצי שנה.

- **שימוש בבינה מלאכותית:** הזנת מידע לבינה מלאכותית דורשת הסכמה מודעת ומפורשת של בעל המידע[15].
- **שמירה וגיבוי:** חובה לשמור באופן מאובטח את תוצרי אבטחת מידע, ובחלק ממערכות המידע חובה לגבות תוצרים אלו.

עיצומים על הפרת חובות הקשורים לטכנולוגיה:

ההפרה	סכום העיצום לפי רמת מאגר			
	יחיד	בסיסית	בינונית	גבוהה
אי החזקה רישום מצאי של מחשוב, תקשורת ותוכנה, וכן אי שמירה על המחשב והתקשורת במקום מוגן פיזית, וכן אי תיעוד אמצעי האבטחה		1,000 ש"ח	20,000 ש"ח	80,000 ש"ח
אי קיום אבטחת מידע טכנולוגית (כדוגמת חומת אש ואנטי וירוס), וכן אי עדכון שוטף של מערכות המחשוב והתוכנה	2,000 ש"ח	2,000 ש"ח	40,000 ש"ח	160,000 ש"ח
אי קביעות נוהל הרשאות ויישומו		2,000 ש"ח	40,000 ש"ח	160,000 ש"ח
אי קיום בקרה ותיעוד גישה פיזית למחשוב, וכן אי גיבוי תיעודי לוגים, וכן אי גיבוי אמצעי אבטחת מידע וכן אי הפרדת מערכות המאגר			20,000 ש"ח	80,000 ש"ח

[15] סעיף 6.3 לטיוטת הנחייה לבינה מלאכותית.
יש לציין כי הרשות פרסמה ביוני 2025 המלצות פרקטיות לכתיבת פרומפטים והתנהלות עם בינה מלאכותית.

אי התקנת לוגים, בקרתם, עדכון בעלי ההרשאות, אי עריכת דיווחים על תקלות, וכן אי קיום ביקורת אבטחת מידע תקופתית			40,000 ש"ח	160,000 ש"ח
אי קיום סקר סיכונים				320,000 ש"ח

פרק ג' יציאת נתונים

נתונים עשויים לצאת מהארגון, ביוזמתו או בניגוד לרצונו.

1 | איסור העברת מידע

- אסור להעביר מידע אישי לצד שלישי בלא הסמכה חוקית או הסכמה.
- העברה לחו"ל מותרת בשני תנאים[16]:

(1) למדינות שחל בהם דין המחייב רמת אבטחת מידע דומה לישראל, או מקבל המידע מתחייב לעמוד בדרישות החוק החל בישראל[17] להבטיח את הגנת הפרטיות[18] או באישור בעל המידע.

(2) מקבל המידע מבטיח לשמור את פרטיות הנתונים[19].

2 | סייבר

הסייבר הוא האיום המרכזי על פרטיות נתוני הארגון.

ישנם שני סוגים של אירועי סייבר:

(1) אירוע סייבר (טעות, כגון שליחת מידע לגורם שגוי);

(2) מתקפת סייבר (פגיעה) עוינת[20].

החובות שנקבעו לגבי סייבר:

[16] תקנה 2 לתקנות הגנת הפרטיות (העברת מידע אל מאגר מידע שמחוץ לגבולות המדינה), תשס"א-2001 (להלן – "**תקנות העברת מידע**").
[17] הרשות פרסמה טיוטת גילוי דעת ובו פירוט ההסדרים החלים בישראל עליהם הספק נדרש להתחייב.
[18] מן הראוי לציין שהסדר זה הוגבל באיחוד האירופי, ביחס לחברות בארה"ב במסגרת פס"ד שרמס2 ובעקבות פס"ד שרמס2 הנ"ל הרשות פרסמה גילוי דעת מקביל בישראל, אך הסירה את גילוי הדעת.
[19] תקנה 3 לתקנות העברת מידע. יוער כי תקנה 3 דורשת גם התחייבות של הגורם בחו"ל שלא יעביר לגורם נוסף, אך הרשות הגדירה דרישה זו כ"גזרה שאין הציבור יכול לעמוד בה".
[20] הרשות פרסמה 8 דוגמאות מעשיות להתקפה עוינת.

חובות בשגרה:

- **נוהל סייבר:** יש לקבוע נוהל לטיפול באירועי מתקפות סייבר, מותאם לחומרת האירוע ורגישות המידע (לרבות ביטול הרשאות).
- **דיווח ותיעוד:** יש לדווח למנהלים על כל אירוע סייבר, לתעד אותם, ובחלק ממאגר המידע גם לתעד את שחזור המידע, ולשמור את התיעוד.
- **דיונים:** חובה לקיים דיונים בסוגיות של סייבר, תדירות הדיונים משתנה בהתאם לגודל המאגר[21].

במתקפת סייבר[22]:

- **דיווח:** בחלק ממאגרי המידע חובה לדווח מידית לרשות הפרטיות על תקיפת סייבר.

עיצומים על הפרת חובות הקשורים לסייבר:

ההפרה	סכום העיצום לפי רמת מאגר			
	יחיד	בסיסית	בינונית	גבוהה
אי תיעוד אירועי סייבר	2,000 ש"ח	2,000 ש"ח	40,000 ש"ח	160,000 ש"ח
אי תיעוד הליך שחזור המידע			20,000 ש"ח	80,000 ש"ח
אי קיום דיון תקופתי על אירועי הסייבר			40,000 ש"ח	160,000 ש"ח
אי דיווח לרשות על מתקפת סייבר			80,000 ש"ח	320,000 ש"ח

[21] תקנה 11(ג) לתקנות אבטחת מידע.
[22] הגדרת מתקפת סייבר נחלקת (תקנה 1 לתקנות אבטחת מידע):
במאגר ברמה גבוהה – כל פגיעה עוינת;
במאגר ברמה בינונית – רק אם נפגע חלק מהותי במאגר;

GOLDMAN
גולדמן משרד עורכי דין
סייבר | פרטיות | מערכות מידע



גולדמן משרד עורכי דין, דיני סייבר, פרטיות ואבטחת מידע:

- ייעוץ משפטי;
- ניסוח מסמכי חובה;
- ניסוח מסמך הסכמה ומדיניות פרטיות;
- ניסוח חוזים עם ספקים;
- ליווי משפטי במשבר סייבר;
- ייצוג בפני רשות הפרטיות ובתי משפט;

israel@israelgoldman.co.il | https://israelgoldman.co.il

טלפון: 03-5533799 | נייד: 052-6400720 | פקס: 077-4703857