Or-Hof Tech & IP Law

אור-חוף
טכנולוגיות וקניין רוחני

2018

המדריך ל - GDPR

כללים עקרונות ותחולה על חברות ישראליות

כתבו וערכו: עו"ד דן אור-חוף
וצוות משרד עורכי דין אור-חוף טכנולוגיות וקניין רוחני

רחוב הברזל 7, רמת החייל, תל אביב 6971011
www.or-hof.com
mailto:office@or-hof.com
03-5620992 ; 1 (415) 906-5260

הנה שלושת הדברים החשובים ביותר שצריך לדעת על חוק הגנת המידע האירופי:

בינואר 2012 פורסמה טיוטת החוק הראשונה. מטרתה - עדכון דיני הגנת המידע האישי באירופה ויצירת הרמוניזציה חקיקתית ברחבי האיחוד האירופי. רק ארבע שנים אחר כך הגיע האיחוד האירופי לנוסח הסופי. את דירקטיבת הגנת המידע האישי[1] - החוק המנחה האירופי, שמכוחו חוקקו חוקי הגנת המידע האישי על ידי המדינות החברות באיחוד האירופי, החליף החוק הכללי להגנת מידע– General Data Protection Regulation, או בקיצור, ה – GDPR[2].

הוראות ה – GDPR נכנסו לתוקף ביום 25 במאי 2018. ה – GDPR מרחיב את תחולתם של דיני הגנת הפרטיות החלים באיחוד האירופי באופן דרמטי, גם אל מעבר לטריטוריית האיחוד האירופי. הוא שולח את זרועותיו הארוכות לחברות האוספות ומנהלות מידע אישי אגב אספקת שירותים או מוצרים לשוק האירופי. הוא חל גם על חברות היוצרות פרופילים התנהגותיים של אנשים הנמצאים פיסית באיחוד האירופי, ללא קשר לתושבותם או אזרחותם.

כל אלה הן דוגמאות לחברות ישראליות שה – GDPR חל עליהן, אם במהלך השירותים שהן מספקות, הן מנהלות או משתמשות במידע אישי:

דוגמאות לדרישות המופיעות בחוק האירופי וחלות במקרים הרלוונטיים:

- שינוי מהותי של מדיניות הפרטיות.
- מינוי של קצין הגנת מידע (תפקיד שונה ונפרד מקצין אבטחת מידע).
- מינוי נציג של החברה בשטחי האיחוד האירופי.

[1] 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.

[2] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

לתוכן העניינים

- שילוב שיקולים של הגנת מידע לתוך תכנון מערכות ושירותים חדשים.
- דיווח לרשויות האיחוד האירופי על פריצות למידע.
- ניהול מנגנון פשוט לביטול ההסכמה לשימוש במידע.
- תיעוד מפורט של אופני עיבוד מידע.
- חובה לאפשר לנושאי המידע (בני האדם שהמידע מתייחס אליהם) למחוק מידע לא רלוונטי, לנייד מידע מספק שירותים אחד לשני ולהתנגד לקבלת החלטות לגביהם המבוססות על עיבוד אוטומטי.

חברה שלא תציית להוראות החוק תשלם מחיר כבד של עד 4% מהתוצר השנתי הגלובאלי שלה או עד 20,000,000 אירו – לפי הגבוה מבין השניים. זהו גובה הקנס המנהלי (ללא צורך באישור של בית משפט), שרשויות הגנת מידע אירופיות תוכלנה להטיל.

החוק רחב ומורכב והוא כולל 173 סעיפים בדברי האקדמה ו – 99 סעיפים בחוק עצמו.

בשל חשיבותו הרבה לחברות ישראליות רבות, ערכנו את המדריך הזה, המתייחס להוראות שלדעתנו הן המשמעותיות ב – GDPR לחברות ישראליות. ביארנו את המושגים הכלולים בו והמלצנו המלצות כיצד לדעתנו יש להיערך לציות לו.

זהו כמובן לא תרגום של החוק. המדריך איננו ממצה, כיוון שישנן הוראות ב – GDPR שעוד תדרושנה מלאכת פרשנות רבה ולעתים תמצאו בו גם את דעתנו.

<u>לתשומת הלב</u>: איננו מוסמכים לעריכת דין באיחוד האירופי והמדריך איננו בגדר חוות דעת משפטית. תפקידו לשמש כמעין מורה נבוכים למושגים ולעקרונות הכלולים בחוק ולסייע בהבנת יישום הוראותיו, אך הוא איננו תחליף ליעוץ מקצועי בנוגע לחוק זה.

אנו מקווים שמדריך זה יועיל לכם.

לתוכן העניינים

אודות משרד עו"ד אור-חוף טכנולוגיות וקניין רוחני

אור-חוף טכנולוגיות וקניין רוחני הוא משרד בוטיק המתמחה במשפט מסחרי בינלאומי, בטכנולוגיות, קניין רוחני, הגנת מידע וסייבר.

המשרד מייצג חברות ישראליות ובינלאומיות בתחומי הטכנולוגיות, פיננסים, תקשורת, מדיה ופרסום, חינוך, ניהול זכויות יוצרים, רשויות ממשל ורשויות מקומיות, ועוד ; המשרד מספק מעטפת משפטית לחברות ומיזמים טכנולוגיים, לרבות חוזים מסחריים ומסחור טכנולוגיות (כולל מוצרי ה"אינטרנט של הדברים" (IoT), רחפנים, רובוטיקה, אינטיליגנציה מלאכותית (AI), מציאות רבודה(AR), נתוני עתק (Big Data) ועוד), דיני תאגידים, עסקאות בינלאומיות, בניה והוצאה לפועל של תכניות ציות, רישום ואכיפת זכויות קניין רוחני, בחינת אסטרטגיות עסקיות, ניתוח רגישויות וסיכונים ותהליכי בדיקת נאותות (Due Diligence) בעולמות החדשנות והטכנולוגיה.

מזה מספר שנים שתחום הגנת הפרטיות, ניהול מידע אישי ואבטחת מידע מגדיל באופן ניכר את השפעתו על הפעילות המסחרית בארץ ובעולם. סיכוני האבטחה והסייבר ההולכים ומתרבים, לצד גידול בקנסות ובעצירת פעילויות על ידי הרגולטורים בארץ ובחו"ל, מחייבים שינוי גישה מהותי. לשם כך פרסמנו את המדריך הנוכחי, ופיתחנו מתודולוגיה ייחודית במטרה לסייע לחברות וארגונים בהיערכותם לעמידה בדרישות ה –GDPR, ואכן המשרד סייע ומסייע לעשרות חברות ישראליות ובינלאומיות בנושא.

עו"ד דן אור-חוף

עו"ד דן אור-חוף, בעל רישיון לעריכת דין בישראל ובמדינת ניו יורק ארה"ב, בעל ותק של 20 שנה ובעל תואר שני בהצטיינות יתרה מאוניברסיטת תל אביב בשיתוף עם אוניברסיטת ברקלי, קליפורניה. דן הקים את המשרד בשנת 2013 לאחר ששימש קודם לכן כשותף וכמנהל צוות טכנולוגיות מידע, אינטרנט וזכויות יוצרים בפירמה בינלאומית. דן בעל ניסיון רב במשפט אזרחי- מסחרי עם התמחות בתחומי הטכנולוגיות וקניין רוחני. לצד עבודה משפטית – מסחרית, דן עוסק ברגולציה, ציות וחקיקה ;

עו"ד דן אור-חוף, עוסק בהיבטי הגנת מידע ופרטיות מזה שנים רבות. הוא מומחה מוסמך להגנת מידע אישי (CIPP/US; CIPP/E) וחבר האיגוד הבינלאומי למומחים בתחום ההגנה על פרטיות במידע (IAPP), יו"ר הפורום להגנת מידע ופרטיות (KnowledgeNet), מלמד הגנת מידע ופרטיות בתוכנית ללימודי הסייבר באוניברסיטת תל אביב, חבר המועצה הציבורית להגנת הפרטיות, מייעץ בתהליכי חקיקה, מרצה בארץ ובחו"ל וכותב לפרסומים מקומיים וזרים.

נשמח לעמוד לרשותכם.

למידע נוסף אודות הצוות המשפטי בקרו באתרנו www.or-hof.com

תוכן העניינים

לתוכן העניינים

מושגי יסוד

המלצה לפעולה	הכירו את ההגדרות העיקריות ב – GDPR. הן שונות מהדין הישראלי וחשובות מאד לצורך הבנת החוק.

סעיפים רלוונטיים	סעיף 4 ל – GDPR

כדי להבין את ה – GDPR, יש להכיר את הטרמינולוגיה שבה החוק משתמש. היא דומה לזו שהדירקטיבה השתמשה בה עד מועד כניסתו לתוקף של ה-GDPR, אך כוללת גם מושגים נוספים. היא מזכירה במידה מסוימת הוראות והגדרות בחוק הגנת הפרטיות, התשמ"א-1981 ("חוק הגנת הפרטיות הישראלי") ובתקנות שמכוחו, אך בכל זאת שונה במידה רבה.

בחרנו להציג אחד עשר מושגים דומיננטיים, שמומלץ להכיר אותם על מנת להבין את הוראות ה – GDPR:

- **בעל השליטה במידע** (Data Controller)[3] – אדם, לרבות תאגיד וחבר בני אדם, רשות ציבורית, סוכנות או כל גוף אחר, אשר לבד, או יחד עם אחרים, קובע את המטרות והאמצעים לעיבוד של מידע אישי; כאשר המטרות והאמצעים לעיבוד המידע נקבעים על ידי איגוד או חוק של מדינה חברה באיחוד האירופי, בעל השליטה במידע או אמות הבחינה לקביעתו יכולים להינתן על ידי האיגוד או החוק של המדינה החברה.

- **הסכמה** (Consent)[4] - הסכמה של נושא מידע משמעה חיווי שניתן באופן חופשי, מסוים, מודע וחד-משמעי של רצונותיו של נושא המידע, שבאמצעותו, בדרך של הצהרה או פעולה ברורה ומחייבת (affirmative), נושא המידע מעיד על הסכמתו לעיבוד המידע האישי הנוגע אליו.

- **יצירת פרופיל** (Profiling) משמעה כל צורה של עיבוד אוטומטי של מידע אישי הכוללת את השימוש במידע אישי כדי להעריך היבטים אישיים מסוימים הקשורים לאדם, במיוחד לצורך ניתוח או כדי לנבא היבטים הנוגעים לתפקודו של אדם בעבודה, בתהליך כלכלי, בהקשר לבריאותו, להעדפותיו ולאינטרסים שלו, לאמינותו, להתנהגותו למיקומו ולתנועותיו.

- **מידע אישי** (Personal Data)[5] – משמעו מידע הנוגע לאדם 'טבעי' [דהיינו שאינו תאגיד או חבר בני אדם – ד.א.] מזוהה או שניתן לזיהוי ('נושא המידע'); אדם שיכול להיות מזוהה הוא אדם שניתן לזהותו במישרין או בעקיפין, במיוחד בדרך של התייחסות למזהה כדוגמת שם, מספר מזהה, מידע על מיקום, מזהה אינטרנטי, או לאחד או יותר מאפיינים פיזיים, פיזיולוגיים, גנטיים, מנטאליים, כלכליים, או מזהים תרבותיים-חברתיים של אותו אדם.

- **מעבד** (Processor)[6] – אדם, לרבות תאגיד וחבר בני אדם, רשות ציבורית, סוכנות או כל גוף אחר המעבד מידע אישי בשמו של בעל השליטה במידע.

- **נושא מידע** (Data Subject) – אדם מזוהה או שניתן לזיהוי באמצעות מידע אישי.

---

[3] השוו ל"בעל מאגר מידע" – מונח שחוק הגנת הפרטיות משתמש בו, אך איננו מגדיר אותו וכן להגדרת "מנהל מאגר" בסעיף 7 לחוק.
[4] השוו להגדרת "הסכמה" בסעיף 3 לחוק הגנת הפרטיות.
[5] השוו להגדרת "מידע" בסעיף 7 לחוק הגנת הפרטיות.
[6] השוו להגדרת "מחזיק" בסעיף 3 לחוק הגנת הפרטיות.

לתוכן העניינים

- **נציג** (Representative) – אדם או תאגיד, הנמצא באיחוד האירופי ושבעל שליטה במידע או מעבד מידע ייפה את כוחו בכתב לייצג אותם בקשר עם החובות החלות עליו בהתאם ל – GDPR.

- **עיבוד** (Processing)[7] משמעו כל פעולה או קבוצת פעולות המבוצעת במידע אישי או באוסף של מידע אישי, בין באמצעות אמצעים אוטומטיים ובין בדרכים אחרות, כגון: איסוף, הקלטה, סידור, הבניה, שמירה, התאמה או שינוי, אחזור, התייעצות, שימוש, גילוי/שיתוף באמצעות שידור, הפצה, או הפיכת המידע האישי לזמין, תיווי (alignment), שילוב, הגבלה, מחיקה או השמדה.

- **פסאודונימיזציה** (Pseudonymisation)[8] – משמעה עיבוד של מידע אישי באופן שהמידע האישי איננו יכול עוד להיות משויך לנושא מידע מסוים ללא שימוש במידע נוסף, בכפוף לכך שהמידע הנוסף נשמר בנפרד והוא כפוף לאמצעים טכניים וארגוניים להבטיח שהמידע האישי לא ישויך לאדם מזוהה או שניתן לזיהוי.

- **פריצה למידע אישי** (Personal Data Breach) – משמעה פריצת אבטחה המובילה להשמדה, אובדן, שינוי, חשיפה בלתי מורשית או גישה למידע אישי השמור, משוגר, או מעובד בדרך אחרת, בטעות או באופן בלתי חוקי.

- **שירות חברת המידע** (Information Society Service)[9] – זהו שירות המסופק באופן שגרתי עבור תמורה, ממרחק, באמצעים אלקטרוניים ולבקשת האדם שהשירות מסופק לו.

---

7 השוו להגדרת "שימוש" בסעיף 3 לחוק הגנת הפרטיות.

8 זהו מושג חדש. הוא איננו קיים בחוק הישראלי וגם לא קיים בדירקטיבה שה – GDPR החליף. שימו לב שזהו מושג נפרד מאנונימיזציה. בדברי האקדמה ל – GDPR מצוין שחוק זה איננו חל על מידע אנונימי, דהיינו על מידע שאיננו משויך לאדם מזוהה או שניתן לזהותו.

9 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1). Point (b), Article 1(1).

תחולת החוק וכניסתו לתוקף

מועד כניסה לתוקף

המלצה לפעולה	החוק נכנס לתוקף ביום 25.5.2018 ולכן מומלץ להשלים את הליך הציות ללא דיחוי.

חברות וארגונים שהחוק חל עליהם חייבים להיערך בהתאם, כיוון שדרישות החוק הן רבות ומורכבות והסיכון שבאי ציות להן גבוה מאד.

תחולה מהותית וטריטוריאלית – תמצית

המלצה לפעולה	✓ בידקו היטב: האם אתם "נמצאים" באיחוד האירופי? האם אתם מעבדים מידע אישי של נושאי מידע הנמצאים באיחוד האירופי? האם אתם מנטרים התנהגות של נושאי מידע הנמצאים באיחוד האירופי? אם התשובה חיובית לאחת או יותר מהשאלות הללו, ה – GDPR חל עליכם ומשכדעליכם להיערך לבניית תוכנית ציות מתאימה. ✓ אם אין לכם נוכחות באירופה, אך ה – GDPR חל עליכם, ייתכן שתצטרכו למנות נציג מטעמכם באיחוד האירופי. ✓ שימו לב שה – GDPR איננו תחליף לחקיקה ורגולציה בתחומים מסוימים, כדוגמת שירותי בריאות, שירותים כלכליים וכיו"ב. לצד תוכנית ציות מתאימה ל – GDPR, יש לבדוק וליישם הנחיות רגולטוריות ספציפיות בהתאם לנדרש.

סעיפים רלוונטיים	סעיפים 2, 3, 27 ל – GDPR. סעיפים 6-17, 19-24, 36 לדברי האקדמה.

בהשוואה לדירקטיבת הגנת המידע, ה – GDPR מרחיב את תחולת דיני הגנת המידע האירופיים והוא כולל שני היבטים מרכזיים:

- החוק חל על כל בעל שליטה במידע ומעבד מידע שמקום מושבם בגבולות האיחוד האירופי (למה הכוונה ב"מקום מושבם"? – על כך בהמשך) כאשר המידע האישי מעובד בהקשר לפעילותם.
- החוק חל גם על בעלי שליטה במידע או מעבדי מידע שמקום מושבם איננו בגבולות האיחוד האירופי אם הם:
- (1) מעבדים מידע על נושאי מידע באיחוד האירופי בקשר עם הצעה של מוצרים או שירותים לנושאי מידע אלה, כדוגמת שירותי 'תוכנה כשירות' (SaaS). כלומר, ישראליים המספקים שירותים ללקוחותיהם האירופים שבתורם מציעים שירותים או מוצרים לנושאי מידע הנמצאים בשטחי האיחוד האירופי; או,

(2) מנטרים את ההתנהגות של נושאי המידע באיחוד האירופי, כדוגמת שירותי פרסום ואנליטיקה אינטרנטיים.

"מקום מושבם": ה – GDPR יחול על ארגונים בעלי מקום מושב (Established) באיחוד האירופי, כאשר המידע האישי מעובד בהקשר לפעילות של נוכחות זו. כלומר, החוק יכול לחול גם כאשר עיבוד המידע נעשה בפועל בטריטוריה אחרת.

המונח "מקום מושב" פורש בפסיקה האירופית בהרחבה, כך שהוא כולל כל פעילות אמיתית ואפקטיבית שמקיים ארגון באמצעות הסדרים קבועים בתוך האיחוד האירופי, אפילו אם הפעילות היא מינימלית.[10] הצורה המשפטית שבה הפעילות נעשית – לדוגמה באמצעות סניף או משרד, איננה מרכיב מכריע בהחלטה לגבי נוכחות החברה בשטחי האיחוד האירופי.

בדברי האקדמה מצוין עוד כי מקום המושב המרכזי של מעבד המידע צריך להיות מרכז ניהול עסקיו בתוך האיחוד האירופי ואם אין לו מרכז כזה – המקום שבו עיקר פעילות עיבוד המידע נעשית.[11]

כך לדוגמה –

- הנוכחות של אדם אחד המייצג את החברה בתוך האיחוד האירופי יכולה לספק.
- אתר אינטרנט בהונגרית המפרסם מוצרים או נכסים בהונגרית, עם סוכן מקומי וכתובת מקומית בהונגרית, הוכר כבעל נוכחות באיחוד האירופי, על אף שפעל ממדינה אחרת.[12]
- ארגונים בעלי משרדי מכירות באיחוד האירופי, המפרסמים או משווקים לתושבי האיחוד האירופי, כפופים אף הם ל – GDPR.[13]

ה – GDPR חל על מכירת מוצרים ושירותים לנושאי מידע הנמצאים באיחוד האירופי

ה – GDPR חל בנוסף על ארגונים שמקום מושבם איננו באיחוד האירופי, אך הם מציעים מוצרים ושירותים לנושאי מידע הנמצאים באיחוד האירופי. מדובר על הצעה של שירותים ומוצרים ואין הכרח שיבוצע בפועל תשלום. ההחלטה בסופו של דבר ניתנת על בסיס כל מקרה לגופו והרשימה של הדוגמאות שלהלן איננה ממצה. כל אלה יכולים להשפיע על תחולת ה – GDPR –

- לאתר או לאפליקציה יש גירסה בשפה של אחת ממדינות האיחוד האירופי;
- אפשרות לרכוש מוצרים או שירותים באמצעות מטבע האיחוד האירופי - האירו;
- טקסט שיווקי המכוון לתושבי האיחוד האירופי;
- קמפיינים פרסומיים המכוונים לתושבי האיחוד האירופי;
- שימוש בשם מתחם בסיומת eu. או סיומת מדינתית של אחת מהמדינות החברות באיחוד האירופי;

מנגד, עצם העובדה שניתן יהיה לגשת לשירות מתוך האיחוד האירופי, איננה מספיקה.

ה – GDPR חל על ניטור של פעילות נושאי מידע הנמצאים באיחוד האירופי

עיבוד מידע אישי של נושאי מידע על ידי בעל שליטה במידע או מעבד מידע שאין להם נוכחות באיחוד האירופי חלה כאשר עיבוד המידע האישי נוגע לניטור ההתנהגות של נושאי המידע או כאשר ההתנהגות מתרחשת ברחבי האיחוד האירופי.

---

[10] ראו החלטת ה – Court of Justice of the European Union (CJEU) בתיק C-230/14 Weltimmo v. NAIH, החלטה מיום 1.10.2015.
[11] ראו סעיף 36 לדברי האקדמה.
[12] ראו בעניין Weltimmo לעיל.
[13] ראו החלטת ה – CJEU מיום 13.5.2014 בתיק C-131/12 בעניין גוגל נ' רשות הגנת המידע הספרדית ומריו גונזלס (ההחלטה שמיסדה את "הזכות להישכח").

לתוכן העניינים

בהתאם לדברי האקדמה של ה – GDPR, כדי לקבוע אם פעילות עיבוד מידע אישי תיחשב כניטור התנהגות של נושאי מידע, יש לברר אם נושאי מידע מנוטרים באינטרנט ולאחר מכן נעשה שימוש בטכניקות עיבוד מידע אישי לצורך יצירת פרופילים התנהגותיים, במיוחד כדי לקבל החלטות הנוגעות לנושאי המידע, או כדי לנתח או לנבא את ההעדפות, ההתנהגות והגישות של נושאי המידע.

מינוי נציג באירופה

בעלי שליטה במידע או מעבדי מידע שאין להם נוכחות באיחוד האירופי, צריכים לבחון האם חלה עליהם חובה למנות נציג מטעמם באיחוד האירופי.[14]

על מה החוק לא חל?

ל – GDPR אין תחולה על שורה של פעילויות וביניהן –

- ❖ שימוש במידע אישי לצרכים אישיים בלבד.
- ❖ שימוש במידע אישי לצורכי חקירה ומניעת עבירות פליליות.
- ❖ שימוש במידע אישי לצורכי ביטחון לאומי.

האם זה יהיה החוק היחיד?

הדירקטיבה להגנת מידע שהיתה בתוקף עד ליום 24.5.2018, שימשה כחוק מנחה בלבד, שמכוחו כל מדינה החברה באיחוד האירופי חוקקה חוק הגנת מידע משלה. הדבר יצר חוסר אחידות ביישום העקרונות שנקבעו בדירקטיבה.

ה – GDPR לעומתה הוא חוק שחל כפי שהוא בכלל מדינות האיחוד האירופי. עם זאת, החוק כולל מספר רב של מקומות המאפשרים למדינות החברות לחוקק חוקים משלהן, הנגזרים מה – GDPR, לדוגמה, חקיקה הנוגעת למידע גנטי וביומטרי, חקיקה הנוגעת לפרטיות ילדים בשירותים לא אינטרנטיים והסדרת השימוש במידע על עבירות פליליות והרשעות.

זו אליה וקוץ בה. לכאורה מדובר במהלך של הרמוניזציה בחקיקה והקלה על הפעילות הכפופה לה, אך בפועל נמשיך להיזדקק לבדיקה פרטנית של החקיקה הרלוונטית במדינות החברות באיחוד האירופי.

[14] ראו הוראות בעניין זה בסעיף 27 ל – GDPR.

עקרונות הגנת המידע

המלצה לפעולה	✓ יש לעבור ולעדכן את נוהלי החברה הרלוונטיים, קוד ההתנהגות של החברה, הסכמי העסקה של עובדי החברה, התקשרויות חוזיות של החברה עם לקוחות וספקים, מסמכי מדיניות הפרטיות ואבטחת המידע הארגוניים ואלה המכוונים כלפי לקוחות החברה - כדי שיכללו התייחסות הולמת לעקרונות הגנת המידע. ✓ יש לערוך הדרכה מתאימה לעובדי החברה ביחס לעקרונות הגנת המידע.

סעיפים רלוונטיים	סעיף 5 ל – GDPR וסעיף 39 לדברי האקדמה.

כללית, ה – GDPR שומר על מבנה עקרונות הגנת המידע הקיים בדירקטיבת הגנת המידע, בהבדל אחד אך רב משמעות – ל – GDPR נוספה הוראה מפורשת לפיה על בעלי השליטה במידע להיות בעלי יכולת להראות שהם מציייתים לעקרונות הגנת המידע (Demonstration of Compliance with the GDPR).

מהוראה זו נגזרות שורה של פעולות נדרשות של תיעוד ובכלל זה שימוש בכלים טכנולוגיים שיאפשרו לבעלי השליטה במידע להציג ראיות אלקטרוניות המוכיחות שהם ביצעו את הנדרש מהם על פי דין.

אלה הם ששת עקרונות הגנת המידע:

- **חוקיות**: מידע אישי יעובד באופן חוקי, הוגן ובשקיפות.
- **מגבלת מטרה**: מידע אישי ייאסף למטרות מוגדרות, מסוימות ולגיטימיות ולא יעובד, אלא למטרות הללו. עיבוד למטרות נוספות כדוגמת ארכוב ומטרות לטובת הציבור, לצורכי מדע, מחקר היסטורי, סטטיסטי, לא ייחשב כחורג ממגבלת מטרות השימוש.
- **מזעור מידע**: מידע אישי יעובד באופן הולם, רלוונטי ומוגבל לנדרש בקשר עם מטרות העיבוד.
- **דיוק**: מידע אישי יהיה מדויק והיכן שנדרש, יישמר מעודכן. מידע לא מדויק יימחק או יתוקן ללא דיחוי.
- **תקופת שמירה**: מידע אישי יישמר באופן המאשר זיהוי של נושאי המידע לפרק זמן שאיננו עולה על הנדרש לשם מימוש מטרות עיבוד המידע. מידע יכול להישמר למטרות ארכוב ומטרות נוספותבכפוף לאבטחתו כראוי ולשמירת זכויות נושאי המידע.
- **שלמות וסודיות**: מידע אישי יעובד באופן המבטיח אבטחה ראויה שלו, לרבות הגנה מפני עיבוד בלתי מורשה או לא חוקי וכן מפני אובדן, השמד ונזק, תוך שימוש באמצעים טכנולוגיים וארגוניים מתאימים.

חוקיות עיבוד המידע ומטרות נוספות לעיבוד

המלצה לפעולה	✓ עליכם לבדוק אם תהליך קבלת ההסכמה שאתם מציעים הולם את דרישות ה – GDPR. ✓ ניהול מידע רגיש מחייב התייחסות מיוחדת. בדקו אם הנכם עומדים בדרישות הנוגעות לעיבוד מידע מסוג זה. ✓ בדקו אם עליכם למלא אחר הוראות הנוגעות לפרטיות ילדים מתחת לגיל 16. ✓ אם פעילות במידע נשענת על 'אינטרס לגיטימי', עליכם להיות מוכנים להראות את תהליך קבלת ההחלטות המתועד שהוביל אתכם להחלטה בעניין זה.

סעיפים רלוונטיים	סעיפים 6, 7, 8, 9 ל – GDPR וסעיפים 41-50 לדברי האקדמה.

ה – GDPR חוזר במידה רבה על התנאים לעיבוד חוקי של מידע אישי, שקבועים בדירקטיבת הגנת המידע, אולם כולל הגדרות ומגבלות חדשות בנוגע לתנאים אלה.

אלה הם ששת התנאים החלופיים לעיבוד מידע אישי באופן חוקי:

- הסכמת נושא המידע.
- עיבוד המידע נחוץ לביצוע חוזה עם נושא המידע או כדי לערוך חוזה כזה.
- עיבוד המידע נחוץ כדי לציית לחובה חוקית.
- עיבוד המידע נחוץ כדי להגן על אינטרס חיובי של נושא המידע או של אדם אחר, כאשר נושא המידע איננו מסוגל לתת את הסכמתו.
- עיבוד המידע נחוץ כדי לבצע משימה לצורך האינטרס הציבורי או במהלך ביצוע סמכות רשמית שניתנה בידי בעל השליטה במידע.
- עיבוד המידע נחוץ לצורך אינטרס לגיטימי.

מבין התנאים הללו בחרנו לעמוד על העיקריים שבהם ובכלל זה: מושג ההסכמה לפי ה – GDPR, תוך התייחסות נפרדת להסכמת קטינים ולהסכמה בעניין ניהול מידע רגיש, עיבוד נוסף שאיננו מבוסס על הסכמה וכן עיבוד מידע לצורך אינטרסים לגיטימיים.

מושג ההסכמה

המלצה לפעולה	✓ יש לעבור על כלל תהליכי קבלת ההסכמה ולוודא שהם עומדים בדרישות ה – GDPR. ✓ יש להוסיף להודעות ומסמכי מדיניות הפרטיות הוראות בעניין האפשרות לבטל את ההסכמה. ✓ יש להוסיף מנגנונים התומכים בביטול הסכמה. ✓ יש לבחון את כלל מטרות השימוש הנדרשות ולבדוק אם איזה מהן איננה נדרשת לצורך ביצוע החוזה עם נושאי המידע. ככל שכך, יש לקיים דיון מיוחד בנושא זה.

לתוכן העניינים

סעיפים רלוונטיים	סעיף 7 ל – GDPR וסעיפים 32-33, 42-43 לדברי האקדמה.

ה – GDPR מגדיר בסעיף 4 הסכמה כחיווי שניתן באופן חופשי, מסוים, מודע וחד-משמעי של רצונותיו של נושא המידע, שבאמצעותו, בדרך של הצהרה או פעולה ברורה ומחייבת (affirmative), נושא המידע מעיד על הסכמתו לעיבוד המידע האישי הנוגע אליו.

סעיף 32 לדברי האקדמה מבאר למה הכוונה ב"חיווי חד משמעי" של רצון נושא המידע. חיווי כזה יכול להיות –

- בכתב או באמצעי אלקטרוני וכן באמצעות הצהרה בעל פה;
- באמצעות הקשה על תיבת סימון באתר אינטרנט;
- בדרך של בחירה מתוך הגדרות בשירות חברת המידע[15];
- כל פעולה או הצהרה אחרת המביעה באופן ברור את הסכמת נושא המידע.

שתיקה איננה יכולה להיחשב כהסכמה. באותה מידה, תיבת סימון שמסומנת כברירת מחדל לא תהווה אינדיקציה להסכמת נושא המידע.

סעיף 7 ל – GDPR כולל הוראות בעניין מהות ההסכמה הנדרשת. לפיו, על בעל השליטה במידע להיות בעל היכולת להראות שנושאי המידע אכן נתנו את הסכמתם לעיבוד המידע.[16] בנוסף, ההסכמה צריכה לעמוד בתנאים הבאים:

- **מובנת ונגישה.** הסכמה למסמך בכתב צריכה להיות ניתנת להבחנה (distinguishable) מתוכן המסמך עצמו, היא צריכה להיות מובנת ונגישה בקלות וצריכה להיות בשפה פשוטה ומובנת.
- **ניתנת לביטול**. נושא מידע יכול לבטל הסכמה שמסר. ביטול ההסכמה צריך להיות קל ופשוט בדיוק כמו קבלת ההסכמה. ביטול ההסכמה לא יפגע בחוקיות עיבוד המידע בהתבסס על ההסכמה, לפני שבוטלה, אך נושאי המידע צריכים להיות מודעים לכך.
- **הסכמה לאיסוף מידע שלא למטרת השירות**. כאשר מעריכים אם הסכמה ניתנה מרצון חופשי, יילקח בחשבון באופן המרבי אם ביצוע החוזה עם נושא המידע (לדוגמה, אספקת השירות), מותנה בכך שנושא המידע ימסור מידע שאיננו נדרש לצורך ביצוע החוזה. זוהי דרישה לא פשוטה שהיקפה עדיין לא ברור. לדוגמה, האם בעל שירות יכול לאסוף ולהשתמש במידע אישי גם לצורך המשך פיתוח השירות ולא רק כדי לספק אותו? נראה בכל אופן שהמחוקק רומז ברמז עבה שלא ניתן לאסוף מידע אישי שאיננו נדרש לצורך אספקת השירות.[17]
- **הסכמה לאיסוף מידע למחקר מדעי**. ה – GDPR מכיר בכך שלעתים קרובות, בעת איסוף המידע לצרכי מחקר מדעי, לא ניתן לדעת את כל מטרות השימוש במידע. לפיכך הוא קובע שיש לאפשר לנושאי המידע לתת הסכמה לתחומי מחקר מסוימים כאשר הדבר תואם סטנדרטיים אתיים מוכרים וכן לאפשר להם לתת הסכמה רק לתחומי מחקר מסוימים, או לחלקים מסוימים של פרויקטי מחקר, ככל שהדבר מתאפשר על ידי מטרת השימוש.[18]

---

15 ראו הגדרה לשירות חברת המידע בסעיף ההגדרות.
16 אנו ממליצים מזה שנים לתעד ולשמור את הלוגים של פעולות ההקשה על "אני מסכים" המעידות על הסכמת המשתמש לאמור במדיניות הפרטיות.
17 ראו גם את האמור בסעיף 43 לדברי האקדמה.
18 ראו בסעיף 33 לדברי האקדמה.

לתוכן העניינים

הגנה על קטינים

המלצה לפעולה	✓ שירות אינטרנטי המוצע במישרין לילדים מחויב למסד מנגנון לקבל הסכמת הורים ולוודא שהודעות הפרטיות מנוסחות כהלכה. ✓ חברות שעברו תהליך ציות ל – Children Online Privacy Protection Act (COPPA) האמריקני, קרוב לוודאי שתוכלנה להסתמך במידה רבה על המנגנונים שיושמו לצורך זה, כיוון שעקרונות ההגנה על מידע על ילדים לפי ה – GDPR דומים למדי. ✓ חברות השייכות לתעשיית הפרסום האינטרנטי המבוססת על מידע התנהגותי צריכות לבצע הערכת מצב בקשר עם ההוראות בנושא ילדים.

סעיפים רלוונטיים	סעיפים 8, 12, 57 ל – GDPR וסעיפים 38 ו - 58 לדברי האקדמה.

דירקטיבת הגנת המידע, אותה החליף ה – GDPR, לא כללה הוראות כלשהן המכוונות באופן ספציפי לעיבוד מידע אישי על ילדים. להבדיל, ה – GDPR כולל מספר הוראות הנוגעות לילדים. הן מפוזרות במספר מקומות, הן בסעיפי ה – GDPR והן בדברי האקדמה לו. נציג להלן את העיקריות שבהן:

- סעיף 8 ל – GDPR קובע הוראה לפיה אם נעשה עיבוד מידע אישי במסגרת שירות חברת המידע[19] המוצע במישרין לקטין מתחת לגיל 16, הרי שעיבוד המידע יהיה חוקי רק אם ההסכמה ניתנה או אושרה על ידי הורה או אפוטרופוס של הקטין. מדינות החברות באיחוד האירופי יכולות להנמיך את הגיל שמכוחו נדרשת הסכמת הורים ל – 13.

- היות שההסדר ב – GDPR מכוון לשירותי חברת המידע, שהם בעיקרם שירותים אינטרנטיים, ההסדר איננו נוגע לשירותים שאינם מקוונים (offline). אלה ימשיכו להיות תחת הסדרה מדינתית.

- ה – GDPR איננו מציין מנגנון ספציפי כלשהו המתחייב לצורך קבלת הסכמת ההורים, אלא קובע כי על בעל השליטה במידע לעשות מאמצים סבירים לוודא את הסכמת ההורים, בהתאם לכלים הטכנולוגיים הזמינים.

- סעיף 12 ל – GDPR מחייב דגש מיוחד על הפשטות והבהירות של ההודעות לילדים בקשר לשימוש במידע עליהם.[20] שימו לב שהמונח "ילד" איננו מוגדר ולכן הוא עשוי להיות תקף גם לנוער.

- לפי סעיף 6(1)(f) ל – GDPR, היכולת להשתמש באינטרס לגיטימי כבסיס לעיבוד מידע אישי, קטנה יותר כאשר מדובר במידע על ילדים.

- שימוש במידע אישי על ילדים לצורכי שיווק ויצירת פרופילים הוא נושא הדורש הגנה מיוחדת.[21] מנגד, אין צורך בהסכמת הורים בהקשר לשירותי ייעוץ ומניעה לילדים.[22]

- בהתאם לסעיף 57(1)(b), כאשר רשויות ההגנה על המידע נוקטות בפעולות להעלאת המודעות ולהבנת הסיכונים, הכללים, אמצעי ההגנה והזכויות בקשר עם עיבוד של מידע אישי, עליהן לתת תשומת לב מיוחדת לפעילויות הנוגעות לילדים.

19 ראו הגדרה לשירות חברת המידע בסעיף ההגדרות.
20 ראו גם את ההסבר בסעיף 58 לדברי האקדמה.
21 ראו בסעיף 38 בדברי האקדמה.
22 שם.

לתוכן העניינים

תנאים לעיבוד מידע בקטגוריות מיוחדות ("מידע רגיש")

המלצה לפעולה	✓ בידקו אם הנכם מעבדים מידע באחת או יותר מהקטגוריות המיוחדות המצוינות ב – GDPR. לדוגמה, חברה המפעילה משרד באירופה המחייב זיהוי ביומטרי (טביעת אצבע, סריקת כף יד וכיו"ב) לצורך כניסה למשרד. יש לוודא שמתקבלת הסכמה מתאימה.

סעיפים רלוונטיים	סעיפים 4 (הגדרת מידע גנטי ומידע ביומטרי), 9 ו-10 ל – GDPR. סעיפים 34, 35, 41, 53, 71 לדברי האקדמה.

בהתאם לסעיף 9 ל – GDPR אסור לעבד מידע אישי החושף מוצא גזעי או אתני, דעות פוליטיות, אמונות דתיות או פילוסופיות, חברות באיגוד מקצועי וכן אסור לעבד מידע גנטי, מידע ביומטרי לצורך זיהוי חד ערכי של אדם, וכן אסור לעבד מידע הנוגע לבריאות או מידע הנוגע לחיי המין או לזהותו המינית של אדם.

הקטגוריות המיוחדות של המידע אינן כוללות מידע אישי הנתפס בישראל כמידע רגיש כדוגמת מידע כלכלי ומידע פלילי.

ה – GDPR כולל הסדר נפרד לגבי מידע הנוגע לעבירות פליליות והרשעות ולפיו ניתן לעבד מידע מסוג זה בתנאי שהעיבוד נעשה תחת פיקוח של רשות מוסמכת או כאשר העיבוד מותר בדין מדינתי.[23] הוראה זו מנציחה איפוא שונות בדינים של המדינות החברות באיחוד האירופי בהקשר זה.

לאיסור הגורף הנ"ל יש חשיבות הצהרתית והוא נועד להפריד באופן ברור בין סוגי המידע המופיעים בו, לבין כלל סוגי המידע האישי. מייד לאחר האיסור הנ"ל, קובע ה – GDPR שבכל זאת אפשר לעבד מידע רגיש אם מתקיים אחד מהתנאים הבאים:

- נושא המידע מסר את הסכמתו המפורשת לעיבוד המידע עליו, למעט אם דין מדינתי אוסר את עיבוד המידע גם אם נתקבלה הסכמה כזו.[24]
- עיבוד המידע נדרש לצורך ביצוע חובות הנדרשות בהקשר לדיני עבודה, ביטוח לאומי או הסכם קיבוצי.
- עיבוד המידע נדרש כדי להגן על אינטרסים חיוניים של נושא המידע שאיננו מסוגל לתת הסכמה בשל מגבלה פיסית או מנטאלית.
- עיבוד המידע הכרחי לצורכי הליכים משפטיים, לצורך אינטרס ציבורי מהותי, לצורכי בריאות העובד או בריאות הציבור, לצורך ארכוב המשרתים את האינטרס הציבורי וכן לצרכי מחקר מדעי והיסטורי, או לצרכים סטטיסטיים.
- עיבוד המידע נעשה על ידי גוף ללא מטרות רווח עם מטרה פוליטית, פילוסופית או דתית, או שהוא איגוד מקצועי, בכפוף לכך שעיבוד המידע נוגע רק לחברים או לחברים לשעבר ומידע לא יועבר לצדדים שלישיים ללא קבלת הסכמה.
- נושא המידע פרסם לציבור את המידע.[25]

---

[23] ראו סעיף 10 ל – GDPR.

[24] השוו לסעיפים 29 ו – 30 לחוק מידע גנטי, תשס"א – 2000, האוסרים שימוש במידע גנטי לצורכי קבלה לעבודה וביטוח. בהקשרים אלה, הסכמת נושא המידע איננה מעלה או מורידה. זוהי גישה פטרנליסטית, אליה מכוון גם ה – GDPR.

[25] שאלה מעניינת יכולה לעלות אם ההוראה הזו חלה גם כאשר נושא המידע פרסם את המידע בטעות.

לתוכן העניינים

ה – GDPR מוסיף שמדינות החברות באיחוד האירופי יכולות להוסיף ולחוקק חוקים ספציפיים בנוגע למידע גנטי, מידע ביומטרי ומידע בריאותי.

עיבוד נוסף שאיננו מבוסס על הסכמה

המלצה לפעולה	✓ הישענות על מטרות עיבוד נוסף שלא התקבלה לגביהן הסכמה נושאת בחובה מקדם סיכון שכדאי להימנע ממנו. לעולם עדיף לבנות מראש את ההסכמה המתקבלת באופן שצופה בצורה המיטבית את כלל מטרות השימוש. ✓ אם נוצר הצורך להישען על מטרת עיבוד נוסף שלא התקבלה לגביה הסכמה, יש ליצור תהליך קבלת החלטה מסודר ומתועד היטב המתאר את שקילת השיקולים הנדרשים והגעה למסקנה סבירה המתירה את השימוש הנוסף.

סעיפים רלוונטיים	סעיף 6(4) ל – GDPR.

לפי ה – GDPR בעל השליטה במידע רשאי להורות על עיבוד מידע למטרה חדשה השונה מהמטרה שלשמה נאסף המידע מלכתחילה ושנושאי המידע לא נתנו את הסכמתם אליה. ה – GDPR קובע כי בעל השליטה צריך לשקול אם המטרה החדשה תואמת את המטרות המקוריות שלשמן נאסף המידע ולצורך זה עליו לשקול את השיקולים הבאים:

- הקשר שבין המטרות המקוריות והמטרה החדשה;
- ההקשר שבו נערך איסוף המידע מלכתחילה ובמיוחד הקשר שבין בעל השליטה במידע לבין נושאי המידע;
- מהות המידע, לרבות אם המידע הוא מידע רגיש;
- ההשלכות האפשריות הנובעות מעיבוד המידע לצורך המטרה החדשה;
- קיומם של אמצעים לאבטחת המידע, גם בהקשר של המטרה החדשה, לרבות הצפנה ופסאודונימיזציה.

זהו חריג מעניין המאפשר הלכה למעשה לעבד מידע אישי ללא קבלת הסכמה מנושאי המידע. עם זאת, מתוך ההקשר הכללי והשיקולים המוצגים לעיל, נראה שחריג זה הוא צר למדי.

עיקרון האינטרס הלגיטימי

המלצה לפעולה	✓ יש להיערך להוסיף לכל ההודעות לנושאי המידע ומסמכי מדיניות הפרטיות, תוכן מפורש הכולל שימושים במידע שייחשבו כשימושים שנועדו לשרת אינטרסים לגיטימיים.

סעיפים רלוונטיים	סעיפים 6(1)(f), 13(1)(d) ו – 14(2)(b) ל – GDPR. סעיפים 47-50 לדברי האקדמה.

ה – GDPR חוזר על עיקרון שהיה קיים בדירקטיבת הגנת המידע ולפיו אם יש אינטרס לגיטימי לעיבוד המידע, הרי שאינטרס זה יהווה בסיס חוקי לעיבוד. במלים אחרות, אינטרס לגיטימי מהווה תחליף לקבלת הסכמה מנושא המידע.

המושג "אינטרס לגיטימי" הוא זר לדין הישראלי. הוא איננו מופיע כבסיס לעיבוד חוקי של מידע אישי. הוא אף איננו מופיע (לפחות לא במפורש) כאחת ההגנות המופיעות בסעיף 18 לחוק הגנת הפרטיות הישראלי.

מהו אינטרס לגיטימי? זו שאלה שהאיחוד האירופי התחבט בה רבות במשך שנים, לרבות בתהליך חקיקת ה – GDPR שנמשך ארבע שנים. גם ב – GDPR לא נמצא הגדרה המשרטטת בצורה מדויקת את גבולות המונח הזה. עם זאת, נמצא מספר כלי עזר שיסייעו בהבנת המושג:

בניגוד לדירקטיבת הגנת המידע, בהתאם ל – GDPR, רשויות ציבוריות לא יכולות להשתמש באינטרסים לגיטימיים כדי להצדיק עיבוד מידע אישי.

על פי ה – GDPR, לא ניתן להשתמש בטיעון של קיומו של אינטרס לגיטימי, כאשר התוצאה היא פגיעה בזכויות והחרויות הבסיסיות של נושאי המידע (ובמיוחד כאשר נושאי המידע הם ילדים), תוך לקיחה בחשבון של הציפיות הסבירות של נושאי המידע בהתבסס על הקשר שלהם עם בעל השליטה במידע, לדוגמה, כאשר נושא המידע הוא לקוח של בעל השליטה במידע או פועל בשירותו.[26]

דברי האקדמה ל – GDPR מפרטים דוגמאות לעיבוד מידע שיכול להיחשב הכרחי לאינטרס לגיטימי של בעל השליטה במידע. אלה כוללים לדוגמה –

- מניעת הונאות ושיווק ישיר;[27]
- העברת מידע בין חברות בקבוצת חברות לצורך ניהול אדמיניסטרטיבי של המידע;[28]
- אבטחת מידע ואבטחת תקשורת, לרבות מניעת גישה בלתי מורשית לרשתות תקשורת אלקטרונית ועצירת נזק למערכות מחשב ותקשורת;[29]
- דיווח לרשויות על פעילות פלילית או פעילות הנוגעת לביטחון הציבור.[30]

על אף שקיומו של אינטרס לגיטימי פותר את בעל השליטה במידע מקבלת הסכמה מנושאי המידע, עדיין, ה – GDPR מחייב את בעל השליטה במידע לתת הודעה בדבר האינטרסים הלגיטימיים לעיבוד המידע, במסגרת ההודעות שהוא מוסר לנושאי המידע.[31]

התוצאה היא איפוא, שאין מדובר בהקלה, אלא דווקא בדרישה נוספת. נדרש עתה לציין במפורש במסמכי מדיניות הפרטיות, לדוגמה, את האינטרסים הלגיטימיים לעיבוד המידע.

---

26 ראו סעיף 47 לדברי האקדמה.
27 שם.
28 ראו סעיף 48 לדברי האקדמה.
29 ראו סעיף 49 לדברי האקדמה.
30 ראו סעיף 50 לדברי האקדמה.
31 ראו סעיפים 13(1)(d) ו – 14(2)(b) ל – GDPR.

זכויות הפרט הקיימות והחדשות

הודעה בדבר איסוף המידע

המלצה לפעולה	✓ יש לעדכן את ההודעות לנושאי המידע ואת מסמכי מדיניות הפרטיות, באופן שישקף את הדרישות של המחוקק האירופי וכן לוודא ששפת המסמכים תמציתית, נהירה ופשוטה.

סעיפים רלוונטיים	סעיפים 12, 13 ו-14 ל – GDPR. סעיפים 58-62 לדברי האקדמה.

על בעל השליטה במידע מוטלת החובה לספק הודעה לנושאי המידע אודות איסוף המידע. החוק מדגיש את הצורך במתן הודעה תמציתית, מובנת וברורה שתינתן בשקיפות מלאה ובשפה פשוטה (במיוחד כאשר נושאי המידע הם ילדים).

כאשר המידע נאסף מנושא המידע, ההודעה צריכה להכיל את הפרטים הבאים:

- זהות ופרטי ההתקשרות של בעל השליטה במידע;
- פרטי ההתקשרות של קצין הגנת המידע (ככל שיש);
- הסיבות אשר לשמן נאסף המידע והבסיס המשפטי (או האינטרס הלגיטימי) לאיסוף;
- ככל שיש מקבלי מידע יש לציין את זהותם, באופן ספציפי או בקטגוריות;
- פרטים אודות העברת המידע לארגון בינלאומי או לגורם המצוי מחוץ לתחומי האיחוד האירופי, לרבות: כיצד תתבצע הגנת המידע אצל מקבל המידע הזר וכיצד נושאי המידע יכולים לעיין או לקבל עותק מכללי שמירת המידע של מקבל המידע הזר;
- תקופת שמירת המידע ואם לא ניתן לחזות אותה – פירוט של הקריטריונים לקביעת תקופת שמירת המידע.
- פרטים אודות זכות הגישה למידע של נושא המידע וכן על זכותו של נושא המידע לפנות אל בעל השליטה במידע על מנת למחוק, לתקן או להגביל את המידע.
- פרטים אודות הזכות של נושא המידע להתנגד לעיבוד המידע. במידה ועיבוד המידע מבוסס על הסכמת נושא המידע יש לציין גם פרטים לגבי אופן ביטול הסכמה זו.
- פרטים לגבי זכותו של נושא המידע לפנות בתלונה לרשות המפקחת.
- פרטים אודות החובה הסטטוטורית או החוזית שבגינה על נושא המידע לספק את המידע וכן פרטים לגבי ההשלכות של התנגדות למתן המידע.
- פרטים אודות תהליכי קבלת החלטות אוטומטיים (ככל שישנם) ועל ההשלכות הצפויות מעיבוד המידע.

כאשר בעל השליטה במידע מתכוון לעבד את המידע למטרות נוספות פרט למטרות אשר לשמן התקבל המידע עליו לספק לנושא המידע פרטים על מטרות אלה לפני עיבוד המידע למטרות הנוספות.

לתוכן העניינים

במקרים בהם המידע נאסף מגורם אחר יש צורך במתן הודעה לנושא המידע, אשר תכיל את הפרטים המפורטים לעיל ובנוסף את הפרטים הבאים:

- הקטגוריות של המידע האישי הנאסף.
- מהו המקור ממנו נאסף המידע והאם נמסר מגורם פומבי.

כשהמידע נאסף מגורם שאיננו נושא המידע, על בעל השליטה במידע לספק את ההודעה בדבר איסוף המידע:

- תוך תקופת זמן סבירה בהתחשב בנסיבות הספציפיות של איסוף ועיבוד המידע , אך לא יותר מחודש ימים ממועד קבלת המידע אודות נושא המידע.
- כאשר המידע נאסף לצורך יצירת קשר עם נושא המידע – לכל המאוחר במועד ההתקשרות הראשונה עם נושא המידע.
- אם המידע צפוי להיחשף בפני גורם אחר – לא יאוחר ממועד חשיפת המידע כלפי אותו גורם.

הזכות לקבלת מידע

המלצה לפעולה	✓ יש להיערך למתן הודעות לבקשת נושאי המידע ולמתן גישה למידע (במלואו או בחלקו). ✓ יש לבחון מה במידע הנאסף עלול לפגוע בזכויות בעל השליטה במידע וכיצד ניתן להצדיק את אי חשיפתו.

סעיפים רלוונטיים	סעיף 15 ל – GDPR. סעיפים 63 ו-64 לדברי האקדמה.

לנושא המידע הזכות לקבל פרטים מבעל השליטה במידע לגבי השאלה האם מידע אודותיו מעובד על ידי בעל השליטה. במידה והתשובה לשאלה זו חיובית על בעל השליטה במידע לספק לנושא המידע גישה לכל אותו מידע אישי הנוגע לנושא המידע וכן את הפרטים הבאים:

- הסיבות לעיבוד המידע.
- הקטגוריות של המידע האישי הנאסף.
- זהותם של מקבלי המידע (באופן ספציפי או בקטגוריות) אשר קיבלו או יקבלו את המידע האישי ובפרט את זהותם של מקבלי מידע זרים (מקבלי מידע שהם ארגונים בינלאומיים או מקבלי מידע שמצויים בטריטוריות אשר מחוץ לתחומי האיחוד האירופי). כאשר ישנם מקבלי מידע זרים, נושא המידע זכאי גם לקבל פרטים אודות כללי הגנת המידע המיושמים על העברת המידע .
- תקופת שימור המידע ואם לא ניתן לחזות אותה – פירוט של הקריטריונים לקביעת תקופת שימור המידע .
- פרטים אודות זכותו של נושא המידע לפנות אל בעל השליטה במידע על מנת למחוק או לתקן את המידע ועל הזכות להגביל או להתנגד לעיבוד המידע .
- פרטים אודות הזכות של נושא המידע להתנגד לעיבוד המידע . במידה ועיבוד המידע מבוסס על הסכמת נושא המידע, יש לציין גם פרטים כיצד ניתן לבטל הסכמה זו.
- פרטים לגבי זכותו של נושא המידע לפנות בתלונה לרשות המפקחת.
- כאשר המידע נאסף מגורם שאיננו נושא המידע עצמו יש לספק פרטים אודות הגורם אשר ממנו נאסף המידע .
- פרטים אודות תהליכי קבלת החלטות אוטומטיים (ככל שישנם) ועל ההשלכות הצפויות מעיבוד המידע.

בעל השליטה במידע ימציא לנושא המידע עותק של המידע האישי המעובד על ידו ללא תשלום ובמידה והבקשה של נושא המידע הועברה באופן אלקטרוני ניתן להמציא את המידע המבוקש גם באופן אלקטרוני. בעל השליטה במידע רשאי לגבות את עלות הוצאות המשרד הכרוכות בהפקת עותקים נוספים של המידע האישי, ככל שאלה יתבקשו על ידי נושא המידע.

בדברי האקדמה מוצע לבעל השליטה במידע לספק לנושאי המידע מערכת אלקטרונית מאובטחת אשר תקנה לנושאי המידע גישה ישירה להפקת הנתונים.

עוד נכתב בדברי האקדמה, כי בעל השליטה במידע צריך לנקוט באמצעים סבירים על מנת לאמת את זהותו של נושא המידע אשר ביקש את הגישה למידע אודותיו, בפרט כאשר מדובר על בקשה וגישה מקוונים של נושא המידע. בעל השליטה במידע לא נדרש לשמור מידע רק במטרה לספק אותו לנושאי המידע.

המחוקק האירופי מודע לכך שגישה של נושאי המידע למלוא מסד הנתונים של בעל השליטה במידע עלולה להוביל גם לחשיפת סודות מסחריים ולפגיעה בזכויות אחרות של בעל השליטה במידע ולכן החוק מציין במפורש כי זכות הגישה למידע לא תפגע בזכויות וחרויות של הזולת.

עם זאת, דברי האקדמה מציינים כי סירוב גורף ליתן גישה לכלל המידע איננו מקובל. ניתן, למשל, במקרים בהם מדובר בכמויות גדולות של מידע אודות נושא המידע, לבקש מנושא המידע לציין מה המידע או פעילויות העיבוד הספציפיות אשר הוא מעוניין לקבל פרטים אודותם.

הזכות לתקן מידע והזכות להימחק ('הזכות להישכח')

המלצה לפעולה	✓ יש לנקוט במדיניות השמדת מידע של מידע שאיננו רלוונטי או מידע שאיננו נדרש עוד למטרות אשר לשמן נאסף. ✓ יש להכין מדיניות מסודרת של האופן בו יינתן מענה לבקשות לתיקון ולמחיקת מידע .

סעיפים רלוונטיים	סעיפים 16 ו-17 ל – GDPR. סעיפים 65 ו-66 לדברי האקדמה.

נושא המידע זכאי לתיקון אי דיוקים וטעויות במידע אודותיו ולהשלמת מידע שאיננו שלם אודותיו ללא דיחוי מצד בעל השליטה במידע.

בנוסף, ה-GDPR עיגן לראשונה את הזכות שהוכרה על ידי בית הדין האירופי בהחלטתו ממאי 2014 – הזכות להישכח.[32]

לנושא המידע הזכות לדרוש את מחיקת המידע אודותיו ולבעל השליטה יש את החובה למחוק את המידע אודות נושא המידע, ללא דיחוי, במקרים הבאים:

- ❖ המידע האישי לא נדרש עוד בהקשר של המטרות אשר לשמן נאסף.
- ❖ איסוף ועיבוד המידע מבוססים על הסכמתו של נושא המידע ונושא המידע ביטל את הסכמתו.
- ❖ נושא המידע מתנגד לעיבוד המידע בהתאם לזכותו להתנגד לעיבוד המידע וליצירת פרופיל התנהגותי (סעיף 21 ל-GDPR אשר יפורט בהמשך) ואין עילה לגיטימית לעיבוד המידע .
- ❖ המידע עובד באופן בלתי חוקי.
- ❖ מחיקת המידע נדרשת כדי לעמוד במחויבויות רגולטורית של האיחוד האירופי או של מדינה חברה אשר בעל השליטה במידע כפוף לחוקיה.
- ❖ המידע נאסף כדי לספק הצעה למתן שירותי חברת המידע.[33]

במקרים בהם בעל השליטה במידע הפך את המידע האישי לפומבי וחלה עליו החובה כעת לממש את זכותו של נושא המידע ולמחוק את המידע, על בעל השליטה במידע לנקוט באמצעים סבירים (בהתחשב במגבלות טכנולוגיות ובהוצאות הכרוכות ביישום ההוראה) ליידע בעלי שליטה אחרים שמעבדים את המידע אודות נושא המידע, על כך שנושא המידע ביקש למחוק את המידע אודותיו.

ההוראות בעניין הזכות להישכח לא חלות כאשר עיבוד המידע נדרש למטרות הבאות:

- ❖ מימוש הזכות לחופש ביטוי או לחופש המידע.

[32] ראו את החלטת ה – CJEU מיום 13.5.2014 בעניין Case C-131/12 Google Spain SL, Google Inc. v. Agencia Espanola de Protection de Datos, Mario Costeja Gonzalez

[33] ראו הגדרה לשירות חברת המידע בסעיף ההגדרות.

- כאשר העיבוד נדרש לצורך מילוי חובה חוקית הנדרשת על ידי האיחוד האירופי או על ידי מדינה חברה אשר בעל השליטה במידע כפוף להוראותיה וכאשר עיבוד המידע נדרש לטובת מילוי אינטרס ציבורי שנתבקש על ידי רשות מוסמכת אשר בעל השליטה במידע כפוף לה.
- לטובת אינטרס ציבורי הנוגע לבריאות הציבור.
- למטרות ארכוב לטובת הציבור, מטרות מחקר מדעי, מחקר היסטורי או איסוף של נתונים סטטיסטיים.
- לצורך הגנה מפני טענות ותביעות משפטיות.

הזכות להתנגד לעיבוד מידע

המלצה לפעולה	✓ יצירת חציצה לוגית אשר תאפשר להעביר קבצי מידע האסורים לעיבוד באופן שיאפשר את המשך הפעילות התקינה של עיבוד הנתונים השוטף.

סעיפים רלוונטיים	סעיף 18 ל – GDPR. סעיף 67 לדברי האקדמה.

לנושא המידע הזכות להתנגד לעיבוד המידע על ידי בעל השליטה במידע ובעל השליטה במידע יחדל מעיבוד המידע במקרים הבאים:

- כאשר נושא המידע מערער על מידת הדיוק של המידע אודותיו יופסק העיבוד לתקופה שבה בעל השליטה במידע מאמת את המידע כאמור.
- כאשר המידע נאסף באופן לא חוקי ונושא המידע מתנגד למחיקת הנתונים ודורש את הגבלת השימוש במידע במקום.
- כאשר המידע אינו נדרש לבעל השליטה במידע לצרכים אשר לשמם המידע נאסף אך יש צורך בשימורו להגנה מפני טענות או תביעות משפטיות.
- כאשר נושא המידע התנגד לעיבוד המידע ויצירת פרופיל התנהגותי (סעיף 21 ל-GDPR אשר יפורט בהמשך) יש לחדול את העיבוד עד למועד קבלת אישור כי העילה הלגיטימית של בעל השליטה במידע גוברת על זכותו של נושא המידע.

כאשר בקשת נושא המידע עומדת באחד מהתנאים המפורטים לעיל על בעל השליטה במידע לחדול מכל עיבוד של המידע אך הוא רשאי לאחסנו.

על אף האמור לעיל, עיבוד המידע יתאפשר:

- בהסכמת נושא המידע.
- כאשר יש צורך בעיבוד המידע לצורך הגנה מפני תביעות או טענות משפטיות או כדי להגן על אדם או ישות משפטית אחרת.
- במקרים של אינטרס ציבורי חשוב של האיחוד האירופי או של מדינה חברה.

על בעל השליטה במידע ליידע את נושא המידע בטרם יסיר את מגבלת עיבוד המידע שנתבקשה.

בדברי האקדמה מוצעות שיטות שיסייעו לבעלי השליטה במידע להגביל את עיבוד המידע כמו: העברת המידע המוגבל למערכת עיבוד אחרת, הגבלת הגישה של משתמשים למידע שאסור בעיבוד או הסרה זמנית של פרסומים המכילים את המידע האסור לעיבוד מאתרי אינטרנט.

כאשר המידע מעובד באופן אוטומטי יש להשתמש באמצעים טכניים כדי לאפשר לנושא המידע להתנגד ולהפסיק את עיבוד המידע המבוקש.

עדכון מקבלי המידע והעברת פרטי מקבלי המידע לנושא המידע

בעל השליטה במידע יעביר הודעה לגבי כל תיקון, מחיקה או הגבלת עיבוד המידע גם לכל מקבלי המידע, אלא אם כן העברת הודעה שכזו בלתי אפשרית או כרוכה במאמץ בלתי סביר. על בעל השליטה ליידע את נושא המידע אודות מקבלי המידע, במידה ונושא המידע ביקש זאת.

הזכות לניוד המידע

המלצה לפעולה	✓ יצירת פורמט הולם לניוד מידע של נושא המידע.

סעיפים רלוונטיים	סעיף 20 ל – GDPR. סעיף 68 לדברי האקדמה.

הזכות לניוד מידע היא זכות צרה אשר מאפשרת לנושא המידע לקבל לידיו את המידע אשר סופק על ידו (ולא על ידי גורמים אחרים) לבעל השליטה במידע בפורמט מוכר, מובנה וניתן לקריאה אלקטרונית וכן יש לו את הזכות להעביר את המידע לבעל שליטה במידע אחר במקרים הבאים:

- ❖ המידע עובד באופן אוטומטי (ללא רשומות נייר).
- ❖ המידע עובד בהסכמת נושא המידע או שמטרת העיבוד היא מילוי התחייבויות חוזיות.

נושא המידע רשאי לבקש כי המידע האמור יועבר ישירות מבעל שליטה במידע אחד למשנהו, כאשר הדבר ישים מבחינה טכנולוגית.

הזכות לניוד המידע לא פוגעת בזכויות והחירות של הזולת ולא פוגעת בזכותו של נושא המידע להישכח.

הזכות לניוד המידע לא חלה במקרים בהם עיבוד המידע נדרש לצורך אינטרס ציבורי.

הזכות להתנגד ליצירת פרופיל התנהגותי

המלצה לפעולה	✓ חברות העוסקות בדיוור ישיר צריכות ליצור נוהל למחיקה של פרופילים התנהגותיים של נושאי מידע. ✓ יש ליצור נוסח הודעה בדבר הזכות להתנגד ליצירת פרופיל התנהגותי.

סעיפים רלוונטיים	סעיף 21 ל – GDPR. סעיפים 69 ו-70 לדברי האקדמה.

נושא המידע רשאי להתנגד לעיבוד המידע וליצירת פרופיל התנהגותי באמצעותו, בהתבסס על הנסיבות הספציפיות הנוגעות למקרה, כאשר הבסיס לאיסוף המידע הוא כדי לבצע משימה לצורך האינטרס הציבורי או לצורך אינטרס לגיטימי. אם בעל השליטה במידע רוצה להמשיך בפעילות במידע על אף ההתנגדות, עליו להראות עילה לגיטימית אשר תגבר על האינטרסים של נושא המידע או להראות כי עיבוד המידע נעשה לצורך הגנה מפני תביעות או טענות משפטיות.

כמו כן, לנושא המידע יש זכות אבסולוטית להתנגד ליצירת פרופיל התנהגותי כאשר הסיבה ליצירת הפרופיל ההתנהגותי היא שיווק ישיר במידה ונושא המידע החליט על מימוש זכות זו על בעל השליטה לחדול מכל עיבוד של המידע למטרה זו.

על בעל השליטה במידע ליידע את נושא המידע בדבר הזכות להתנגד ליצירת פרופיל התנהגותי בעת ההתקשרות הראשונה עם נושא המידע, לכל המאוחר. הפרטים אודות הזכות יובאו לידיעת נושא המידע במפורש ובמנותק מכל מסמך אחר.

בנוסף, נושא המידע רשאי להתנגד ליצירת פרופיל התנהגותי כאשר מטרת יצירת הפרופיל היא מחקר מדעי, היסטורי או עבור צרכי סטטיסטיקה, בהתבסס על הנסיבות הספציפיות הנוגעות למקרה. ככל שעיבוד המידע נחוץ לביצוע משימה שבבסיסה אינטרס הציבור יגבר אינטרס הציבור על זכות ההתנגדות של נושא המידע.

במקרים בהם השירות הניתן הוא שירות מקוון על בעל השליטה במידע לאפשר לנושא המידע להתנגד ליצירת הפרופיל ההתנהגותי באמצעים טכנולוגיים.

הזכות להתנגד לתהליכי קבלת החלטות אוטומטיים

המלצה לפעולה	✓ יש ליצור מנגנוני הגנה ופיקוח אשר ימנעו קבלת החלטות אוטומטיות שגויות. ✓ יש לקבל את הסכמתם המפורשת של נושאי המידע לביצוע תהליכי עיבוד אוטומטיים.

סעיפים רלוונטיים	סעיף 22 ל – GDPR. סעיפים 71 ו-72 לדברי האקדמה.

לנושא המידע יש את הזכות להתנגד לעיבוד מידע שמתבצע באופן אוטומטי כאשר לאותו עיבוד מידע יש השלכות משפטיות או השלכות משמעותיות אחרות על נושא המידע. למשל, כאשר נושא המידע מקבל הודעת סירוב אוטומטית מאפליקציית אשראי מקוונת או כאשר מתקבלת החלטה לגבי נושא מידע במסגרת גיוס מקוון (e-recruiting).

דברי האקדמה גם מבארים כי בהשלכות משמעותיות אחרות הכוונה לתהליכי עיבוד אוטומטיים אשר תפקידם לנבא או לנתח את ביצועי העבודה של נושא המידע, את מצבו הכלכלי, הבריאותי, העדפותיו האישיות, אמינותו, התנהגותו, מיקומו, תנועתו וכו'.

לא ניתן יהיה לאסור את תהליך קבלת ההחלטות האוטומטי במקרים הבאים:

- ❖ תהליך העיבוד האוטומטי נדרש לצורך כניסה או ביצוע של חוזה בין נושא המידע לבעל השליטה במידע.
- ❖ תהליך העיבוד האוטומטי מורשה על ידי האיחוד האירופי או על ידי מדינה חברה אשר בעל השליטה במידע כפוף לה.
- ❖ תהליך העיבוד האוטומטי מבוסס על הסכמה מפורשת של נושא המידע.

במקרים בהם נושא המידע אינו יכול להתנגד לתהליכי עיבוד המידע האוטומטיים על בעל השליטה במידע לקבוע את אמצעי ההגנה על נושאי המידע אשר יבטיחו את השמירה על זכויותיהם, חרויותיהם והאינטרסים הלגיטימיים שלהם ולכל הפחות לאפשר לנושא המידע התערבות אנושית אשר תוכל לבטא את נקודת מבטו ולערער על ההחלטה האוטומטית.

בעל השליטה במידע מנוע מביצוע תהליכי קבלת החלטות אוטומטיים כאשר מדובר במידע רגיש אלא אם:

- ❖ התקבלה הסכמתו המפורשת והברורה של נושא המידע לביצוע תהליך העיבוד האוטומטי במידע .
- ❖ עיבוד המידע האמור נדרש לטובת אינטרס ציבורי משמעותי לאיחוד האירופי או למדינה חברה ובמקרה זה ביצוע התהליך יכרוך בתוכו מנגנוני הגנה על הזכויות והאינטרסים של נושאי המידע.

חובות בעל השליטה במידע ומעבד המידע

המלצה לפעולה	✓ התקשרות בהסכמים לעיבוד מידע המבוססים על דרישות ה – GDPR ; ✓ מינוי נציג באירופה ; ✓ תיעוד פעולות עיבוד המידע ; ✓ יש להיערך לאפשרות שרשות הגנת מידע אירופית תדרוש במישרין מידע ואף תערוך ביקורת אצל מעבד מידע ישראלי.

סעיפים רלוונטיים	סעיפים 24-31, 40, 42 ל – GDPR. סעיפים : 13, 81, 109 לדברי האקדמה.

חובות בעל השליטה במידע[34]

בעל השליטה במידע צריך ליישם אמצעים טכניים וארגוניים הולמים כדי להבטיח שהוא מסוגל להראות שעיבוד המידע האישי נעשה בהתאם להוראות ה – GDPR.

בעל השליטה במידע צריך לנסח וליישם מסמכי מדיניות הולמים. מסמכי מדיניות אלה משפטיים באופיים ולכן מומלץ להיוועץ עם עורך דין, הבקיא ב- GDPR.

ה – GDPR מעודד יצירת קודי התנהגות על ידי איגודים מקצועיים וכיו"ב[35] וכן מנגנוני הסמכה ואישור המעידים על כך שחברה או ארגון עומדים בדרישות ה – GDPR[36]. ה – GDPR מוסיף שעמידת בעל שליטה במידע בקודי התנהגות כאמור, או קבלת אישור כאמור על עמידה בדרישות החוק, ישמשו כאמצעי להוכחת הציות של בעל השליטה במידע להוראות ה – GDPR.

הנדסת הגנת מידע והגנת מידע כברירת מחדל (Data Protection by Design and by Default)[37]

מושגים אלה ידועים היטב בפרקטיקת ההגנה על המידע מזה זמן רב, אולם לא שולבו בדירקטיבת הגנת המידע. ה – GDPR תיקן מצב זה והתייחס אליהם באופן ספציפי.

הנדסה לפרטיות. בהתאם ל – GDPR, בעל השליטה במידע ליישם אמצעים טכניים וארגוניים הולמים להגנת המידע האישי, גם בשלב תהליך קבלת ההחלטות לגבי האמצעים לעיבוד המידע (דהיינו, שלב התכנון) וגם במהלך עיבוד המידע בפועל, כדוגמת פסאודונימיזציה.

פרטיות כברירת מחדל. בנוסף, על בעל השליטה במידע ליישם אמצעים טכניים וארגוניים הולמים לוודא שכברירת מחדל, יעובד רק המידע האישי הנדרש לצורך מימוש מטרות העיבוד. עיקרון זה נוגע לכמות וסוג המידע שנאסף, היקף העיבוד של המידע , תקופת האחסון של המידע וכללים לגישה אליו. בפרט יש לוודא שכברירת מחדל אין גישה ללא התערבות אדם למידע על מספר בלתי מוגבל של אנשים.

מנגנון הסמכה מאושר המעיד על עמידה בהוראות ה – GDPR[38] יכול להצביע על עמידה בהוראות הנוגעות להנדסת פרטיות ופרטיות כברירת מחדל.

---

34 ראו סעיף 24 ל – GDPR.
35 ראו סעיף 40 ל – GDPR.
36 ראו סעיף 42 ל – GDPR.
37 ראו סעיף 25 ל – GDPR.
38 ראו סעיף 42 ל – GPDR.

לתוכן העניינים

נציגים[39]

כאשר בעל השליטה במידע או מעבד המידע אינם בעלי נוכחות באיחוד האירופי, אך ה – GDPR חל על פעילותם, כיוון שהם מעבדים מידע על אנשים הנמצאים באיחוד האירופי בקשר עם אספקת מוצרים או שירותים, או בקשר עם ניטור התנהגות,[40] עליהם למנות נציג באיחוד האירופי.[41]

החובה למינוי נציג באיחוד האירופי לא תחול כאשר מתקיימים כל אלה: (1) מדובר בעיבוד מידע מזדמן בלבד; (2) עיבוד המידע אינו כולל מידע בקטגוריות מיוחדות בקנה מידה גדול; (3) אין בעיבוד המידע כדי להוות פגיעה ממשית בזכויות נושאי המידע.

הנציג חייב להיות בעל נוכחות במדינות האיחוד האירופי שמידע אישי של הנמצאים בה מעובד על ידי בעל השליטה במידע או מעבד המידע והוא צריך להיות בעל יפוי כוח הולם שיאפשר לו (במקום או בנוסף לבעל השליטה במידע או למעבד המידע) להיות הכתובת לפניות של נושאי מידע ושל רשויות הגנת המידע בקשר עם עיבוד המידע.

חובות מעבד המידע[42]

בעל שליטה במידע רשאי להשתמש במעבדי מידע, רק אם קיבל מהם התחייבויות חוזית הולמות לעמידה בהוראות ה– GDPR .

מעבד מידע איננו רשאי להתקשר עם מעבד-משנה (sub-processor) ללא אישור בכתב - כללי או ספציפי, מבעל השליטה במידע. אם מדובר באישור כללי, על מעבד המידע ליידע את בעל השליטה במידע על כל שינוי (לדוגמה, החלפת מעבד-משנה אחד באחר) ולאפשר לבעל השליטה במידע להתנגד לשינוי.

ה – GDPR מעודד יצירת קודי התנהגות על ידי איגודים מקצועיים וכיו"ב[43] וכן מנגנוני הסמכה ואישור המעידים על כך שחברה או ארגון עומדים בדרישות ה – GDPR.[44] ה – GDPR מוסיף שעמידת מעבד המידע בקודי התנהגות כאמור, או קבלת אישור כאמור על עמידה בדרישות החוק, ישמשו כאמצעי להוכחת הציות של מעבד המידע להוראות ה – GDPR.

ההסכם בין בעל השליטה במידע למעבד המידע[45]

ההסכם בין בעל השליטה במידע למעבד יהיה בכתב (לרבות אלקטרוני), בהתאם לדין האיחוד האירופי, או לפי דין מדינה החברה באיחוד האירופי ויכלול את ההוראות הבאות:

- נושא ההתקשרות;
- תקופת עיבוד המידע;
- מהות עיבוד המידע;
- סוגי המידע שיעובד ואם מדובר בקטגוריות מיוחדות של מידע;
- החובות והזכויות של בעל השליטה במידע;
- התחייבות מעבד המידע –

[39] ראו סעיף 27 ל – GDPR.
[40] ראו לעיל את הפרק הנוגע לתחולת החוק.
[41] ראו סעיף 27 ל – GDPR.
[42] ראו סעיף 28 ל – GDPR.
[43] ראו סעיף 40 ל – GDPR.
[44] ראו סעיף 42 ל – GDPR.
[45] ראו סעיף 28 ל – GDPR.

- ❒ לעבד את המידע רק בהתאם להנחיות המתועדות של בעל השליטה במידע, לרבות בנוגע להעברת המידע למדינה אחרת או לארגון בינלאומי;
- ❒ עובדי ונציגי מעבד המידע חתומים על הסכם סודיות הולם, או מחויבים לסודיות לפי דין;
- ❒ מעבד המידע נוקט בכל האמצעים הנדרשים לאבטח את המידע כנדרש;[46]
- ❒ מעבד המידע לא יתקשר עם מעבדי-משנה, אלא בכפוף לדרישות ה – GDPR ויוודא שגם מעבדי המשנה עומדים בדרישות אלה;
- ❒ מעבד המידע יסייע לבעל השליטה במידע ביישום זכויות נושאי המידע לפי ה –GDPR (כדוגמת הזכות לעיין במידע, למחוק מידע ולנייד מידע).[47]
- ❒ מעבד המידע יסייע לבעל השליטה במידע בציות לחובות מכוח ה – GDPR בנוגע לאבטחת מידע, דיווח על פריצה למידע, ביצוע סקר סיכוני פרטיות והתייעצות מראש עם הרשות להגנת המידע.[48]
- ❒ מעבד המידע, לפי בחירת בעל השליטה במידע, ימחק או יחזיר את כל המידע האישי לבעל השליטה במידע בתום אספקת שירותיו, אלא אם דין האיחוד האירופי או דין איזה מהמדינות החברות בו קובע שיש לשמור מידע.[49]
- ❒ מעבד המידע יספק לבעל השליטה במידע גישה לכל המידע הנדרש כדי להוכיח עמידה בהוראות סעיף זה ל – GDPR הדן בחובות בעל השליטה במידע ומעבד המידע וכן יאפשר ביצוע בקורת על ידי בעל השליטה במידע, או מבקר מטעמו.

בדומה להסדר שהיה קיים בדירקטיבת הגנת המידע, האיחוד האירופי יהיה רשאי גם מכוח ה – GDPR ליצור נוסח סטנדרטי להתקשרות בין בעל השליטה במידע למעבד המידע (Standard Contractual Clauses).

תיעוד עיבוד המידע[50]

הוראות התיעוד שלהלן חלות על כל אחד מהמקרים הבאים:

- ❖ על גופים המעסיקים 250 אנשים ומעלה;
- ❖ כאשר עיבוד המידע צפוי לכלול סיכון לחרויות ולזכויות של נושאי המידע;
- ❖ עיבוד המידע איננו מקרי/אגבי (occasional);
- ❖ על עיבוד מידע בקטגוריות מיוחדות (מידע רגיש);
- ❖ על עיבוד מידע הנוגע לעבירות פליליות והרשעות.

עיקרון התחולה השני מתוך החמישה לעיל הוא רחב וגבולותיו ייקבעו כנראה על בסיס כל מקרה לגופו. היות שכך, יש להתייחס לתחולת הוראות התיעוד שלהלן כרחבה, דהיינו כחלה על מרבית פעילות עיבוד המידע.

בעל השליטה במידע (או נציגו) ישמרו תיעוד בכתב (לרבות אלקטרוני) של עיבוד המידע שיכלול:

---

46 ראו סעיף 32 ל – GDPR.
47 ראו פרק III ל – GDPR.
48 ראו סעיפים 32 עד 36 ל – GDPR.
49 זו הוראה בעייתית ליישום כאשר למעבד המידע אין נוכחות באיחוד האירופי. לדוגמה, מה תעשה חברה ישראלית המשמשת כמעבדת מידע, אם הדין הישראלי מחייב שמירת מידע מסוים לתקופה מסוימת ואין הוראה מקבילה בדין האירופי?
50 ראו סעיף 30 ל – GDPR.

- פרטי בעל השליטה במידע;
- פרטי קצין הגנת המידע;
- מטרת העיבוד;
- קטגוריות המידע המעובד;
- קטגוריות נושאי המידע;
- העברת מידע אל מחוץ לגבולות האיחוד האירופי;
- צפי למועד מחיקת המידע;
- תיאור כללי של אמצעי אבטחת המידע.

מעבד מידע (או נציגו) ישמרו תיעוד בכתב (לרבות אלקטרוני) של עיבוד המידע שיכלול:

- פרטי מעבד המידע;
- פרטי קצין הגנת המידע;
- קטגוריות המידע המעובד;
- העברת מידע אל מחוץ לגבולות האיחוד האירופי;
- תיאור כללי של אמצעי אבטחת המידע;

על התיעוד להיות זמין לביקורת על ידי רשות הגנת המידע.

שיתוף פעולה עם הרשות[51]

הן בעל השליטה במידע והן מעבד המידע (גם מעבדי המידע שמקום מושבם איננו באיחוד האירופי), מחויבים לשתף פעולה עם הרשויות להגנת המידע של מדינות האיחוד האירופי.

[51] ראו סעיף 31 ל – GDPR.

אבטחת מידע ודיווח על פריצה למידע

המלצה לפעולה	✓ אבטחת המידע היא נושא בעל חשיבות גבוהה מאד במסגרת ההתקשרויות החוזיות עם חברות מהאיחוד האירופי. מומלץ: למנות קצין אבטחת מידע, לקבוע נהלי אבטחה ברורים, לבצע הדרכה והטמעה של הנהלים ולעדכן אותם בהתאם לנדרש. ✓ מומלץ לשקול לקבל הסמכות אבטחת מערכות מידע מוכרות דוגמת ISO 27001 או SOC2 (אולם אין דרישה מפורשת לכך ב- GDPR). ✓ יש לצפות לרגישות מיוחדת של חברות מהאיחוד האירופי בעניין דיווח על פריצות למידע ולהיערך, עם נוהל פנימי מתאים, לניהול אירועים מסוג זה.

סעיפים רלוונטיים	סעיפים 33-35 ל – GDPR. סעיפים 85-88 לדברי האקדמה.

חובה כללית[52]

ה – GDPR כולל חובה כללית להשתמש בכלים טכניים וארגוניים הולמים לשם הגנת המידע האישי, בהתאם לרמת הסיכון, ובכלל זה להשתמש ביכולות הבאות:

- פסאודונימיזציה והצפנה;
- היכולת לוודא סודיות, שלמות, זמינות ועמידות המערכות והשירותים;
- היכולת להחזיר לפעולה את המערכות בהקדם, לאחר אירוע אבטחה;
- בדיקות והערכות שוטפות של רמת ההגנה על המידע.

ה – GDPR מעודד יצירת קודי התנהגות על ידי איגודים מקצועיים וכיו"ב[53] וכן מנגנוני הסמכה ואישור המעידים על כך שחברה או ארגון עומדים בדרישות ה – GDPR.[54] ה – GDPR מוסיף שעמידת מעבד המידע בקודי התנהגות כאמור, או קבלת אישור כאמור על עמידה בדרישות החוק, ישמשו כאמצעי להוכחת הציות של מעבד המידע להוראות ה – GDPR.

דווח על פריצה למידע (Data Breach Notification)[55]

דיווח לרשות. בעל שליטה במידע חייב ללא דיחוי ואם ישים – לא יותר מלאחר 72 שעות לאחר שנודע לו, לדווח לרשות להגנת המידע, אלא אם לא סביר שהפריצה תגרום לפגיעה בזכויות ובחרויות של נושאי המידע. אם הדיווח נעשה לאחר 72, על בעל השליטה במידע לנמק את הדחיה בדיווח. הדיווח יכלול:

- מהות וכמות המידע שנחשף;
- פרטי קצין הגנת המידע של הארגון;
- התוצאות הצפויות מהפריצה למידע;

---

52 ראו סעיף 32 ל – GDPR.
53 ראו סעיף 40 ל – GDPR.
54 ראו סעיף 42 ל – GDPR.
55 ראו סעיף 33-34 ל – GDPR.

לתוכן העניינים

- האמצעים המוצעים על ידי בעל השליטה במידע לטיפול בפריצה;

בעל השליטה במידע יתעד כראוי את הליך הטיפול בפריצה.

מעבד מידע חייב לדווח לבעל השליטה במידע ללא דיחוי על פריצה למידע.

דיווח לנושאי המידע. אם הפריצה צפויה לגרום לסיכון גבוה לזכויות ולחרויות של נושאי המידע, בעל השליטה במידע חייב לשלוח ללא דיחוי הודעה ברורה על הפריצה למידע לאותם נושאי המידע, שתכלול את המידע הנזכר לעיל ביחס להודעה לרשות.

דיווח לנושאי המידע איננו מחויב אם –

- המידע האישי הוצפן כראוי;
- בעל השליטה נקט באמצעים שימנעו מהסיכון לזכויות וחרויות נושאי המידע להתממש;
- אם הודעה לכל נושא מידע תחייב מאמץ לא פרופורציונאלי. במקרה כזה אפשר יהיה כתחליף לשלוח הודעה באמצעי תקשורת ציבוריים.

סקר סיכוני הגנת מידע[56]

(Data Protection Impact Assessment)

המלצה לפעולה	✓ סקר סיכוני הגנת פרטיות הוא פרקטיקה נכונה ורצויה – בין אם היא קבועה בחוק ובין אם לאו. מומלץ מאד ליישם אותה. היא מאפשרת לקבל תמונה ברורה של הסיכונים הכרוכים בפעילות ומסייעת בהפחתת הסיכונים לארגון ולנושאי המידע.

סעיפים רלוונטיים	סעיפים 35, 36 ל – GDPR. סעיפים 84, 90, 91, 92, 94, 95 לדברי האקדמה.

סקר הערכת סיכוני הגנת מידע הוא מושג ידוע ומוכר אצל חברות רבות בעולם ובפרט בארה"ב ובאיחוד האירופי. מושג זה מעוגן ב- GDPR. סקר הערכת סיכוני הגנת מידע נדרש כאשר עיבוד המידע צפוי לגרום לסיכון גבוה לזכויות ולחרויות של נושאי המידע, בעיקר כאשר מדובר בשימוש בטכנולוגיות חדשות. בעל השליטה במידע צריך, לפני תחילת עיבוד המידע, לבצע סקר הערכת סיכונים.

הסקר יידרש במיוחד במקרים הבאים:

- הערכה שיטתית ורחבת היקף של נושאי המידע בכלים אוטומטיים, לרבות יצירת פרופילים;
- עיבוד בהיקף גדול של קטגוריות מיוחדות של מידע (מידע רגיש);
- ניטור שיטתי ובהיקף גדול של מקום ציבורי.

ברבות הזמן אנו צפויים לראות פרסומים רשמיים של האיחוד האירופי אודות מקרים ופרויקטים המחייבים ביצוע סקר סיכונים, לעומת נושאים הפטורים מכך.

הסקר יכלול לפחות את הפרטים הבאים:

- תיאור שיטתי של פעולות העיבוד ומטרות העיבוד, לרבות האינטרס הלגיטימי של בעל השליטה במידע, אם רלוונטי;
- הערכת ההכרח בעיבוד והמידתיות שלו, ביחס למטרות העיבוד;
- הערכת הסיכונים האפשריים;
- האמצעים שייעשה בהם שימוש כדי להתמודד עם הסיכונים ולציית להוראות ה – GDPR.

אם מסקנות הסקר כוללות צפי לסיכון גבוה לפגיעה בזכויות נושאי המידע, על בעל השליטה במידע להתייעץ עם רשות הגנת המידע ולקבל את חוות דעתה.[57]

[56] ראו סעיף 35 ל – GDPR.
[57] ראו סעיף 36 ל – GDPR.

קצין הגנת מידע (Data Protection Officer)[58]

המלצה לפעולה	✓ קצין הגנת מידע הוא מושג ידוע ומוכר בעולם בכלל ובארה"ב ואירופה בפרט מזה שנים רבות, אך הוא איננו מוכר בשוק הישראלי. חלקו מיושם, לפחות תיאורטית, באמצעות מושג "מנהל המאגר" לפי חוק הגנת הפרטיות הישראלי, אלא שהתפקידים הקבועים לפי ה – GDPR הם מפורטים וברורים יותר. בעוד ש"מנהל מאגר" אחראי לפי הדין הישראלי לאבטחת המאגר (ובכך יוצר הקבלה לא ברורה עם קציני אבטחת המידע הארגוניים), הרי שקצין הגנת המידע אחראי בצורה ברורה על היבטי הציות לדיני הגנת המידע.

סעיפים רלוונטיים	סעיפים 37 – 39 ל – GDPR. סעיף 97 לדברי האקדמה.

בעל שליטה במידע ומעבד מידע חייבים למנות קציני הגנת מידע בכל אחד מהמקרים הבאים:

- ❖ בעל השליטה במידע או מעבד המידע הם רשות ציבורית;
- ❖ עיבוד מידע בדרך של ניטור שיטתי רחב היקף;
- ❖ עיבוד מידע רחב היקף של קטגוריות מיוחדות של מידע ("מידע רגיש");
- ❖ דין מדינתי של מדינה החברה באיחוד האירופי מחייב מינוי קצין הגנת מידע.

מאפייני התפקיד:

- ❖ קצין הגנת המידע יהיה מעורב בזמן ובאופן הולם בכל נושא הנוגע להגנת מידע אישי.
- ❖ קצין הגנת המידע יקבל כלים ועזרה מתאימים כדי לבצע את תפקידו.
- ❖ לא ניתן לפטר את קצין הגנת המידע בגלל ביצוע תפקידו.
- ❖ קצין הגנת המידע ידווח לרמה הניהולית הבכירה ביותר בארגון.
- ❖ קצין הגנת המידע יכול למלא גם תפקידים אחרים, כל עוד אין ניגוד עניינים בין התפקידים.
- ❖ פרטי קצין הגנת המידע יפורסמו ויישלחו לרשות להגנת המידע.

תפקידי קצין הגנת המידע:

- ❖ ליידע ולהנחות בנוגע לחובות מכוח ה – GDPR וחקיקה מדינתית רלוונטית;
- ❖ לנטר ציות להוראות ה – GDPR, לרבות קביעת תחומי אחריות, הדרכה והעלאת מודעות;
- ❖ לייעץ בעריכת סקרי סיכוני הגנת מידע;

[58] ראו סעיפים 37 – 39 ל – GDPR.

לתוכן העניינים

- לשתף פעולה עם הרשות להגנת המידע ולשמש כאיש הקשר הארגוני לדין ודברים עם הרשות.

מלבד ההוראות המקובצות ב – GDPR בקשר עם הגדרת התפקיד של קצין הגנת מידע, קיימות הוראות נוספות המתייחסות אליו והמצויות בסעיפים נוספים בחוק זה. לדוגמה –

- ציון פרטי קצין הגנת המידע במסגרת מתן הודעה לנושא המידע לפי סעיף 13 ל – GDPR.
- ציון פרטי קצין הגנת המידע במסגרת תיעוד לפי סעיף 30 ל – GPDR ;
- ציון פרטי קצין הגנת המידע במסגרת דיווח על פריצה למידע לפי סעיף 33 ל – GDPR ;

העברת מידע

המלצה לפעולה	✓ מומלץ לבחון את האפשרות לעבוד עם שירותי תשתית ענן המציעים לאחסן את המידע בתחומי האיחוד האירופי בלבד. ✓ חברות צריכות להיערך לחתימה על ה – Standard Contractual Clauses ✓ חברות ישראליות המתקשרות בהסכמים באמצעות חברות קשורות אמריקניות, צריכות להיערך לכך שחברות אירופאיות אינן מוכנות להסתמך יותר על ה – Privacy Shield.

סעיפים רלוונטיים	סעיפים 40 – 45 ל – GDPR. סעיפים 101 – 116 לדברי האקדמה.

העברת מידע אישי מהאיחוד האירופי אל מדינות אחרות ממשיך להיות מוסדר על ידי הוראות הקובעות מנגנונים להעברה כזו. באופן כללי, מנגנונים אלה דומים למנגנונים שהיו קבועים בדירקטיבת הגנת המידע, בשינויים קלים. לדוגמה, אין ב- GDPR יותר חובת דיווח לרשויות הגנת המידע על חתימה על הסכמי Standard Contractual Clauses (הסכמים סטנדרטיים על פי הדין האירופי, להעברת מידע אל טריטוריות מחוץ לאיחוד האירופי).

הפרת ההוראות לענין העברת מידע אישי היא אחת מההפרות שבצידן קנס של 20,000,000 אירו או עד 4% מהמחזור השנתי הגלובאלי של החברה – לפי הגבוה מביניהם, ומכאן הסיכון הגדול הכרוך בכך.

לפיכך, חברות מן האיחוד האירופי צפויות להציב דרישות נוקשות ביחס לנושא זה.

העברת מידע לישראל

אחד מהמנגנונים להעברת מידע אישי אל מחוץ לאיחוד האירופי היא בדרך של העברה למדינה אשר קיבלה את אישור האיחוד האירופי לכך שדיני הגנת המידע שלה הולמים את רמת ההגנה הנדרשת (adequate protection) לפי דיני האיחוד האירופי.

ב – 31.1.2011 ישראל קיבלה את אישור האיחוד האירופי בדבר ההלימה של דיני הגנת המידע הישראליים בנוגע לעיבוד מידע אוטומטי, לדיני האיחוד האירופי.[59]

לכאורה, האישור הנ"ל מקל על חברות ישראליות לתפקד כמעבדי מידע עבור לקוחותיהן מן האיחוד האירופי, כיוון שבהתאם לאישור אין צורך במנגנון נוסף כלשהו לצורך עיבוד המידע האישי, אולם לכך יש שני סייגים משמעותיים מאד:

- חברות ישראליות רבות מעבדות את המידע באמצעות שירותי תשתית מבוססי ענן. שירותים אלה מחזיקים את המידע לעיתים קרובות בארצות הברית. דיני ארה"ב לא קיבלו אישור דומה לזה של ישראל מהאיחוד האירופי. יש ספקי שירותי ענן המסוגלים לספק כיום התחייבות לאחסן את המידע האישי בתוככי האיחוד האירופי ובכך לפתור את הבעיה, אולם פתרון זה ישים רק בחלק מהמקרים. פתרון נוסף הוא עמידת החברות המאחסנות או מעבדות מידע בארה"ב בכללי ה – Privacy Shield, אולם, כפי שמפורט להלן, אף מנגנון זה ניצב בימים אלה בסימן שאלה.
- מקורו של אישור ההלימה שקיבלה ישראל היה בדירקטיבת הגנת המידע. בהתאם ל – GPDR, אישור זה יישאר בתוקף, עד שיתוקן, יוחלף או יבוטל על ידי האיחוד האירופי. ה – GDPR קובע הוראות

[59] Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (2011/61/EU).

מפורטות ביחס לפרוצדורות והקריטריונים שעל האיחוד האירופי לשקול כאשר הוא קובע אם דין של מדינה הולם את דיני האיחוד האירופי. לפיכך, אין בטוחה כי ישראל תמשיך ליהנות מאישור ההלימה גם בעתיד.

העברת מידע לארצות הברית

מנגנון אחר וספציפי להעברת מידע, ה – Safe Harbor[60] התקיים בין האיחוד האירופי לארצות הברית. אלא שמנגנון זה בוטל ב – 6.10.2015 בהחלטה של בית המשפט לצדק האירופי בעניין מקסימיליאן שרמס,[61] תוך קביעה שדיני הגנת הפרטיות בארצות הברית אינם מספקים הגנה נאותה לנושאי מידע מהאיחוד האירופי.

מעט לאחר החלטה זו החלו הנציבות האירופית וממשלת ארה"ב לדון במסגרת חדשה שתספק הגנה נאותה למידע אישי וב-2.2.2016 הגיעו הצדדים להסכם מדיני בו התמסד הסדר חדש – Privacy Shield שמו.[62]

עם זאת, הקולות באיחוד האירופי לביטול גם של ה – Privacy Shield הולכים וגוברים. הפרלמנט האירופי קיבל החלטה ב – 26.6.2018 הקוראת למועצת האיחוד (EU Commission) להשעות את ה – Privacy Shield.[63] כתוצאה מהבקורת הזו, אנו עדים לחברות אירופאיות המסרבות להתיר לספקי השירותים שלהם לעבד מידע בארה"ב בהסתמך על ה – Privacy Shield ודורשות מהן לחתום על ה – Standard Contractual Clauses.

60 http://www.export.gov/safeharbor/

61 תיק Case C-362/14 מקסימיליאן שרמס נ' הרשות להגנת המידע האירית.

62 להסבר על ה – Privacy Shield ראו: http://europa.eu/rapid/press-release_MEMO-16-434_en.htm

63 Resolution on the adequacy of the protection afforded by the EU-US Privacy Shield - 2018/2645(RSP)

אכיפה

המלצה לפעולה	✓ חובה לבצע בדיקת ניתוח הפערים בין המצב הקיים לבין החובות החלות על החברה מכוח ה – GPDR. יש לגבש תוכנית עבודה עם לוחות זמנים ליישום ותעדוף המשימות בהתאם למידת הדחיפות והחשיבות של המשימה. על הפרק: - עדכון נהלים וקודי ההתנהגות בחברה; - מיסוד תהליכים (הנדסת הגנת מידע, פסאודונימיזציה, ארכוב/השמדת מידע, ניהול אירועי פריצה, טיפול פניות לקוחות, דיווחים לרשויות...). - עדכון הסכמים עם ספקים, לקוחות עסקיים, לקוחות קצה; - מינוי נושאי תפקיד. ✓ חברות המנהלות סיכונים כחלק מהממשל התאגידי צריכות לשלב את הסיכונים הנובעים מה – GDPR למכלול הסיכונים שהתאגיד צריך להתמודד איתו. ✓ יש לבדוק ולעדכן את הכיסוי הביטוחי של החברה.

סעיפים רלוונטיים	סעיף 77-83 ל – GDPR. סעיפים 141-150 לדברי האקדמה.

אחריות וסעדים

לנושאי מידע הזכות בקשר עם הפרות ה – GDPR:

- ❖ להגיש תלונות לרשויות להגנת מידע;
- ❖ להגיש תביעה משפטית. החידוש ב – GDPR הוא שלפי חוק זה, להבדיל מדירקטיבת הגנת המידע, נושאי מידע יכולים לתבוע במישרין גם את מעבדי המידע ולא רק את בעלי השליטה במידע ובכלל זה לקבל פיצוי כספי ממעבדי המידע.
- ❖ המדינות החברות באיחוד האירופי תוכלנה לקבוע שהפרות של ה – GPDR יהוו גם עבירות פליליות.[64]

בעלי השליטה במידע אחראים כלפי נושאי המידע לכל נזק שנגרם להם כתוצאה מעיבוד המידע שבשליטתם בניגוד להוראות ה – GDPR.

מעבדי מידע אחראים כלפי נושאי המידע לכל נזק שנגרם כתוצאה מהפרת ההוראות ב – GDPR החלות על מעבדי המידע (לדוגמה, החובה לאבטח את המידע כראוי) וכן שנגרם כתוצאה מהפרת הוראות העיבוד שבעל השליטה במידע נתן למעבד המידע.

ה – GDPR מדגיש כי הזכות לפיצוי נוגעת לא רק לנזקים כספיים, אלא גם לנזקים "לא ממוניים" כדוגמת עוגמת הנפש שנגרמה מהפרת זכויותיו של נושא המידע.

[64] ראו סעיף 149 לדברי האקדמה.

קנסות מנהליים

על פי הדין שהיה קיים טרם כניסת ה- GDPR לתוקף, דהיינו, דירקטיבת הגנת המידע, מדינות החברות באיחוד האירופי רשאיות היו לקבוע לעצמן את היקף הקנסות המנהליים שרשויות הגנת המידע יכולות להטיל על הפרת דיני הגנת המידע המדינתיים, שחוקקו מכוח הדירקטיבה.

ה – GDPR שינה זאת וקבע מסגרת אחידה ומרחיקת לכת להטלת קנסות. הטלת הקנסות נותרת עדיין בשיקול דעת רשויות הגנת המידע על בסיס כל מקרה לגופו וה – GDPR קובע אף שבמקרים של הפרות קטנות או שוליות, או במקרים שבהם הקנס יצור מעמסה כלכלית בלתי מידתית על אדם, ניתן להחליף את הקנס בהתראה/נזיפה.[65]

רשות להגנת מידע רשאית להטיל קנסות מנהליים על בעלי שליטה במידע ועל מעבדי מידע. שתי רמות של קנסות קובע ה – GPDR:

רמת הקנס הגבוהה – קנס עד ל – 20 מיליון (20,000,000) אירו, או במקרה של גוף המנהל פעילות כלכלית[66] - עד 4% מסך המחזור השנתי הגלובאלי במהלך השנה הפיננסית הקודמת – לפי הגבוה מבין השניים.

ההפרות הכלולות ברמת הקנס הגבוהה הן:

- הפרת עקרונות הגנת המידע והתנאים להסכמה – סעיפים 5, 6, 7 ו – 9 ל – GDPR;
- הפרת זכויות נושאי המידע – סעיפים 20-22 ל – GDPR;
- הפרת ההוראות בעניין העברת מידע מחוץ לאיחוד האירופי – סעיפים 44-49 ל – GDPR;
- הפרת התחייבויות בהתאם לחוקים של מדינות החברות באיחוד האירופי, שאומצו בהתאם לפרק 9 ל – GDPR;

רמה קנס הנמוכה – קנס עד ל – 10 מיליון (10,000,000) אירו, או במקרה של גוף המנהל פעילות כלכלית - עד 2% מסך המחזור השנתי הגלובאלי במהלך השנה הפיננסית הקודמת – לפי הגבוה מבין השניים.

ההפרות הכלולות ברמת הקנס הנמוכה הן:

- אי קבלת הסכמה בקשר עם עיבוד מידע על ילדים – סעיף 8 ל – GDPR;
- היעדר יישום הנדסת הגנת מידע והגנת מידע כברירת מחדל – סעיף 25 ל – GDPR;
- אי הסכמה על חלוקת אחריות בין בעלי שליטה במידע משותפים – סעיף 26 ל – GDPR;
- אי מינוי נציג לבעלי שליטה במידע או מעבדי מידע שמקום מושבם איננו באיחוד האירופי – סעיף 27 ל – GDPR;
- הפרות של בעל השליטה במידע בקשר עם ההסכם בינו לבין למעבד המידע – סעיף 28 ל –GDPR ;
- הפרות מעבדי מידע בקשר עם ההתקשרות עם מעבדי-משנה והחובה להישמע להוראות בעל השליטה במידע – סעיפים 28-29 ל – GDPR;
- אי שמירת תיעוד של העיבוד – סעיף 30 ל –GDPR ;
- חוסר שיתוף פעולה עם הרשות להגנת המידע – סעיף 31 ל – GDPR;

---

[65] ראו סעיף 148 לדברי האקדמה.

[66] "Undertaking", בהתאם להגדרת מונח זה בסעיפים 101 ו – 102 ל – Treaty on the Functioning of the European Union. ראו סעיף 150 לדברי האקדמה.

- אי יישום אמצעים לאבטחת מידע– סעיף 32 ל – GDPR ;
- הימנעות מדיווח על פריצות למידע– סעיפים 33-34 ל – GDPR ;
- הימנעות מביצוע סקר סיכוני הגנת מידע– סעיפים 35-36 ל – GDPR ;
- הפרת החובה למנות קצין הגנת מידע– סעיפים 37-39 ל – GDPR ;
- גופי הסמכה – הפרת סעיף 42 ל – GDPR ;
- גופים מנטרים ציות לחוק - הפרת סעיף 41 ל – GDPR ;

במקרה של הפרה של מספר הוראות ב – GDPR, היקף הקנס לא יעלה על הקנס בגין ההפרה החמורה ביותר.

רשויות הגנת המידע מונחות לשקול אחד עשר שיקולים לצורך קביעת גובה הקנס, כדלקמן :

- מהות, חומרת והיקף בזמן של ההפרה. בכלל זה יילקחו בחשבון מטרות העיבוד, כמות נושאי המידע שנפגעים ודרגת הפגיעה ;
- אם ההפרה היא תוצאה של רשלנות או של מעשה מכוון ;
- פעולות שנעשו למזער את הנזק ;
- מידת האחריות של בעל השליטה במידע או מעבד המידע בהתחשב באמצעים הטכניים והניהוליים שיישמו (כדוגמת, אבטחת מידע ברמה הולמת, עמידה בסטנדרטים/קודי התנהגות, הנדסת הגנת מידע והגנת מידע כברירת מחדל) ;
- הפרות קודמות ;
- רמת שיתוף הפעולה עם רשות הגנת המידע ;
- סוגי המידע שנפגעו ;
- האופן שבו הרשות למדה על ההפרה, בפרט אם בעל השליטה במידע או מעבד המידע הודיעו על ההפרה מיוזמתם ;
- היסטוריה קודמת של פעולות אכיפה ;
- ציות לקוד התנהגות מאושר או אישור הסמכה מאושר, בהתאם להוראות 40 ו – 42 ל – GDPR ;
- כל שיקול רלוונטי אחר, כדוגמת הרווח הכלכלי שנוצר מההפרה, הימנעות מהפסדים כתוצאה מההפרה וכיו"ב.
- אם המפר איננו גוף בעל פעילות כלכלית, הרשות תיקח בחשבון גם את שיעור השכר הממוצע במדינה החברה באיחוד האירופי הרלוונטית ואת מצבו הכלכלי הספציפי של המפר.[67]

[67] שיקול זה מופיע בסעיף 150 לדברי האקדמה, לא בסעיפי החוק.