**הכנסת**
**הלשכה המשפטית**
**תחום חקיקה ומחקר משפטי**

# התקנות האירופיות בעניין הגנת המידע (GDPR)

א' בתמוז תשע"ח

12 ביוני 2018

כתיבה: ד"ר ירון אונגר, עו"ד

אישור: ד"ר ליאור בן דוד, עו"ד ממונה בכיר (חקיקה ומחקר משפטי)

סקירה זו, שעוסקת בתקנות האירופיות בעניין הגנת המידע (GDPR), נכתבה לבקשת חברת הכנסת רויטל סויד, כחומר רקע לכנס המשותף לחברי כנסת וחברי פרלמנט מסלובקיה, שייערך בברטיסלבה, ב-21 ליוני 2018.

תקנות ה-GDPR (General Data Protection Regulation) הן רגולציה של הפרלמנט האירופי, המטילה הגבלות שונות שנועדו להגן על פרטיותם של אנשים. ההגבלות חלות על גופים אירופיים ועל גופים מחוץ לאירופה המחזיקים במידע אישי על תושבי האיחוד האירופי או מספקים שירותים או מוצרים לתושביו. [1] בהתאם לכך, לתקנות יש תחולה אקס טריטוריאלית, ועשויה להיות להן השפעה לא רק על עסקים במדינות האיחוד אלא גם על עסקים בישראל ובמקומות אחרים בעולם.[2]

התקנות מבחינות בין "מידע אישי" ל"מידע אישי רגיש", שעליו חל משטר אבטחה מחמיר יותר. "מידע אישי" מוגדר כמידע הקשור לאדם שהמידע עוסק בו (להלן: נשוא המידע), שניתן להשתמש בו כדי לזהות במישרין או בעקיפין את נשוא המידע, לרבות שם, תמונה, כתובת דואר אלקטרונית, פרטי בנק, מידע רפואי, כתובת IP של מחשב ונתונים אישיים רגישים כנתונים גנטיים או ביומטריים. מידע הנוגע לנתונים אישיים שחושפים מוצא גזעי או אתני, דעות פוליטיות, אמונות דתיות או פילוסופיות, חברות באיגוד מקצועי, נתונים גנטיים או ביומטריים, נתונים הנוגעים לבריאות או לחיי המין של האדם מוגדר כ"מידע אישי רגיש".

להלן העקרונות המרכזיים שבתקנות[3]:

**1. גוף לא יעבד ויאגור <u>מידע אישי</u> אלא בתנאים הבאים –**

א. המידע יעובד על פי חוק, בהגינות ובשקיפות.

ב. המידע יעובד למטרה מיוחדת ולגיטימית, והעיבוד לא יחרוג ממטרה זו, למעט עיבוד למטרות של שימור מידע לשם קידום מטרות ציבוריות, מחקר היסטורי או סטטיסטי.

ג. המידע יישמר ויעובד באופן שיבטיח את היותו מדויק ועדכני.

ד. המידע יישמר לתקופה הנחוצה לשם זיהוי נשוא המידע לטובת המטרה שלשמה נאסף המידע, ולא מעבר לכך, אלא אם השמירה נחוצה לשם קידום מטרות ציבוריות, מחקר היסטורי או סטטיסטי.

ה. המידע יאובטח באופן שימנע גישה בלתי מורשית אליו, אובדן, השמדה או נזק.

**2. גוף לא יעבד ויאגור <u>מידע אישי רגיש</u> אלא בהתקיים התנאים שבסעיף 1, וכן אחד מן התנאים הבאים –**

א. נשוא המידע נתן את הסכמתו לכך (Opt in). יש לוודא שנשוא המידע יוכל לבטל את הסכמתו בכל עת, בדרך פשוטה ובדומה לאופן שבו נתן את הסכמתו מלכתחילה;

ב. עיבוד המידע נחוץ לשם ביצוע חוזה שנשוא המידע צד לו;

ג. קיימת חובה חוקית לביצוע עיבוד המידע;

ד. העיבוד הכרחי לצורך הגנה על האינטרסים של נשוא המידע או אדם אחר;

---

[1] טקסט עדכני של התקנות ניתן למצוא באתר החקיקה של האיחוד האירופי, <u>כאן</u>. יש להדגיש שבהיותן חקיקה ישירה של הפרלמנט האירופי, התקנות חלות מאליהן על גופים בכל מדינות האיחוד האירופי, ויישומן אינו מותנה באישור או אימוץ התקנות בחקיקה של המדינות.

[2] חשוב לציין, שהתקנות אינן חלות על המשטרה או על רשויות האכיפה. תקנות בעניין הגנת הפרטיות החלות על גופים אלו נקבעו ב- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[3] למידע שימושי נוסף ראו: דן אור-חוף ושרון גיא, <u>כללים עקרונות ותחולה על חברות ישראליות</u>, אור-חוף טכנולוגיות וקניין רוחני, 2016 וכן באתר <u>GDPR ISRAEL</u>.

ה. העיבוד נחוץ לטובת הגנה על אינטרס ציבורי, לשם מתן טיפול רפואי וכדומה, או בהפעלת סמכות רשמית שניתנה לחברה;

ו. העיבוד חיוני לשם הגנה על אינטרסים לגיטימיים שגוברים על זכויות נשואי המידע;

ז. המידע נעשה זמין לציבור בידי נשוא המידע;

ח. המידע מעובד לטובת מטרות של שמירת מידע היסטורי, מחקר היסטורי או סטטיסטי, ובכפוף לנקיטה באמצעים שיבטיחו את פרטיותו של נשוא המידע.

**3. יש להקפיד שיובטחו לנשוא המידע הזכויות הבאות –**

א. **גישה למידע -** נשוא המידע זכאי לקבל מן המחזיק במידע, ללא עלות, אישור בעניין המידע שנאסף אודותיו; ומידע הנוגע לאיסוף ועיבוד הנתונים, מטרת העיבוד, ואף לקבל עותק אלקטרוני המכיל את המידע המעובד בצורה מובנת, פשוטה ושקופה.

ב. **תיקון מידע** – נשוא המידע זכאי לבקש תיקון של מידע אישי הנוגע אליו.

ג. **הזכות "להישכח"** – נשוא המידע זכאי לדרוש מהמחזיק במידע למחוק את המידע האישי המוחזק אודותיו, להפסיק את עיבוד המידע ו/או להפסיק את ביצוע העיבוד על ידי צדדים שלישיים, בעיקר כאשר המידע האישי כבר אינו נחוץ לשם המטרה שלשמה נאסף או כאשר אין אינטרס לגיטימי להמשך עיבוד המידע.

ד. **ניידות המידע האישי -** נשוא המידע זכאי להעתיק או להעביר את המידע האישי מסביבה אחת לאחרת בצורה בטוחה וללא הפרעה לשימוש.

ה. **מידתיות** – אין לאסוף או לעבד מידע אישי שאינו נדרש בפירוש לצורך אספקת השירותים ו/או המוצרים לנשוא המידע.

ו. **זכות להתנגד לעיבוד המידע -** לנשוא המידע שמורה הזכות להתנגד לאיסוף או עיבוד מידע בענייננו, למשל, לצרכים סטטיסטיים.

ז. **אפיון וקבלת החלטות אוטומטיות -** נשוא המידע זכאי לכך שמידע אודותיו לא יהיה נתון לפעולות עיבוד וקבלת החלטות אוטומטיות באופן העשוי להשפיע באופן משפטי או באופן משמעותי על חייו, וכן תהיה לו זכות להביע דעתו ולקבל הסבר על החלטה שנתקבלה באופן אוטומטי ואף להתנגד לה. (למשל, כאשר מתקבלת החלטה בעניין סיווג דירוג האשראי של נשוא המידע בהתאם לנתונים שבמאגר, נשוא המידע יוכל להתנגד לקבלת החלטה בדרך זו ואף לטעון כי הפרטים המצויים במאגר אינם מדויקים או שאין לבסס על פיהם את ההחלטה).

**4. המחזיק במידע נושא בחובות הבאות –**

א. **מינוי אחראי הגנת מידע -** בעל מאגר ומעבד מידע נדרש למנות ממונה אבטחת מידע, כאשר עיבוד מידע אישי מהווה חלק מרכזי בפעילותו המצריך פעולות ניטור קבוע ושיטתי בקנה מידה גדול; או כאשר מתבצע עיבוד של מידע אישי רגיש בקנה מידה גדול, או ברשות ציבורית. הממונה יהיה אחראי על הציות להוראות התקנות ולכל רגולציה אחרת להגנה על מידע אישי, יודיע וייעץ לחברה ועובדיה באשר להוראות, ינהל פעולות פנימיות לאכיפתן ולביצוע החובות החלות מכוחן בתוך הארגון, יבצע ביקורות עצמיות בחברה וישמש איש הקשר בין החברה לרשויות הפיקוח ומול נשואי המידע האישי.

ב. **דיווח ותיעוד** – על המחזיק במידע לתעד ולנהל רשומות בנוגע לעיבוד המידע האישי, תוך סיווג המידע לקטגוריות, פירוט של העברות מידע לצד שלישי ואמצעי האבטחה שננקטו. אם בשל הפרה של ההוראות נפגעה הזכות לפרטיות של נשוא המידע באופן משמעותי (למשל, מאגר

המידע נפרץ והדבר עלול לגרום נזק כלכלי לנשוא המידע), יש להודיע על כך לרשויות הפיקוח ולנשוא המידע.

ג. **אבטחת המידע** - על המחזיק במידע לעשות שימוש באמצעים טכניים וארגוניים המבטיחים ציות להוראות. אמצעים אלו יכללו אמצעים טכניים, הכשרת עובדים, ביקורת פנימית, עיצוב והגנה על נתונים באופן שיצמצם את הסיכון לזיהויו של נשוא המידע (צמצום מידע, שמות בדויים וכדומה).

חשוב לציין, שבו ביום שבו נכנסו התקנות לתוקף, ב-25 למאי השנה, הוגשו תלונות נגד חברות Google, Facebook, WhatsApp ו-Instagram על ידי הארגון להגנת זכויות הצרכן באירופה, Noyb, בטענה שהחברות האמורות הפרו את התקנות.[4] התלונות התמקדו בכך שהחברות ביקשו אמנם את הסכמת המשתמשים לקבל את פרטיהם האישיים, אך הסכמה זו, כך נטען, לא ניתנה באופן חופשי, כנדרש על פי התקנות. זאת משום שהחברות חסמו חשבונות של משתמשים שלא הסכימו למסור את פרטיהם או שהקשו עליהם את השימוש בשירותיהן, באופן שאילץ את המשתמשים לתת את הסכמתם. בתגובתן לתלונות אלו, טענו החברות האמורות שהן פעלו במשך למעלה משנה לפני כניסת התקנות לתוקף על מנת להתאים את שירותיהן לדרישות שבתקנות, והן אף ממשיכות בימים אלו לפעול לשיפור שירותיהן באופן שיעלה בקנה אחד עם התקנות.[5] במידה והתלונות תתקבלנה, החברות האמורות צפויות לספוג קנסות שיכולים להגיע עד לסכום של 3 ביליון יורו.

להשלמת התמונה, מן הראוי לציין שכחודש לפני כניסתן של התקנות לתוקף, בישראל נכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע), תשע״ז-2017. התקנות הישראליות מאמצות חלק ניכר מן החובות המוטלות על המחזיק במאגר על פי תקנות הגנת המידע האירופיות, אך הן אינן עוסקות בזכויותיו של נשוא המידע. חלק מן הזכויות שנקבעו בתקנות האירופיות קבועות בחוק הגנת הפרטיות, כמו הזכות לעיין במידע (סעיף 13) והזכות לתקן מידע שגוי (סעיף 14).

---

[4] קישורים לתלונות ניתן למצוא באתר הארגון, כאן.

[5] ראו דיווח באתר הבינלאומי של עיתון ה׳גארדיאן׳, כאן.