קצת על ההשתלטות העוינת הפרטית של אירופה על העולם העסקי /עו"ד עדי מרכוס*

בשנת 2018 החלה השתלטות עוינת אירופית על עולם העסקים העולמי. לא הרגשתם אותה? אם החברה שלכם עושה עסקים עם גופים באיחוד האירופי או מתקשרת עם לקוחות מהאיחוד האירופי – סביר שעוד תרגישו. שם הקוד אשר ניתן למבצע ההשתלטות: GDPR, ויש לו לכאורה נגיעה לכל דבר הנוגע לאבטחת מידע ושימוש במידע אישי, אבל בפועל יש לו נגיעה לכל פעילות עסקית, בכל מקום בעולם!

ב 25 במאי 2018 נכנסה לתוקף הדירקטיבה האירופאית להגנה על מידע (שמה המלא הינו: The General Data Protection Regulation, אולם כולם מכירים אותה תחת הקיצור: GDPR), אשר הביאה עימה את השינוי המקיף ביותר לדיני אבטחת מידע מזה מספר עשורים ויצרה מהפך אמיתי בדרישות המוטלות על חברות האוספות או מעבדות מידע אישי של אנשים. השינוי המשמעותי ביותר שהביאה הדירקטיבה היא החלת אחריות ישירה ומוחלטת על חברות ואנשים פרטיים האוספים מידע אישי או מעבדים אותו, לשמירה על סודיות המידע האישי שהן אוספות ולהצדיק מבחינה חוקיות את השימוש בו.

הדירקטיבה אימצה קונספט חדש של פרטיות מתוכננת בנוסף על פרטיות כברירת מחדל והפרתה חושפת לקנסות כבדים הנעים בין 20,000 יורו ל 4% מרווחי החברה. כך, השמירה על סודיות המידע צריכה להיות בשקיפות מלאה מול הלקוח וכזו אשר תוכננה מראש באופן פרו-אקטיבי, מובנית לתוך הטכנולוגיה או תהליך איסוף המידע, ומובטחת באופן אוטומטי, כאשר הלקוח נשוא המידע אינו נדרש לעשות כל פעולה נוספת מצידו על מנת להבטיח את אבטחת או סודיות המידע. עוד, העברת מידע לגבי אזרחי האיחוד מחוץ לגבולות האיחוד האירופי מותרת רק למדינה שנבחנה על ידי האיחוד האירופי ונמצאה עומדת בקריטריונים. יתרה מכך, גם ללא העברת מידע מחוץ לגבולות האיחוד האירופי, הדירקטיבה חלה על כל מידע הקשור לאזרחי האיחוד או לחברות הפועלות באיחוד.

במילים אחרות, אם החברה שלכם מוכרת מוצרים או אוספת מידע אישי של אזרחי האיחוד האירופי או מתקשרת בהסכם עם חברה רשומה באיחוד לפיו אתם חשופים למידע של אותה חברה – עליכם לעמוד בכללי הדירקטיבה. למעשה, גם אם החברה שלכם מספקת שירותים ומקבלת מידע רק לגבי אזרחים ישראליים, די שאחד מהם מחזיק במקביל גם באזרחות אירופאית (דבר נפוץ בישראל), כדי להחיל את הדירקטיבה על החברה

רוב החברות הישראליות מתאימות עצמן לחקיקת הפרטיות הישראלית ולתקנות שהותקנו מכוחה ומאמינות שבכך הן מוגנות, אבל אינן מודעות לכך שהחקיקה הישראלית חסרה רבים מהמרכיבים הקיימים בדירקטיבה האירופאית כמו הזכות להישכח, הזכות של אדם לחזור בו מהסכמה שנתן לעיבוד או שימוש במידע אישי שלו או החובה על חברה האוספת מידע להצהיר בפני לקוחותיה על הסיבה החוקית המצדיקה את איסוף המידע מלכתחילה. במקביל, חברות ישראליות רבות מתקשרות עם גופים אירופאים או אזרחים אירופאים ואוספות מידע אישי לגביהם, תוך שאינם מודעות לכך שעמידה בכללים הישראליים אינה מגינה בפני הפרה של כללי הדירקטיבה.

מה אם כך נדרשים ארגונים ישראלים לעשות על מנת לעמוד בדרישות הדירקטיבה? מומלץ להיעזר בעורך דין בעל מומחיות בתחום כדי לייצר תכנית אכיפה פנימית בנושא, לאחר בדיקה ארגונית פנימית על מנת לאבחן איזה מידע אישי אוספת החברה, איזה שימושים נעשים בו, ומה הסיבות החוקיות המצדיקות איסופו וזאת על מנת לקבוע האם הוראות הדירקטיבה חלות. כחלק מתוכנית האכיפה הפנימית יש לאמץ נהלים פנימיים לאבטחת מידע ושמירה על סודיות, לעדכן את מדיניות הפרטיות ותנאי השימוש, לאמץ נוהל שקיפות, לשנות את ההסכמים עם עובדים וקבלני משנה בעלי גישה למידע ולנקוט בכל צעד נדרש אחר כדי למנוע הפרת הדירקטיבה האירופית.

---

* **עו"ד עדי מרכוס.** הינה עורכת דין במשרד אפיק ושות' (www.afiklaw.com) המתמקדת במשפט מסחרי ודיני חברות, זכויות יוצרים, דיני תקשורת ואומנים ועסקאות בינלאומיות. עו"ד מרכוס הינה בוגרת הפקולטה למשפטים ובעלת תואר שני בתקשורת באוניברסיטת תל אביב ותואר שני במנהל עסקים בינלאומי מאוניברסיטת בר אילן. היא התמחתה במשרד המשפטית אצל המשנה ליועץ המשפטי לממשלה בתחום הדין האזרחי וזכויות היוצרים, לאחר מכן עבדה 18 חודש במשרד שלמה כהן בתחום הקניין הרוחני, כ-11 שנה במחלקה המשפטית בגוף התקשורת "רשת נגה בע"מ"(ערוץ 2 של הטלוויזיה), כאשר תפקידה האחרון בטרם מיזוג החברה עם ערוץ 10, כראש תחום במחלקה המשפטית ולאחר כן, טרם הצטרפותה למשרד, כיועצת המשפטית הפנימית של קנלר ייצוג אמנים, בכל נושא היעוץ המשפט של אמנים ואנשי תרבות, בין בישראל ובין במישור הבינלאומי. אין בסקירה כללית זו משום ייעוץ משפטי כלשהו ומומלץ להיוועץ בעורך דין המתמחה בתחום זה בטרם קבלת כל החלטה בנושאים המתוארים בסקירה זו. לפרטים נוספים: 03-6093609, או באמצעות הדואר האלקטרוני: afiklaw@afiklaw.com.

Some thought on Europe's private hostile takeover of the business world/ Adi Marcus, Adv. *

In 2018, a hostile European takeover of the global business world has began. Didn't you feel it? If your company does business with entities in the EU or contacts with customers from the EU - you are likely to feel it. The code name given to the takeover operation: GDPR, and it ostensibly touches on everything related to information security and use of personal information, but in practice it has a touch on every business activity, anywhere in the world!

On May 25, 2018, the European data protection directive came into force (its full name is: The General Data Protection Regulation, but everyone knows it under the abbreviation: GDPR), which brought with it the most comprehensive change to information security law in decades and created a real revolution in requirements for businesses that collect or process people's personal information. The most significant change brought about by the directive is the application of direct and absolute responsibility to companies and individuals who collect or process personal information, to maintain the confidentiality of the personal information they collect and to legally justify its use.

The directive adopted a new concept of planned privacy in addition to privacy by default and its breach exposes to heavy fines ranging from Euro 20,000 to 4% of the business' profits. Thus, the confidentiality of the information must be fully transparent to the customer and one that is pre-planned proactively, built into the technology or information collection process, and guaranteed automatically, with the subject of the information is not required to take any further action on its part to ensure security or confidentiality of data. Furthermore, the transfer of information about EU citizens outside the borders of the EU is only allowed to a country that has been examined by the EU and found to meet the criteria. Moreover, even without transferring information outside the EU, the Directive applies to all information related to EU citizens or companies operating in the EU.

In other words, if your company sells products or collects personal information of EU citizens or enters into an agreement with a company registered in the EU according to which you are exposed to data of such company - you must comply with the Directive. In fact, even if your company provides services and receives information only about Israeli citizens, it is enough that one of them also holds European citizenship (a common thing in Israel), in order to apply the Directive to you.

Most Israeli companies comply with Israeli privacy legislation and regulations enacted under it and believe that they are safe, but are unaware that Israeli legislation lacks many of the elements in the European Directive such as the right to be forgotten, a person's right to withdraw consent given to processing or use of data or the obligation of the collecting company to declare to its customers the legal reason justifying the collection of information in the first place. At the same time, many Israeli companies communicate with European entities and collect personal data about them, while not being aware that compliance with Israeli rules does not protect against violating the Directive.

What, then, are Israeli organizations required to do in order to meet the requirements of the Directive? It is advisable to enlist the help of a lawyer with expertise in the field, to produce an internal enforcement plan, after an internal organizational review to diagnose what personal information the company collects, what uses are made thereof, and what legal reasons justify its collection, to determine whether the Directive applies. As part of the internal enforcement plan, internal procedures for information security and confidentiality and a transparency police are to be adopted, privacy policies and terms of use updated, as well as amendments to agreements with employees and subcontractors with access to data and any other step taken to prevent breach of the Directive.

---

* **Adi Marcus, Adv.** is an attorney in the office of Afik & Co. (www.afiklaw.com) who focuses primarily on commercial and corporate law, copyrights, media law and international transactions. Advocate Marcus holds a major in law, an M.A in communication from Tel Aviv University and an international MBA from Bar Ilan University. She completed her internship at the Ministry of justice under the Deputy Attorney General focusing civil law and copyright law, then worked for about 18 months in the office of Shlomo Cohen in the field of intellectual property, about 11 years in the legal department of the communications network "Noga Network" (Channel 2 of TV), with her last position before the company merged with Channel 10, was head of department in the legal department and then, before joining the firm, as Kneller Artists Representation's internal legal advisor, representing in all matters of legal advice to artists and cultural figures, both in Israel and internationally. Nothing herein should be treated as a legal advice and all issues must be reviewed on a case-by-case basis. For additional details: +972-3-6093609 or at the e-mail: afiklaw@afiklaw.com.