

דצמבר 2017

מהפכת ה-GDPR (General Data Protection Regulation)

מבוא

התקנות הכלליות של הפרלמנט האירופי לשמירה על מידע של אנשים פרטיים המכונות בשם הקיצור GDPR¹ ("GDPR" או "ההוראות") הן הוראות רגולטוריות-אירופאיות שמטרתן להגן על פרטיותם של תושבי האיחוד האירופי ("האיחוד") בעולם טכנולוגי משתנה, חדשני ושונה לחלוטין מהעולם בו נכתבו הוראות פרטיות קודמות העוסקות בנושא זה².

על אף שמדובר ברגולציה זרה קשה להפריז בחשיבותן של ההוראות עבור כל מי שמנהל מאגרי מידע הכוללים תושבים אירופאים או מי שמבצע פעולות ניטור ועיבוד של מאגרים כאלה. ההוראות, שתיכנסנה לתוקף מחייב בחודש מאי 2018, מבטאות שינוי גישה ברגולציה האירופאית (בעלת השלכה עולמית) המרחיבה את החובות החלות על גופים המחזיקים או מעבדים מידע אישי ביחס לתושבי האיחוד או מספקים שירותים או מוצרים לתושביו. ההוראות קובעות בין היתר את העיקרון המרכזי לפיו ניתן לעבד מידע שנאגר באחד המקרים הבאים- (א) ניתנה לשם כך הסכמה של נושא המידע (המשתמש); (ב) הדבר נדרש לביצוע חוזה שנושא המידע צד לו; או (ג) קיימת חובה חוקית לביצוע עיבוד המידע. למעט במקרים מיוחדים בהם נדרשים קיומם של תנאים נוספים, אסור יהיה לעבד או לאגור מידע אישי שנאגר ללא שנתקימו תנאים אלה.

הסיבות המרכזיות, אם כי לא היחידות, בגללן תקנות ה-GDPR משמעותיות כל-כך גם לחברות שאינן אירופאיות הן:

- תחולתן של התקנות היא אקס טריטוריאלית;
- קיימת תחולה של ההוראות המרכזיות הן לגבי בעלים של מאגרי מידע והן לגבי מי שיש לו גישה למאגרי מידע (כגון מי שנותן שירותי עיבוד של מידע וכו');;
- ההסכמה הנדרשת לעיבוד המידע היא אקטיבית;
- ניתנות זכויות מיוחדות למי שהמידע עליו שמור במאגר מידע: הזכות "להישכח" מהמאגר, הזכות לדעת מה תוצרי המידע שהופק לגביו, הזכות להתנגד לעיבוד המידע ועוד.
- הקנס בגין עבירות על הוראות GDPR עלול להגיע עד 20 מיליון יורו או 4% מהמחזור של הגוף המבוקר;

להלן במזכר זה נסרוק את עיקרי הנושאים הקשורים בתקנות ה-GDPR. כבר עתה נציין כי משרדנו, בשיתוף עם המשרד הגרמני [HYAZINTH](#), שקד בתקופה האחרונה על הכנת המידע וההתאמות הנדרשות לחברות ישראליות אשר כללי GDPR עשויים לחול עליהן ואנו נעמיד לרשות לקוחותינו, באמצעות משרד HYAZINTH, את מיטב המידע ואנשי המקצוע על מנת להתמודד עם דרישות אלה.

¹ Regulation (EU) 2016/679 of the European parliament on the protection of natural persons with regard to the processing of personal data and on the free movement of such data Directive (General Data Protection Regulation

² הוראה EC / 95/46 של הפרלמנט האירופי ושל המועצה מיום 24 באוקטובר 1995 להגנת הפרט ביחס לעיבוד נתונים אישיים ותנועה חופשית של נתונים אלה.

מידע כללי – תחולת הוראות GDPR

להלן יוצגו עקרונות הקשורים בGDPR, הוראות שונות ודוגמאות. יש בהן כדי לתת מושג עקרוני על הדרישות החדשות ועל תחולתן. המידע שלהלן אינו ממצה ואינו מהווה חוות דעת משפטית. ביצוע ההתאמות הנדרשות, עדכון תנאי הפרטיות הנדרשים והתאמת הדרישות צריכות להנתן פרטנית, בשיתוף היועצים המשפטיים ממשרד HYAZINTH.

הגופים שיחולו לגביהן הוראות GDPR

ה-GDPR מפריד בין שני סוגי גופים שעליהם חלות ההוראות: הגוף השולט במידע ("Controller"), להלן יקרא "בעל המאגר", האוסף והמחזיק את המידע האישי והגוף המעבד ("Processor") להלן יקרא "מעבד" - גוף שמבצע פעולת עיבוד והפקת נתונים עבור מי ששולט במידע (למשל, חברה שמנתחת נתוני מידע אישי שנאספו)³. היקף החובות הרלוונטיות והאחריות המשפטית נקבעת בהתאם לסוג הגוף (בעל מאגר ו/או מעבד) ולפעילותו. כך למשל קובעות ההוראות, שמעבד נדרש לשמור רשומות של פעילויות עיבוד אותן ביצע על מידע אישי שהעמיד לרשותו בעל המאגר, ואם תופר החובה – המעבד יישא באחריות. יובהר כי לעיתים בעל המאגר יהיה זה שגם מעבד את נתוני המידע – ובמצב דברים כזה על אותו גוף "כפול" יחולו כלל החובות הרלוונטיות המנויות בהוראות (הן אלו החלות על בעל המאגר והן אלו החלות על המעבד).

תחולה אקס-טריטוריאלית

הוראות ה-GDPR חלות גם ביחס לגופים שאינם ממוקמים או רשומים באירופה, כאשר הם אוספים או מעבדים מידע אישי ביחס לאותם אנשים פרטיים שהמידע לגביהם נאסף ("נושאי המידע") המתגוררים במדינות האיחוד האירופי ("האיחוד"). ההוראות יחולו אף אם פעולת עיבוד המידע עצמה אינה נעשית בתחומי האיחוד, אם גוף אוסף או מעבד מידע מספק שירותים או מוצרים לאזרחי האיחוד ומבצע אגב כך ניטור של התנהגויות (כגון יצירת פרופיל התנהגותי של משתמש) שמתרחש במדינות האיחוד. בנוסף ההוראות יחולו על מעבד או בעל מאגר הפועלים לניטור של התנהגות של נושאי המידע הכלולים במאגר (כגון יצירת פרופיל, ניטור של העדפות התנהגותיות וכו'), ככל שאלה הם תושבי האיחוד. **בעל מאגר או מעבדי מידע שאין להם נוכחות פיזית באיחוד, חייבים למנות נציג מטעמם בתחומי האיחוד, אליו יוכלו לפנות נושאי מידע ורשויות הגנת המידע בקשר עם עיבוד המידע.**

³ להבהרה: אם חברה א' מעניקה שירותים מסויימים באינטרנט ללקוחות האיחוד האירופי או אוגרת מידע על לקוחותיה באינטרנט ועל לקוחותיה של חברה א' מבצעת חברה ב' פעולות עיבוד ו/או ניטור שונות על מנת לספק לחברה א' או צדדים שלישיים מידע כלשהו אזי חברה א' היא "בעל המאגר" וחברה ב' היא "המעבד".

הסכמה

הוראות ה-GDPR קובעות כי נדרשת הסכמת נושא המידע לאגור מידע אודותיו ולעבד אותו וכי עליה להינתן מרצון ולצורך מסוים (שיוסבר לנושא המידע) בהתבסס על הודעה בשפה מובנת, פשוטה, נגישה ונפרדת ממידע נוסף שנמסר לנושא המידע ביחס לשירותים או המוצרים שהם מקבלים. למשל – סימון אקטיבי של תיבה (צ'ק בוקס) הכוללת לצידה את האישור בשפה ברורה. התקנות מציינות במפורש כי שתיקה, תיבות המסומנות מראש באישור, או כל העדר מעשה אקטיבי של הסכמה מצד נושא המידע לא ייחשבו כהסכמה תקפה ולמעשה דורשות הסכמה בתצורת "opt in". יתרה מכך, המעבד עשוי להידרש להוכיח קיומה של "הסכמה תקפה" ולכן עליו לשמור על ראיות לכך. בנוסף, בעל המידע צריך להיות מסוגל לבטל את הסכמתו באופן פשוט ובדומה לאופן בו הוא נותן אותה מלכתחילה. לגבי הסכמות שכבר ניתנו לפני כניסת הוראות ה-GDPR לתוקף, יש לוודא שהן נתקבלו באופן שעומד בהוראות, ובמידת הצורך לקבל הסכמות חדשות.

המידע שלגביו יחולו הוראות ה-GDPR

בהתאם להוראות, מידע אישי כולל כל מידע הקשור לנושא מידע, שניתן להשתמש בו כדי לזהות במישרין או בעקיפין את נושא המידע, לרבות שם, תמונה, כתובת דואר אלקטרוני, פרטי בנק, הודעות על אתרי רשתות חברתיות, מידע רפואי, כתובת IP של מחשב ונתונים אישיים רגישים כדוגמת נתונים גנטיים או ביומטריים. כך למשל, נתוני כוח אדם, רשימות לקוחות, או פרטים ליצירת קשר שנאגרו בארגון מסוים, בין אם נאגרו אוטומטית או במערכות תיוק ידניות בנסיבות מסוימות עשויים להיחשב מידע אישי, אף אם המידע שמור תחת שם בדוי או חסוי ובלבד שניתן ליחסו לנושא מידע מסוים.

זכויות נושאי המידע

הוראות ה-GDPR מעניקות לנושאי המידע זכויות מסוגים שונים ומטילות הוראות מחייבות על מחזיק במידע בקשר עם פעולות של איסוף ועיבוד מידע ואף ביחס להעברתו לצדדים שלישיים:

- זכות גישה למידע. זכאות לקבל אישור ותמצית מהמחזיק במידע ביחס לאיסוף ועיבוד נתונים לגביהם, לרבות מטרת העיבוד, ואף לקבל עותק אלקטרוני המכיל את המידע המעובד בצורה מובנת, פשוטה, שקופה וברורה וכל זאת ללא עלות.
- זכות לתיקון מידע אישי. נושאי המידע זכאים לבקש לתקן את המידע האישי לגביהם.
- זכות "להישכח". הזכות לדרוש מהמחזיק במידע למחוק את המידע האישי המוחזק אודותיו, להפסיק את עיבוד המידע ו/או להפסיק את ביצוע העיבוד על ידי צדדים שלישיים, בנסיבות מסוימות, לרבות כאשר המידע האישי כבר אינו נחוץ לשם המטרה שלשמה נאסף או כאשר אין אינטרס לגיטימי להמשיך עיבוד המידע.
- ניידות מידע אישי. הזכות להעתיק או להעביר את המידע האישי מסביבה אחת לאחרת בצורה בטוחה וללא הפרעה לשימוש.

- הגבלה על עיבוד המידע: הדרישה שלא לכלול ולעבד מידע אישי אשר לא נדרש בפירוש לצורך אספקת השירותים ו/או המוצרים לנושא המידע.
- הזכות להתנגד: לעיתים נושא מידע עשוי להתנגד לאיסוף או עיבוד מידע בענייננו. למשל, היה והתנגד נושא מידע לעיבוד מידע אודותיו לצרכים סטטיסטיים (לצורך הדוגמא, ההתנגדות יכולה להיות גם במקרים נוספים), על מעבד המידע להפסיק את העיבוד.
- זכויות הקשורות לקבלת החלטות אוטומטיות ולאפיון: לנושא מידע הזכות שמידע אודותיו לא יהיה נתון לפעולות עיבוד וקבלת החלטות אוטומטיות ביחס למידע שמשפיעה באופן משפטי או באופן משמעותי על חייו וכן תהיה לו זכות להביע דעתו ולקבל הסבר על החלטה שנתקבלה באופן אוטומטי (ואף להתנגד לה). על המחזיק ו/או המעבד להבטיח שניתן יהיה להתערב בפעולות אוטומטיות. למשל, במקרה שמתקבלת החלטה אוטומטית לסווג נושא מידע כבעל דירוג אשראי בהתבסס על נתונים מהמאגר, נושא המידע יוכל להתנגד לקבלת החלטה בדרך זו ואף לטעון כי הפרטים המצויים במאגר אינם מדויקים וכי אין לבסס לפיהם החלטה זו.

סוג והיקף החובות בארגון

- חובת מינוי אחראי הגנת מידע: הוראות ה-GDPR מקימות חובה על בעלי מאגרים ומעבדים למנות ממונה אבטחת מידע (DPO – Data Protection Officer) להלן: **"הממונה"** כאשר (א) עיבוד מידע אישי מהווה חלק מרכזי בפעילותם המצריכה פעולות ניטור קבוע ושיטתי בקנה מידה גדול; או (ב) מתבצע עיבוד של מידע אישי רגיש (כהגדרתו בהמשך) בקנה מידה גדול; או (ג) ברשות ציבורית. הממונה יהיה אמון על הציות להוראות ה-GDPR ולכל רגולציה אחרת להגנה על מידע אישי, יודיע וייעץ לחברה ועובדיה באשר להוראות, ינהל פעולות פנימיות לאכיפת ההוראות וביצוע החובות החלות מכוחן בתוך הארגון, יבצע ביקורות עצמיות בחברה וישמש איש הקשר בין החברה לרשויות הפיקוח ומול נושאי המידע האישי המעובד (עובדים, לקוחות וכו'), ולשם כל אלו תקצה החברה משאבים מתאימים. הממונה ימונה על בסיס מקצועיות וידע נרחב בחוקי והגנת המידע ונהלי העבודה בתחום, וניתן למנותו גם באמצעות ספק חיצוני. באשר לחברות שאין להן חובה על-פי ההוראות בממונה, מינוי שכזה יהווה סיוע יעיל בשמירה על עמידה בחובות האחרות שההוראות מחילות.
- חובות דיווח; ביקורות; תיעוד: ה-GDPR מטילות חובות שמטרתן להבטיח את ההגנה על המידע, לרבות:
 - חובת יישום ושימוש באמצעים טכניים וארגוניים המבטיחים ומבטאים ציות להוראות לרבות, הטמעת מדיניות הגנה על נתונים פנימיים (כדוגמת הכשרה צוות, ביקורת פנימית של פעילויות עיבוד וכו').
 - עיצוב והגנה על נתונים כברירת מחדל. יישום אמצעים העונים על העקרונות של הגנת נתונים לרבות, צמצום נתונים שנאספים; שם בדוי; שקיפות; מתן אפשרות לנושאי המידע לעקוב אחר העיבוד; ויצירת ושיפור תכונות האבטחה באופן שוטף.
 - תיעוד פעילויות ותהליך עיבוד המידע. כחלק מהחובות המוטלות על בעל מאגר או מעבד, עליהם לנהל תיעוד ורשומות ביחס לעיבוד מידע אישי המתבצע בתוך הארגון. על אף האמור, כשהארגון מונה פחות

מ-250 עובדים לא תחול חובה גורפת כזו, אלא אם כן מתבצע עיבוד מידע אישי שעשוי לסכן את זכויות נושאי המידע, כשהעיבוד אינו אקראי או כשמדובר בעיבוד של מידע רגיש. התיעוד יכלול רשומות פנימיות של פעולות העיבוד במסגרתן יתוארו, בין היתר - שם ופרטי הארגון; מטרות העיבוד; תיאור הקטגוריות של נושאי המידע האישי וקטגוריות של נתונים אישיים; קטגוריות של מקבלי נתונים אישיים; פירוט העברות למדינות שלישיות, כולל תיעוד מנגנוני מנגנון ההעברה; תיאור של אמצעי אבטחה טכניים וארגוניים. רשומות אלו עשויות לעבור לרשות הפיקוח הרלוונטית לצורך חקירה.

○ דיווח על הפרה. במקרה שבו כתוצאה מהפרה של ההוראות, הזכות לפרטיות של נושא מידע נפגעת בצורה שתשבש באופן משמעותי את חייו (למשל פריצה למאגר וחשיפה של צד שלישי למידע אישי שעשוי לגרום לאפליה, נזק למוניטין, הפסד כספי, אבדן סודיות או כל פגיעה כלכלית או חברתית משמעותית אחרת לנושא המידע) – בעל המאגר ו/או המעבד המחזיקים במידה מחויבים להודיע על כך לרשויות הפיקוח והן לנושא המידע עצמו.

● העברות של נתונים אישיים לצד שלישי. העברת נתונים אישיים מחוץ לאיחוד (למשל למדינות או לארגונים בינלאומיים שאינם חלק מהאיחוד) הינה מוגבלת וזאת על מנת להבטיח כי רמת ההגנה של יחידים המחויבת במסגרת ה-GDPR לא תתערער. למעשה מתקיימים ארבעה דרכי העברה שמותר לבצע על פי ההוראות: (1) בהחלטה כללית של ועדה רגולטורית-אירופאית שנוכחה כי מתקיימת במדינה או בארגון הנעבר רמה נאותה של הגנה על מידע אישי; (2) העברה על בסיס אמצעי הגנה נאותים שיספק הגוף הנעבר, למשל - סעיפים בחוזה שאומצו ע"י הועדה ומטרתם להגן על המידע; הסכם מחייב בשמירה על ההגנה בין גופים ציבוריים או בתוך קבוצה תאגידית; תקני הגנה סטנדרטיים שנאכפים אצל הגוף הנעבר ואושרו על-ידי הרשות המפקחת; הסמכה תחת מנגנון אישור מאושר לפי ה-GDPR וכו'; (3) בכל אחד מהמקרים הבאים: כאשר ההעברה נעשית בהסכמה של נושא המידע; ההעברה כרוכה בביצוע חוזה שנושא המידע האישי הוא צד לו; ההעברה הכרחית מטעמי האינטרס הציבורי או לביסוס, מימוש או הגנה על טענות משפטיות לרבות מול רשויות מדינתיות; ההעברה הכרחית כדי להגן על האינטרסים החיוניים של נושא המידע האישי או אנשים אחרים, כאשר נושא הנתונים פיזית או משפטית לא מסוגל לתת הסכמה; ההעברה נעשית מתוך מאגר אשר על פי החוק נועד לספק מידע לציבור; וכן (4) העברה הכרחית וחד פעמית, בהיקף מצומצם וכן שבשקלול הנסיבות נחה דעתו של המעביר כי ההעברה נעשית תחת הגנה נאותה. העברה כאמור, כפופה למתן הודעה לרשות ולנושאי המידע הרלוונטיים.

עיבוד מידע באופן חוקי

עיבוד של מידע אישי עשוי להיחשב כלגיטימי במסגרת הוראות ה-GDPR, בנסיבות בהן יצליח המעבד להראות כי התקיימו אחד מאלו: (א) התקבלה הסכמת נושא המידע האישי; (ב) העיבוד הכרחי לביצוע התחייבות במסגרת התקשרות עם נושא המידע האישי; (ג) העיבוד הכרחי לעמידה בהתחייבות משפטית שבעל המאגר כפוף לה; (ד) העיבוד הכרחי לצורך הגנה על האינטרסים של נושא המידע או אדם אחר; (ה) העיבוד נחוץ לטובת הציבור או בהפעלת סמכות רשמית שניתנה לחברה; (ו) העיבוד הכרחי לאינטרסים לגיטימיים שגוברים על

זכויות נושאי המידע.

גם סוג המידע עצמו עשוי לשנות ולכן כל עיבוד מידע הנעשה ביחס לנתונים אישיים שחושפים מוצא גזעי או אתני, דעות פוליטיות, אמונות דתיות או פילוסופיות, או חברות באיגוד מקצועי, ועיבוד נתונים גנטיים, נתונים ביומטריים לצורך זיהוי ייחודי של אדם, נתונים הנוגעים לבריאות או לנתונים הנוגעים לטבע חיי המין של האדם או הנטייה המינית שלו (לעיל ולהלן: **"מידע אישי רגיש"**) – הינו אסור, למעט אם יתקיימו נסיבות מסוימות (לדגו' - הסכמה מפורשת של נושא המידע; או עיבוד הנחוץ להגן על אינטרסים חיוניים של נושא המידע; או שבוצע על ידי גוף ללא כוונת רווח עם מטרה חברתית (פוליטית, פילוסופית); או העיבוד הכרחי לביסוס הליך משפטי; או אינטרס ציבורי בתחום בריאות הציבור וכו').

הוראות ביחס לנושאי מידע מיוחדים

- **מידע אודות ילדים**. ה-GDPR כוללת הוראות חדשות שנועדו להגן על המידע האישי של הילד כאשר שירותים מוצעים ישירות לילד. כך למשל, על בעל מאגר ו/או מעבד לוודא שהודעת הפרטיות כתובה בצורה ברורה והמובנת לילדים. במקרה של הצעת שירות מקוון לילדים, נקבע כי ילד מתחת לגיל 16⁴ אינו יכול לתת את הסכמתו בעצמו לעיבוד המידע בעניינו ונדרשת הסכמת הורה או אפוטרופוס. על בעל המאגר לעשות מאמצים סבירים לוודא שמדובר באחראי על הילד, בהתחשב בזמינות של אמצעים טכנולוגיים בהקשר זה.
- **מידע אודות עובדים**. ה-GDPR כולל הוראות שנועדו להגן על המידע האישי של עובדים אשר נאסף לגביהם מידע והוא מעובד על ידי המעסיק. עיבוד של מידע על עובדים הינו אסור למעט אם העיבוד מתבצע למטרות העסקתו וניתנה הסכמה של העובד לעיבוד המידע שנשמר אודותיו. בנוסף עיבוד זה מותר אם יש בו צורך למטרות חוק.

אכיפה וענישה

ה-GDPR מטילות סנקציות חריפות כלפי המפרים אותן. אמנם הענישה היא הדרגתית (למשל חברה שלא תשמור על מסמכים ותיעוד תקין או שלא תודיע לרשויות במקרים המחייבים לא תיקנס בקנס המקסימלי) אך גוף שיפר הפרה משמעותית של ההוראות (למשל, אי הסכמה מפורשת של נושא מידע לעבד מידע אודותיו) עשוי לשאת בקנס מקסימלי בגובה של עד 4% מאותו מחזור של גוף זה או 20 מיליון יורו (לפי הגבוה).

לסיכום

החל מכניסתן לתוקף מחייב בסוף מאי 2018, הוראות ה-GDPR יבצעו "מהפכה" בכל הקשור להגנות שחברה האוספת ו/או מעבדת מידע אישי של אדם תחויב בביצוען ויישומן. ההוראות החדשות מבקשות להתמודד עם עולם שבו דרכי האיסוף והעיבוד של מידע על אדם מגוונות, חדשניות ולעיתים נסתרות ואף נלוות למתן שירות או מוצר עיקרי ואחר. לכן ההוראות מטילות חובות וזכויות שונות, ישירות ועקיפות על שלל המעורבים, באופן שעשוי להיות כמעט מבלבל וחסר סדר. על ארגונים שאוגרים מידע אישי של נושאי מידע המתגוררים במדינות

⁴ מדינות מסוימות באיחוד רשאיות לקבוע גיל נמוך יותר, ובלבד שלא יפחות מ-13 שנים.

האיחוד ו/או מעבדים אותו (אם בעצמם ואם באמצעות גורם חיצוני) להתכונן לשינוי המשמעותי שיגרם כתוצאה מתחולת ההוראות ולבדוק היטב את מערך האבטחה שלהם ביחס למידע האישי שנאגר אצלם, את אופן עיבוד המידע ואת מדיניות הפרטיות המוטמעת בארגונים אלו.

בכל מידע נוסף ניתן לפנות לצוות הרלוונטי במחלקת ההי-טק במשרדנו:

עו"ד יריב קסנר yariv@novlaw.com

עו"ד הילה יצחקי hilaizhaki@novlaw.com

עו"ד אורן אברהם oren@novlaw.com

טלפון - 03-5441411

האמור לעיל מהווה סקירה בלבד של עיקרי ה-GDPR, אשר הינן הוראות דין אירופי. המידע הינו למטרות אינפורמציה כללית בלבד, הוא אינו מידע מלא ושלם ואין להסתמך עליו ללא חוות דעת מיועץ משפטי אירופי המוסמך לתת אותה. הסקירה אינה מהווה חוות דעת משפטית או יעוץ משפטי או תחליף לייעוץ משפטי קונקרטי בעניינים ספציפיים. על הקורא לפנות ולהתייעץ עם עו"ד המוסמך לתת ייעוץ על הדין האירופי בטרם ינקוט כל פעולה משפטית או הימנעות מפעולה הקשורה לאמור במזכר זה. משרדנו יכול ללוות את הקורא בעניין זה, לחבר אותו לעו"ד אירופאים אשר עובדים בשיתוף עמנו והינם מוסמכים לתת ייעוץ ומידע שלם בעניין.