מדריך הגנת הפרטיות

ערכה משפטית

ינואר 2024

קהילת אבטחת המידע והגנה על הפרטיות
info@dpc.org.il

קוראת יקרה,

מדריך זה מוגש לך ככלי עזר, המסכם את החקיקה הבסיסית והעקרונות החשובים עליהם מתבסס תחום הגנת הפרטיות בישראל. חוק הגנת הפרטיות ותקנותיו עברו, עוברים ויעברו בעת הקרובה שינויים רבים, ביניהם הרחבת סמכויות האכיפה של הרשות להגנת הפרטיות ("הרשות") והתאמת הדין הישראלי לדיני הגנת הפרטיות בעולם. המשפט והרגולציה מנסות להתאים עצמן לקצב התקדמות הטכנולוגיה והתאמה זו דורשת הבנה והתמצאות בתחום. כל זאת בנוסף להנחיות רגולטוריות, דרישות חוזיות וציפיות הציבור לשמירה על פרטיותו, מחייבים אותנו לפעול באופן אחראי תוך הפעלת שיקול דעת למימוש מטרותנו, לצד האינטרס הציבורי.

המידע המוצג בקובץ זה הוא מידע כללי בלבד, ואין בו כדי להוות ייעוץ או חוות דעת משפטית. המחברים אינם נושאים באחריות כלשהי כלפי הקוראים, ואלה נדרשים לקבל עצה מקצועית לפני כל פעולה המסתמכת על הדברים האמורים.

בברכה,

עו"ד יעקב עוז

עו"ד מיכל ברטוב

כל הזכויות שמורות © dpc.org.il

תוכן העניינים

חשיבות ההגנה על הפרטיות 4

המסגרת המשפטית והרגולטורית 5

תיקון חוק הגנת הפרטיות - עיקרי תיקון 14 6

ישראל קיבלה מחדש את ה- LEVEL OF ADEQUACY 7

יצירה ויישום של מדיניות הגנה על הפרטיות 8

תפקיד ממונה הגנה על הפרטיות 9

הגנת הפרטיות בעולם 10

האיחוד האירופי 10

ארה"ב 10

נספח א - קישורים למידע נוסף 11

נספח ב - קישורים לחוקים והתקנות העיקריים 12

כל הזכויות שמורות © dpc.org.il

חשיבות ההגנה על הפרטיות

השילוב המקיף של הטכנולוגיה בהיבטים שונים של חיי היומיום שלנו, החל מתקשורת אישית ועד עסקאות פיננסיות וניהול שירותי בריאות, הוביל לכמות חסרת תקדים של מידע אישי שנאסף, מאוחסן ומעובד. כתוצאה מכך, שמירה על נתונים רגישים אלה הפכה חיונית למניעת גישה בלתי מורשית, שימוש לרעה או ניצול, שעלולים להוביל לתוצאות חמורות כגון גניבת זהות, הונאה פיננסית והפרה של חירויות אישיות.

כאשר ממשלות, עסקים וארגונים ממנפים נתונים לקבלת החלטות, יש צורך הולך וגובר בפרקטיקות אתיות ואחראיות כדי להבטיח את האמון והביטחון של הציבור לצד שמירה על מוניטין העסק. דליפות מידע והפרות פרטיות יכולות לא רק לפגוע ביחידים אלא גם לשחוק את יסודות האמון במערכות דיגיטליות. איזון בין היתרונות של ההתקדמות הטכנולוגית עם הצורך בשמירה על הפרטיות הוא אתגר מורכב, אך הוא הכרחי לבניית עתיד דיגיטלי בטוח ואמין.

לכל אדם זכות לפרטיות. הזכות הבסיסית לפרטיות הוכרה בחוק יסוד : כבוד האדם וחירותו. בשנת 1981 נחקק חוק הגנת הפרטיות בו נקבע העיקרון הבסיסי לפיו "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". במדינת ישראל פגיעה בפרטיות היא עבירה פלילית - שעונשה עד 5 שנות מאסר - ועוולה אזרחית - בגינה ניתן לתבוע פיצוי כספי בגין כל נזק שנגרם כתוצאה מהפגיעה אף בלא הוכחת נזק.

יחד עם זאת, הגדרת הזכות לפרטיות נחשבת "קשה ביותר, ואולי אף בלתי אפשרית", כדברי בית המשפט העליון, ולכן היא זוכה לפרשנות אשר משתנה לאורך הזמן ובמרחב הגיאוגרפי. פרשנות מודרנית תופסת את הפרטיות כביטוי של שליטה של אדם בהיקף זרימת המידע על אודותיו, וראיה לכך ניתן למצוא בתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי) התשפ"ג – 2022 ("תקנות הגישור").

תחום ההגנה על המידע נשען על שלושה בסיסים :
הבסיס המשפטי – החוקים, התקנות והנהלים של הרגולטורים המתווים את מדיניות ההגנה הדרושה לעסק
הבסיס הטכנולוגי – מהם הכלים הדרושים לעסק להגנה מיטבית על המידע
ניהול סיכונים – מהו "התיאבון לסיכון" של העסק וכיצד מכמתים אותו

במדריך זה בחרנו להתמקד בבסיס המשפטי.

כל הזכויות שמורות © dpc.org.il

המסגרת המשפטית והרגולטורית

תחומי אבטחת המידע והגנה על הפרטיות נשענים וכפופים למספר רב של חוקים, תקנות והנחיות המתוות את המדיניות בכל הנוגע ליישומם. כלל שעולה הסיכון לפגיעה, לצד רגישות המידע החשוף, כך תגבר מעורבות הרגולטור והוא יקשיח את הדרישות המנדטוריות.
את הבסיס המשפטי ניתן למצוא בסעיף 7 לחוק יסוד: כבוד האדם וחירותו, העוסק בפרטיות וצנעת הפרט:

(1) כל אדם זכאי לפרטיות ולצנעת חייו
(2) אין נכנסים לרשות היחיד של אדם שלא בהסכמתו
(3) אין עורכים חיפוש ברשות היחיד של אדם, על גופו, בגופו או בכליו
(4) אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו

לאחר מכן, חוקק חוק הגנת הפרטיות המפרט מהי פגיעה בפרטיות, כיצד יש להגן על פרטיות במאגרי מידע, מהן ההגנות הקבועות בחוק, ועוד. החוק מפורש ונאכף על ידי הרשות להגנת הפרטיות במשרד המשפטים. למרות הארכאיות שלו, זהו אחד החוקים הראשונים בעולם שעדיין מצליח לעמוד בפני התקדמות הזמן. בימים אלה דנה ועדת חוקה, חוק ומשפט בתיקון 14 לחוק, העוסק בעיקר בחיזוק סמכויותיה של הרשות ובהרמת סף הקנסות שהוא יוכל להטיל על גופים מפרים.

לצד חוק הגנת הפרטיות, ניתן למנות גם את חוק האזנת סתר, חוק נתוני אשראי וחוק המחשבים – היחידים שמתייחסים במפורש לעיקרון ההגנה על הפרטיות.

מכוח חוק הגנת הפרטיות הותקנו עוד מספר חוקים ותקנות משנה אשר העיקריים בהם:

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017

תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה) 2001

תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים) 1986

תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023

בישראל הבסיס החוקי לשמירת מידע פרטי הוא באמצעות "מאגר מידע", המוגדר בחוק כ "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט (1) אוסף לשימוש אישי שאינו למטרות עסק; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;

"מידע" יכול להיות "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו" ואילו "מידע רגיש" הוא נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו. אגב, שלושת המאגרים העיקריים שנרשמים על ידי מעסיקים הם: עובדים, לקוחות, ספקים.

לצד זאת מעת לעת מפרסמת הרשות גילויי דעת שמתייחסים לפרטים נוספים ומרחיבים את הגדרת מידע אישי מעבר להגדרות בחוק וזאת עקב התפתחויות והתאמות לזמנים הנוכחים. לדוגמא – במסגרת גילוי דעת של הרשות, כתובות דוא"ל בנסיבות מסוימות נחשבות כמידע אישי.

אם חוק הגנת הפרטיות עוסק בהגדרות של פרטיות ומהי הפרה של פרטיות, הרי שתקנות הגנת הפרטיות (אבטחת מידע) מגדירות את האופן בו יש להגן על מידע ופרטיות. התקנות מחייבות כל גורם שמחזיק במידע להפעיל אבטחה מתקדמת בהתאם לסוג ולכמות המידע הנחלקות לשלוש רמות - בסיסית, בינונית וגבוהה. מודגש כי החובות המפורטות בתקנות אבטחת המידע תקפות בין אם המאגר נרשם ובין אם לאו.

החוק בישראל מחייב לרשום מאגר מידע אצל רשם מאגרי המידע. כאמור, תיקון 14 לחוק יצמצם את חובת הרישום אך לא יבטלה לחלוטין. לעומת זאת, הגדרת "מידע" ו"מידע רגיש" יורחבו ויכללו כל "נתון הנוגע לאדם מזוהה, או אדם הניתן לזיהוי, במישרין או בעקיפין, באמצעים סבירים, לרבות מזהה ביומטרי, מספר זהות או כל נתון מזהה ייחודי אחר". דהיינו, נתונים רבים יותר יהוו פרטי מידע, ויזכו לכל ההגנות בחוק.

כל הזכויות שמורות © dpc.org.il

תיקון חוק הגנת הפרטיות - עיקרי תיקון 14

מאז חקיקתו של חוק הגנת הפרטיות בשנת 1981, נתקבלו מספר תיקונים ומזה כעשור ישנו ניסיון לתקן את החוק לאור השינויים ותמורות בתחום הגנת המידע הפרטיות, בזירה הדיגיטלית כמו גם בזירה הרגולטורית ובמיוחד לאור הצורך הדחוף לשמור בתוקף את אישור התאימות של ישראל אל מול האיחוד האירופי וה - GDPR ה- LEVEL OF ADEQAUCY (בו נעסוק בהמשך) אך ניסיונות אלה לא באו לידי מעשה חקיקה של ממש. כל זאת היה נכון עד ליום 24 ינואר 2022 בו נתקבלה בקריאה ראשונה הצעת תיקון (14) בחוק. ועדת החוקה בכנסת הקודמת (23) וביתר שאת בכנסת הנוכחית מאיצה את דיוניה לקראת הבאתו של תיקון זה לקריאה שניה ושלישית. בשבועות האחרונים מאז פרוץ המלחמה, ראש המל"ל (המועצה לביטחון לאומי) פנה בכתב ליו"ר ועדת חוקה חוק ומשפט ח"כ שמחה רוטמן, והדגיש את חשיבות התיקון כחלק מחוסנה של מדינת ישראל - עד כדי כך.

התיקון בעיקרו ישנה את החוק בתחומים שלהלן:

- שינוי והוספת הגדרות
- הרחבת סמכויות (מנהליות ופליליות) הרשות להגנת הפרטיות
- חובת מינוי ממונה הגנת הפרטיות בגופים בטחוניים
- תוספת לאכיפה והטלת עיצומים כספיים בהפרת תקנות הגנת הפרטיות (אבטחת מידע)

סקירה מורחבת אודות תיקון 14 ניתן למצוא בקישור שלהלן:
https://main.knesset.gov.il/activity/legislation/laws/pages/lawbill.aspx?t=lawsuggestionssearch&lawitemid=2167975

ומה בקשר לתיקון 15 ? גם בענין זה ישנה התקדמות, נסתיימה עבודת המטה במשרד המשפטים - ייעוץ וחקיקה והרשות להגנת הפרטיות והתיקון עבר לאישורו של שר המשפטים בדרך לתחילת חקיקה.

עיקרי התיקון:

- הזכות להישכח/להמחק
- הרחבת חובת מינוי DPO
- חובת ביצוע תסקיר השפעה DPIA
- ניסוח מחדש של ההסכמה
- הסדרי קטינים
- ועוד.....

כל הזכויות שמורות © dpc.org.il

ישראל קיבלה מחדש את ה- LEVEL OF ADEQUACY

נציבות האיחוד האירופי קבעה כי רמת ההגנה על הפרטיות בישראל תואמת את הרמה הנהוגה באיחוד האירופי.מדובר בחידוש של הכרה שניתנה בשנת 2011 ובהחלטה אשר עשויה לחזק את קשרי המסחר עם מדינות אירופה, לפתח קשרי מחקר ולסייע בקידום תחומים נוספים במשק הישראלי.

מעמד התאימות (Adequacy) שניתן למדינת ישראל בשנת 2011, ואשר במהלך השנים הוקנה לקבוצה מצומצמת של מדינות נוספות מחוץ לאיחוד האירופי, מאפשר להעביר באופן חופשי מידע אישי ממדינות אירופה לישראל, ללא צורך במחויבויות רגולטוריות נוספות מצד הגורם האירופי שמעביר את המידע או מצד הגורם שמקבל את המידע בישראל. בפועל, משמעות מעמד זה היא שדין העברת מידע אישי מאירופה לישראל כמוהו כהעברת מידע בתוך האיחוד האירופי.

החלטת נציבות האיחוד האירופי מאפשרת זרימת מידע אישי לישראל באופן פשוט ונוח, ומקלה מבחינה משפטית ורגולטורית על כלל הגופים בישראל (ובכלל זה חברות ישראליות, עסקים, בתי חולים, מוסדות מחקר ורשויות ציבוריות) שמקבלים מידע אישי מאירופה. הכרה זו מונעת את הצורך במנגנונים פרטניים ועתירי משאבים, כגון הסדרים חוזיים מפורטים, ובכך מפחיתה עלויות לעסקים וארגונים בישראל, מצמצמת סיכונים משפטיים, ומייצרת יתרון תחרותי לחברות ישראליות.

ההחלטה צפויה בהמשך לעלות לדיון בפרלמנט האיחוד האירופי ובמוסדות נוספים של האיחוד האירופי.

שר המשפטים, יריב לוין: "אני מברך על החלטת נציבות האיחוד האירופי לחדש את ההכרה במדינת ישראל כמדינה שרמת ההגנה בה על מידע אישי תואמת את רמת ההגנה באיחוד האירופי. מדובר בצעד משמעותי לאחר תהליך רב שנים בהובלת משרד המשפטים, ובהחלטה חשובה עבור מדינת ישראל בהיבטי כלכלה, מסחר, יחסי חוץ והקשרים עם האיחוד האירופי. שימור מעמד התאימות מסייע לחברות ישראלית רבות הפועלות באיחוד האירופי בכך שהוא מקל על העברת מידע מגופים באירופה לישראל".

הבחינה המחודשת של ההכרה שניתנה למדינת ישראל ולמדינות נוספות, החלה לפני מספר שנים בעקבות שינוי פנימי בדיני הגנת הפרטיות באיחוד האירופי וחקיקתן של תקנות ה- GDPR (General Data Protection Regulations), בהתאם לאמות מידה חדשות שנקבעו בהן. בהחלטתה המקצועית היום, אישרה נציבות האיחוד האירופי את המשך תוקפו של מעמד התאימות של ישראל לצד כלל 11 המדינות שזכו למעמד בטרם חקיקת תקנות ה-GDPR.

ההחלטה ניתנה בעקבות תהליך בחינה מקצועי מקיף של נציבות האיחוד האירופי שנמשך מספר שנים, ומטעם ישראל נעשה בהובלת המחלקה החוקתית בייעוץ וחקיקה יחד עם הרשות להגנת הפרטיות ומשרדי ממשלה נוספים. תהליך זה כלל הצגה מפורטת של משטר הגנת הפרטיות בישראל לרבות עמידה על ייחודיות המאפיינים השונים בשיטת המשפט הישראלית, וביצוע מהלכים משלימים בקשר לזכות לפרטיות, בין היתר התקנת תקנות, קבלת החלטת הממשלה בעניין עצמאותה של הרשות להגנת הפרטיות ופרסום הנחיות של הרשות.

מצ"ב ההחלטה (עמ' 12):

https://commission.europa.eu/system/files/2024-01/JUST_template_comingsoon_Report%20on%20the%20first%20review%20of%20the%20functioning.pdf

כל הזכויות שמורות © dpc.org.il

יצירה ויישום של מדיניות הגנה על הפרטיות

מדיניות הגנה על הפרטיות הוא המסמך העיקרי של הארגון אשר מתווה קווים מנחים ונהלים המבטיחים הגנה על מידע ונכסים רגישים.

כתיבת מדיניות פרטיות חיונית מכמה סיבות:

ציות לחוק ולתקנות: תחומי שיפוט רבים דורשים מארגונים לקיים מדיניות פרטיות כדי לציית לחוקי הגנת המידע והפרטיות. אי עמידה בתקנות אלה עלולה לגרור השלכות משפטיות וקנסות. יתר על כן, אם הארגון אוסף מידע רגיש, כגון פרטים פיננסיים או רשומות רפואיות, מדיניות פרטיות היא חיונית כדי להבטיח למשתמשים שהנתונים הרגישים שלהם מטופלים בזהירות מרבית ובהתאם לתקנות הרלוונטיות.

שקיפות והעצמה: מדיניות פרטיות היא דרך לתקשר למשתמשים כיצד המידע האישי שלהם נאסף, מעובד ומוגן. הפגנת מחויבות לפרטיות בונה אמון עם המשתמשים ולקוחות החברה. מדיניות פרטיות מנוסחת היטב אף מעצימה את המשתמשים בכך שהיא מיידעת אותם לגבי זכויותיהם בנוגע לאיסוף, שימוש ושיתוף של המידע האישי שלהם, ובכך מאפשרת להם לקבל החלטות מושכלות אם לשתף את המידע שלהם.

פעילות בינלאומית: אם הארגון פועל בזירה הבינלאומית או מעבד נתונים ממשתמשים במדינות שונות (ראה "תקנות הגישור"), מדיניות פרטיות מסייעת לנווט במורכבויות של חוקים שונים להגנה על נתונים ומבטיחה תאימות בקנה מידה עולמי.

כדי ליצור מדיניות פרטיות חזקה, מומלץ להתחיל בביצוע ביקורת יסודית של הנתונים אשר הארגון אוסף, מעבד ומאחסן. המדיניות צריכה להיות מנוסחת בשפה פשוטה ונהירה לכל קורא, לפרט אילו סוגים של מידע אישי נאספים, את המטרות להן הוא משמש וכיצד הוא מוגן.

בשל מורכבות החוקים והתקנות הנוגעים לדבר, מומלץ ליצור קשר עם בעלי עניין מרכזיים, כולל יועצים משפטיים ואנשי אבטחת מידע, כדי להבטיח דיוק ושלמות. חיוני לערב את צוותי אבטחת המידע כדי לטפל בהיבטים הטכניים של הגנה על מידע. המדיניות צריכה גם להגדיר בבירור את זכויות המשתמשים בנוגע לנתונים שלהם, כולל היכולת לגשת, לתקן או לבקש למחוק את המידע שלהם.

את המדיניות יש להנגיש הן למשתמשים והן לעובדי הארגון. הדרכות תקופתיות הן דרך יעילה לחזק את מודעות העובדים ולתעד את יישום החוק והתקנות. בהתאם לרמת האבטחה של מאגרי המידע, יש לבצע גם בדיקות תקופתיות כדי לוודא התאמה לשינויים בשיטות עסקיות, לדרישות משפטיות חדשות או עדכונים בטכנולוגיה.

לבסוף, יש לקבוע מנגנונים לטיפול בפניות או תלונות הקשורות לחששות בנוגע לפרטיות. על ידי שילוב אלמנטים אלה במדיניות הפרטיות וטיפוח תרבות של מודעות לפרטיות בתוך הארגון, ניתן לבנות אמון עם המשתמשים ולהפגין מחויבות לשמירה על המידע האישי שלהם.

לסיכום, מדיניות פרטיות היא כלי חיוני לציות לחוק, שקיפות וביסוס אמון עם המשתמשים, ובסופו של דבר תורמת למערכת יחסים חיובית בין הארגון לקהל שלו.

כל הזכויות שמורות © dpc.org.il

תפקיד ממונה הגנה על הפרטיות

הרשות להגנת הפרטיות כבר הביעה את עמדתה כי מינויו של ממונה על הגנת הפרטיות ("הממונה") באופן וולונטארי מהווה פרקטיקה ראויה ומומלצת לארגונים האוספים ומעבדים מידע אישי. חוק האיחוד האירופי GDPR אף מטיל חובת מינוי DATA PRIVACY OFFICER המפורטות בה, וחברות ישראליות רבות, המנהלות עסקים עם האיחוד האירופי, אכן מינו DPO.

ממונה הגנה על הפרטיות הוא הגורם מופקד על קידום הזכות לפרטיות ועל יישום דיני ההגנה על מידע אישי בארגון. תפקידו המרכזי הוא להביא להפנמה של עקרונות ושיקולי פרטיות בתהליכי העבודה בארגון, ולסייע לארגון במימוש אחריותו וחובותיו לפי דיני הגנת הפרטיות.

הרשות אף סבורה כי על הממונה להיות חלק מההנהלה הבכירה של הארגון, או לכל הפחות לדווח ישירות להנהלה הבכירה, על מנת שעמדתו הבכירה תאפשר לו להשפיע באופן יעיל ומשמעותי על התהליכים המרכזיים בארגון.

היקף תפקידו של הממונה בארגון ייקבע על פי מורכבות פעולות עיבוד המידע האישי שמתבצעות בארגון וגודלו. בין היתר הוא אמון על הסדרת תהליכי ניהול מידע בארגון באמצעות ניסוח מדיניות הפרטיות של הארגון ואישורה על ידי ההנהלה הבכירה. כמו כן, הממונה יהיה מעורב לאורך כל מחזור החיים של תהליכי עיבוד המידע בארגון, על מנת לוודא שהם מבוצעים באופן המפחית ככל הניתן את הסיכונים לפרטיות לקוחות הארגון.

חשובה במיוחד מעורבותו בעיצוב מערכות המידע של הארגון ובתהליכים הקשורים בהן, על מנת לוודא, ככל הניתן מראש, כי מערכות המידע בנויות באופן שיפחית את הסיכון לפגיעה בפרטיותם של נושאי המידע בהתבסס על תפיסת "עיצוב לפרטיות" Privacy By Design. לבסוף, הממונה הוא הגורם אשר אמור לטפל בתלונות הנוגעות לעיבוד מידע אישי ולזכות לפרטיות, ובפניות של לקוחות הארגון לרבות בקשות לעיון במידע או לתיקונו.

מטבע הדברים, מומלץ כי כישוריו של הממונה יהיו מגוונים ורחבים על מנת שתהיה לו הבנה מיטבית של התהליכים בארגון ברמה הטכנולוגית והעסקית, לצד יכולת לבחון את התאמתם לדרישות החוק ולמדיניות הארגון. במיוחד, ככל שליבת העיסוק של הארגון כרוכה בעיבוד מידע אישי ומידע רגיש, נדרשת מידת הבנה רבה יותר בתחום אבטחת המידע וטכנולוגיות המידע.

קריאה מומלצת:

ממונה הגנת פרטיות – **DPO**גילוי דעת מאת הרשות להגנת הפרטיות

כל הזכויות שמורות © dpc.org.il

הגנת הפרטיות בעולם

קשה לדבר על חוק הפרטיות הישראלי, ללא התייחסות למקבילותיו הזרות, אשר מחלקן הוא שואב השראה. כמו כן, אנו נמצאים בעידן בו מידע חוצה גבולות בין מדינות, אף במרחב הוירטואלי. כיבוד חוקי פרטיות המידע הבינלאומיים מבטיח כי חברות ישראליות ישמרו על סטנדרטים אתיים ומשפטיים באינטראקציות שלהם עם שותפים גלובליים. יתר על כן, הרשות נוטה לפרש את החוק הישראלי בקריצה אל החוק הזר, ובמיוחד זה של האיחוד האירופי, מתוך הצורך בשמירה על מעמד התאימות של ישראל.
קצרה היריעה מלהרחיב על חוקי הפרטיות בעולם כולו ולכן נעסוק כאן בשני הגופים העיקריים להם יש חוקי הגנת פרטיות הרלוונטים לעסקים ישראלים – האיחוד האירופי וארה״ב.

האיחוד האירופי

התקנה הכללית להגנה על מידע (GDPR) היא חוק של האיחוד האירופי שנכנס לתוקף בשנת 2016, ולאחר תקופת מעבר של שנתיים, הפך לחוק החל ישירות בכל המדינות החברות באיחוד האירופי, מבלי לדרוש יישום על ידי המדינות החברות באיחוד באמצעות החוק הלאומי.
התקנה (בניגוד לדירקטיבה שאותה החליפה) חלה ישירות על כל מדינות האיחוד ויש לה השפעה זהה בכל איזורי השיפוט. עם זאת, נותרו תחומים רבים המכוסים על ידי GDPR שבהם המדינות החברות רשאיות לחוקק באופן שונה בחוקי הגנת המידע המקומיים שלהן, ועדיין יש מקום לפרשנויות ושיטות אכיפה שונות בקרב המדינות החברות.

תקנות GDPR הן בעלות תחולה טריטוריאלית אולם יש להן גם השפעה חוץ-טריטוריאלית. חברה שהוקמה מחוץ לאיחוד האירופי עדיין תהיה כפופה להוראות הGDPR אם היא אוספת או מעבדת בצורה כלשהי מידע אישי של אינדיבידואלים הנמצאים באיחוד (ראה ״תקנות הגישור״). לדוגמה, עיבוד מידע יכול להיות גם עצם האיחסון בשרתים הממוקמים במדינות האיחוד.

תקנות הגנת הפרטיות האירופאיות – טקסט מלא

ארה"ב

הגנת הפרטיות בארצות הברית היא מלאכת טלאים מורכבת של חוקים ותקנות פרטיות לאומיים, מדינתיים ומקומיים. בארה״ב יש מספר חוקי פרטיות ואבטחת מידע ספציפיים למגזר עסקי ברמה הפדרלית, כמו גם חוקי פרטיות רבים יותר ברמה המדינתית (והמקומית). בשנים האחרונות החלו מדינות שונות, ובראשן קליפורניה, לחוקק חוקי פרטיות מקיפים משלהן, ומדינות אחרות צפויות לבוא בעקבותיהן. כאמור, אין עדיין חוק פרטיות לאומי מקיף בארצות הברית, למרות שטיוטת חוק דו-מפלגתית (״חוק הפרטיות וההגנה על המידע האמריקאי״) הוצגה בשנת 2022, אך מספר סנאטורים התנגדו להצעת החוק, וחוק פרטיות מקיף ברמה הפדרלית לא צפוי לעבור בקרוב.

החוקים העיקריים בארה״ב:

חוק פרטיות הצרכן של קליפורניה 2018 – CCPA
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

חוק זכויות הפרטיות של קליפורניה 2020 – CPRA
https://securiti.ai/what-is-california-privacy-rights-act-cpra/

כל הזכויות שמורות © dpc.org.il

נספח א - קישורים למידע נוסף

אתר הרשות להגנת הפרטיות

אתר הקהילה לאבטחת מידע והגנת הפרטיותDPC -

אתר כל זכות – הזכות לפרטיות

דיווח על אירוע אבטחה חמור – טופס דיגיטלי

מסמך הגדרות מאגר מידע – תבנית לדוגמא

מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו - מדריך לארגונים

תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017

https://www.nevo.co.il/law_html/law00/144811.htm

לומדת תקנות הגנת הפרטיות (אבטחת מידע)

https://content.justice.gov.il/Guides/Privacy/Takanot/story_html5.html

המדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע)

מדריך תקנות הגנת הפרטיות (אבטחת מידע) לעצמאים ולעסקים קטנים

https://www.gov.il/he/Departments/General/management_by_an_individual

תקנה 15 – מיקור חוץ

מדריך פעולה להתקשרות עם ספקי מיקור חוץ

הצטרפו אל הקהילה - https://dpc.org.il/join-community

עקבו אחרינו – לינקדאין

עקבו אחרינו – פייסבוק

כל הזכויות שמורות © dpc.org.il

נספח ב - קישורים לחוקים והתקנות העיקריים

חוק יסוד : כבוד האדם וחירותו
https://www.nevo.co.il/laws/#/5fc7492713c77a8af6294a42
חוק הגנת הפרטיות, תשמ"א1981-
https://www.nevo.co.il/law_html/law00/71631.htm
תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז2017-
https://www.nevo.co.il/law_html/law00/144811.htm
תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), תשפ"ג-2023
https://www.nevo.co.il/Handlers/LawOpenDoc.ashx?id=215876
תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001
https://www.nevo.co.il/Handlers/LawOpenDoc.ashx?id=71639
תקנות הגנת הפרטיות (קביעת מאגרי מידע הכוללים מידע שלא לגילוי), תשמ"ז-1987
https://www.nevo.co.il/Handlers/LawOpenDoc.ashx?id=71635
תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986
https://www.nevo.co.il/Handlers/LawOpenDoc.ashx?id=71634
תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), תשמ"א-1981
https://www.nevo.co.il/Handlers/LawOpenDoc.ashx?id=71632
תקנות העבירות המינהליות (קנס מינהלי - הגנת הפרטיות), תשס"ד-2004
https://www.nevo.co.il/Handlers/LawOpenDoc.ashx?id=73780
צו הגנת הפרטיות (הקמת יחידת פיקוח), תש"ס-1999
https://www.nevo.co.il/laws/#/603e5969315508eb66488927
צו הגנת הפרטיות (קביעת גופים ציבוריים), תשמ"ו-1986
https://www.nevo.co.il/laws/#/603d2405315508eb664882fa
צו הגנת הפרטיות (קביעת רשות חקירה), תשנ"ח-1998
https://www.nevo.co.il/laws/#/603e56b9315508eb664888fc
חוק המחשבים, תשנ"ה1995-
https://www.nevo.co.il/law_html/law00/72393.htm
חוק זכויות החולה תשנ"ו - 1996
https://www.nevo.co.il/Handlers/LawOpenDoc.ashx?id=71833

כל הזכויות שמורות © dpc.org.il