ISRAEL
TECH POLICY INSTITUTE

21 בדצמבר 2020

לכבוד
עו"ד איל זנדברג
ראש תחום משפט ציבורי
המחלקה למשפט ציבורי-חוקתי
אגף ייעוץ וחקיקה
משרד המשפטים

א.נ,

הנדון: מענה לקול קורא בנושא תיקון חוק הגנת הפרטיות, התשמ"א-1981

אנו מתכבדים להגיש את עמדת המכון הישראלי למדיניות טכנולוגיה לקול הקורא בנושא תיקון תזכיר **חוק הגנת הפרטיות, התשמ"א- 1981** (להלן - הקול קורא והחוק).

המכון הישראלי למדיניות טכנולוגיה (להלן - המכון) הוא מכון מדיניות וצוות חשיבה (Think Tank) הפועל לקידום עיצוב מדיניות בסוגיות חברתיות, אתיות ומשפטיות מורכבות בעידן הטכנולוגי. המכון מהווה פלטפורמה לכינוס קהילות וגיבוש שיח בין בעלי עניין שונים ובכלל זה גופי ממשל, תעשייה, אקדמיה וחברה אזרחית, לצורך גיבוש ניירות עמדה, מאמרים, וכללי התנהגות מוסכמים (Best Practices) בתחומי מדיניות טכנולוגיה, וקידום פרקטיקות אתיות מעשיות תוך קידום חדשנות.

המכון הוא שלוחה ישראלית של הפורום לעתיד הפרטיות בארה"ב Future of Privacy Forum ("FPF" או "הפורום"), מכון מחקר אמריקאי בעל שלוחה אירופאית, בתחום מדיניות הפרטיות וזכויות אדם. הפורום והמכון נתמכים על ידי מגוון רחב של חברות מהעולם ומישראל, העוסקות בתחומים שונים, כולל טכנולוגיה, אינטרנט, תקשורת, פיננסים, בריאות, קמעונאות, ועוד. בנוסף לחברות מן המגזר הפרטי, נתמך הפורום בידי קרנות מחקר ממשלתיות ופרטיות. לפורום והמכון ועדות מייעצות הכוללות נציגי חברה אזרחית ואקדמיה כמו גם נציגי תעשייה. למידע נוסף אודות המכון, מומחיו ותומכיו ראו אתר המכון באן.

מנהלת המכון היא עו"ד לימור שמרלינג מגזניק, אשר בין השנים 2009-2018 שימשה בתפקידים ניהוליים שונים ברשות למשפט, טכנולוגיה ומידע, ששמה היום הרשות להגנת הפרטיות ("הרשות"), והיתה אמונה, בין היתר, על ניהול מערך האכיפה המנהלית של רשם מאגרי המידע ועל תפעול פנקס מאגרי המידע.

העמדות המובעות בניירות העמדה של המכון משקפות את עמדות המכון ואינן מייצגות את עמדותיהם של תומכיו או של חברי הוועדה המייעצת.

המכון מברך על הפצת הקול קורא, כמו גם על הפצת תזכיר חוק הגנת הפרטיות (תיקון מס' 14) (הגדרות וצמצום חובת הרישום), התש"ף – 2020, ועל כוונת הממשלה לבצע תיקונים נוספים בחוק על מנת "להתאימו להתפתחויות הטכנולוגיות, החברתיות והמשקיות המפליגות שהתרחשו מאז נחקק".

המכון תומך בעדכון הדין הישראלי והתאמתו להגנה על זכויות הפרטיות של אזרחי ישראל ("נושאי מידע") במסגרת המציאות הטכנולוגית והעסקית של 2020. כמו כן, ישראל מקיימת קשרי סחר ענפים עם מדינות רבות בעולם, ולכן חשוב להתאים את הדין הישראלי למרקם הרגולטורי הבינלאומי. בעשור האחרון חברה ישראל בארגון המדינות המפותחות OECD, המתווה כללי מדיניות בתחום הגנת הפרטיות והמידע המקובלים על כל המדינות החברות בו, כולל ארה"ב ומדינות האיחוד האירופי. על ישראל להמשיך ליישם את עקרונות ה-OECD, שעודכנו לאחרונה ב-2013, המעניקים השראה לחוקים של המדינות החברות. כמו כן, על ישראל להטמיע את התובנות שנרכשו בעקבות יישומם של חוקי פרטיות והגנת מידע בעולם, כולל General Data Protection Regulation (להלן-GDPR) של האיחוד האירופאי וחוקי הגנת הפרטיות האמריקנים הפדרליים והמדינתיים (כגון CCPA ו-CPRA של קליפורניה), תוך שימת לב לרפורמות החוקיות שמדינות נוספות, כגון קנדה, ניו זילנד, אוסטרליה וסינגפור, מקדמות בחודשים האחרונים ממש.

רפורמות חוקיות אלה משקפות את תפיסותיהן וערכיהן הדמוקרטיים של כל מדינה ומדינה. כך גם ישראל תיישם במסגרת התיקונים לחוק את הכרתה בזכות לפרטיות כזכות יסוד חוקתית שאותה יש לאזן עם זכויות יסוד נוספות, כגון הזכות לחיים ולבריאות, הזכות לקניין, חופש הביטוי, חופש העיסוק, חופש התנועה ועוד. כמו כן, יש לוודא כי בהתאם לפסקת ההגבלה בחוק היסוד ישקפו התיקונים לחוק את מבחני המידתיות, למשל, באמצעות הטמעה של תפיסה של ניהול סיכונים המאפשרת איזון נקודתי ואפקטיבי בין זכויות ועקרונות מתחרים. תפיסה של ניהול סיכונים מעוגנת כבר בהנחיות ה-OECD, ב-GDPR ואף בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן-תקנות אבטחת מידע) החדשות בישראל.

זאת ועוד, כמדינה דמוקרטית בעלת תעשיות טכנולוגיות ומוסדות אקדמאיים מובילים, יכולה ישראל לשחק תפקיד מרכזי בעידוד התעשייה והמחקר המקומיים לפתח פתרונות טכנולוגיים להגנה על מידע לשם הבטחת הפרטיות תוך מתן אפשרות מיטבית לשימוש במידע למטרות מחקר ומטרות ציבוריות נוספות.

להלן יפורטו בהרחבה מספר נושאים.

קביעת בסיסים חוקיים נוספים לעיבוד מידע, מלבד הסכמה והסמכה

הדין הישראלי, מאפשר עיבוד מידע רק בהסכמתו של אדם. ואולם, בהעדר הצדקות חוקיות נוספות לעיבוד מידע, נוצר לחץ עז על ארגונים להכשיר פעולות שונות במידע בהסכמה, שהופכת כך לריקה מתוכן. הלכה למעשה, במקום שיעצים את נושאי המידע, מדלל הדגש על הסכמה את הביקורת הנורמטיבית על עיבוד מידע בידי ארגונים. אמנם, בסעיף 18 לחוק מפורטות הגנות, המצדיקות בדיעבד היבטים שונים של עיבוד מידע ללא הסכמה, וקובעות שאלה לא ייחשבו הפרה לצרכי תביעה אזרחית או פלילית. אך במקרים אלה מועבר הנטל על מעבד המידע להוכיח כי עומדת לו הגנה, בבחינת יוכיח המפר לאחר ההפרה כי זאת הייתה מוצדקת. זאת אינה דרך המלך לשימוש חוקי במידע המתבקש בחברה ובכלכלה דיגיטלית.

הדין המשווה כולל מנגנונים שמטרתם להגן על זכויות נושאי המידע ובה בעת לאפשר זרימה ותנועה חופשית של מידע בין ארגונים ואף בין מדינות. ה-GDPR, למשל, קובעת מספר בסיסים לעיבוד חוקי של מידע, ולצדם חובות ומנגנוני אחריותיות שבהם חבים מנהלי המידע, זכויות לנושאי המידע, וסמכויות אכיפה על ידי רגולטורים. בארה"ב, לעומת זאת, מותרת כל פעולה במידע שאינה גורמת לנשואי מידע נזק, ואילו במקרים מסוימים, הנתפסים כמעוררי סיכון, כגון סוגי מידע רגיש במיוחד או שינוי בדיעבד של נהלי פרטיות, נדרשת הסכמה מפורשת של נושאי המידע.

מדינות אחרות נוקטות בגישות ביניים, בין הגישה האירופית הדורשת הצדקה חוקית לעיבוד מידע לבין הגישה האמריקנית המתירנית יותר. כך למשל, קובע החוק החדש בניו זילנד עקרון של "עיבוד מידע חוקי" מבלי לפרט בסיסים חוקיים לעיבוד מידע. החוק דורש הסכמה לפעולות מסוימות בעלות רמת סיכון גבוהה, כגון העברות מידע או עיבוד מידע רגיש, בהעדר חובה חוקית.[1] מומלץ ללמוד בהקשר זה גם מתיקוני החקיקה שנעשו לאחרונה בסינגפור.[2]

אנו סבורים עוד, כי יש לאפשר שיתוף מידע למטרות מחקר לתועלת הציבור בכפוף לפיקוח והטמעה של מנגנוני הגנה. זאת, למשל באמצעות הקמתן של ועדות אתיקה למחקר שיידרשו לבצע הערכת סיכונים ונחיצות ולאשר שימושים במידע, בכפוף לשילוב אמצעים טכנולוגיים כגון התממה או הצפנה.

שיפור והרחבה של זכויות נושאי המידע

עקרונות ה-OECD ודיני הגנת המידע כמעט בכל מדינות העולם מכירים כיום בשורת זכויות של נושאי מידע, כולל זכות ליידוע, עיון ותיקון, זכות למחיקת מידע, זכות להגביל עיבוד מידע אישי, זכות לניוד המידע בין ספקי שירות (portability), זכות להתנגד לעיבוד מידע וזכויות ביחס לקבלת החלטות אוטומטיות בעניינו של אדם ויצירת פרופיל אודותיו. מומלץ שזכויות אלה יעוגנו גם בחוק הישראלי, תוך שמירה על אינטרסים עסקיים מקובלים (למשל, סודיות מסחרית) ועל אבטחת מידע (למשל, באמצעות אימות זהות נושאי מידע הדורשים גישה). עוד מוצע לקבוע כללים מעשיים להגנה על זכויותיהם של נושאי מידע מפני החלטות המתקבלות באמצעות אלגוריתמים וכלי בינה מלאכותית, בעיקר במגזר הציבורי ובענפים בעלי השלכות משפטיות משמעותיות כגון אשראי, ביטוח, דיור ועבודה.[3]

קביעת חובות נוספות על בעלים של מאגרי מידע ומחזיקים במאגרי מידע, לרבות מתחום האחריותיות (accountability)

עקרון האחריותיות (accountability) נקבע לראשונה בשנות ה-80 בכללי ה-OECD ומהווה מאז אבן יסוד בדיני הגנת מידע ברחבי העולם. עקרון זה, שראוי שיעוגן גם בחוק הישראלי, דורש כי ארגונים יטמיעו מנגנונים מנהליים, טכנולוגיים ומשאבי אנוש לשם יישום דיני הגנת הפרטיות. כך, למשל, נהוג לדרוש כי ארגונים ימנו עובד האחראי על יישום דיני הגנת הפרטיות בארגון. ארגונים רבים בעולם הן במגזר הציבורי והן במגזר הפרטי מינו לשם כך קציני ציות לפרטיות (Chief Privacy Officer או Data Protection Officer). כמו כן, יש לדרוש מארגונים לערוך במקרים מתאימים הערכות סיכון (risk assessments) כולל Data protection impact assessment לפעילויות עיבוד מידע בסיכון גבוה.

עיגון בחוק של עקרונות לעיבוד מידע

אנו סבורים שהחוק צריך לעגן את עקרונות הגנת הפרטיות של ה-OECD, הכוללים מגבלות על איסוף מידע; חובת שמירה על איכות המידע; השתתפות הפרט בקבלת החלטות לגבי מידע; צמידות המטרה; הגבלת שימושים; אבטחת מידע; שקיפות ואחריותיות.[4] כמו כן, מומלץ להטמיע את עקרונות האיחוד האירופאי המפורטים בהנחיית התאימות האירופית מ-2018.[5] זאת, מאחר שעקרונות אלה משקפים את עקרונות ה- OECD המקובלים ממילא בישראל וכן נדרשים לצורך הבטחת המשך ההכרה בישראל על ידי האיחוד האירופי כמדינה בעלת הגנה הולמת.

---

[1] A Deep Dive into New Zealand's New Privacy Law: Extraterritorial Effect, Cross-Border Data Transfers Restrictions and New Powers of the Privacy Commissioner, December 8th, 2020, Dr. Gabriela Zanfir-Fortuna, FPF

[2] Singapore's Personal Data Protection Act Shifts Away from a Consent-Centric Framework, November 18, 2020, Dr. Gabriela Zanfir-Fortuna, FPF

[3] Bridging the Gaps: A path forward to federal privacy legislation, Cameron F. Kerry, John B. Morris, Jr., Caitlin T. Chin, and Nicol E. Turner Lee, June 2020, Governance Studies at Brookings, Part III

[4] The **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**, [2013], OECD

[5] Adequacy Referential, 6 February 2018, (18/EN), Article 29 Working Party

הרחבה של סמכויות הפיקוח והאכיפה של הרשות להגנת הפרטיות

אנו סבורים שיש להסמיך את הרשות לגבש ולפרסם הנחיות ביצוע מעשיות-המבהירות לארגונים כיצד הרגולטור מצפה מהם לממש את עקרונות החוק. הניסיון בעולם מלמד, כי לא פשוט ליישם את עקרונות הגנת הפרטיות בסקטורים שונים ובהקשרים עסקיים פרקטיים. הנחיות מפורטות מקדמות ציות מהותי והגנה אפקטיבית על הפרטיות, והן כלי נפוץ ברשויות הגנת הפרטיות ברחבי העולם. כמו כן, יש לשקול תשתית ליצירת כללי התנהגות מקובלים (code of practice) או מערכי הסמכה (certification) שיאפשרו הטמעה ארגונית של עקרונות הגנת הפרטיות ובדיקתה בעזרת מבקרים חיצוניים.

התייחסות פרטנית לאוכלוסיות מיוחדות

אנו סבורים כי יש מקום לספק הגנה מיוחדת לאוכלוסיות בסיכון כגון קטינים. בהקשר זה, מדינות שונות בעולם קבעו מגוון מנגנונים להגנה על זכויותיהם של קטינים, כולל לא רק כלים משפטיים אלא גם חינוך לציבור.

נושאים נוספים:

- הגם שתיקון 14 המוצע מגדיר מחדש "מידע" ו"מידע רגיש", יש מקום ליישב בין הגדרת "מידע" החדשה לבין המונח הרווח בסעיף 2 לחוק, "ידיעות על ענייניו הפרטיים של אדם";

- יש ליישב בין הנחיצות והגדרות התפקיד של "מנהל המאגר" ו"קצין הגנת הפרטיות" ככל שיוחלט להחיל חובת מינוי של האחרון;

- פרק הדיווח הישיר מיושן ולא ברור. הוא כולל התייחסות למדבקות ולדפוס אשר כבר אינם עיקר הפעילות העסקית בתחום זה, וההבדל בין דיווח ישיר לבין שירותי דיווח ישיר והדין החל לגביהם ראוי להבהרה בחקיקה ראשית;

- מוצע להתאים את תקנות הגנת הפרטיות (העברות מידע לחו"ל) לעקרונות ה-OECD אשר שמים דגש על רמת האחריותיות של מקבל המידע. יש לאפשר העברות מידע לחו"ל בכפוף להערכת סיכונים ומנגנוני הגנה מתאימים;

- יש לקבוע בחוק או בחקיקה נפרדת חריגים והסדרים ברורים לגבי סמכויות של גורמי אכיפת חוק ושירותי הביטחון לעשות שימוש במידע לצרכי משימותיהם. על ההסדרים לכלול גבולות שימוש במידע ואמצעי פיקוח אפקטיביים על הרשויות. זאת הן לטובת ההגנה על פרטיותו של הציבור הישראלי והן לטובת שימור מעמדה של ישראל כמדינה שדיניה תואמים את ה-GDPR;

- יש להכיר בפסאודונימיזציה חזקה ככלי המאפשר שימושים במידע לצרכים לגיטימיים ובכפוף לביצוע הערכת סיכונים והטמעה של מנגנוני הגנה ארגוניים נוספים (ראו החוק היפני[6]). זאת, מתוך הכרה כי אנונימיזציה מוחלטת אינה אפשרית וכי החלה של מלוא הסדרי החוק על מידע מותמם או פסאודונימי יוצרת קשיים פרקטיים ומתמרצת ארגונים שלא לטרוח להתמים מידע;

[6] Amended Act on the Protection of Personal Information (Tentative Translation)

- יש לאמץ עקרונות עיצוב לפרטיות (Privacy by Design) ולתמרץ שימוש בכלים טכנולוגיים משפרי הגנת פרטיות (Privacy Enhancing Technologies), באופן המאפשר שימוש במידע תוך הקטנת סיכונים. כך יתאפשרו שימושים במידע במסגרות טכנולוגיות המצמצמות את הסיכונים מפני פגיעה בזכויותיהם של אנשים יחד עם מתן היכולת להפיק תועלות חברתיות ובלכליות מהשימוש במידע. הברה זאת תתמוך גם בשוק המתפתח של חברות טכנולוגיה ישראליות העוסקות בפיתוח מגוון מוצרים בקטגוריה הזו לרבות:

privacy program management, de-identification, secure communications, synthetic data, .homomorphic encryption, multi-party computation, active monitoring, data mapping and discovery

נשמח להשתתף בתהליך החשיבה והפיתוח של תיקוני חקיקה חשובים אלו.

בכבוד רב ובברכה,

עו"ד לימור שמרלינג מגזניק
מנהלת המכון

העתק:
ד"ר שלומית וגמן, ראשת הרשות להגנת הפרטיות
עו"ד ראובן אידלמן, היועץ המשפטי, הרשות להגנת הפרטיות