

תסקיר השפעה על פרטיות עדכון לקוחות - מחלקת הייטק וטכנולוגיה – אוגוסט 2021

לקוחות יקרים,

ביום 1.8.2021, פרסמה הרשות להגנת הפרטיות ("הרשות") טיוטת מדריך עזר מתודולוגי לעריכת תסקיר השפעה על פרטיות ("המדריך"), שמטרתו (אם ולכשיפורסם כמסמך סופי) לפרט את המלצות הרשות ביחס לביצוע התסקיר כאמור ("התסקיר") ולהחליף מסמך קודם בנושא שפרסמה הרשות בשנת 2015.

טיוטת המדריך, כוללת, בין היתר, פירוט אודות היתרונות שרואה הרשות בביצוע התסקיר, פירוט ביחס לזמן בו נכון לדעת הרשות לערוך את התסקיר, פירוט אודות שלבי המפתח בביצוע התסקיר ופירוט הגורמים שנכון שיקחו חלק בעריכת התסקיר.

לפי פרסום הרשות, המדריך עתיד להיות חלק מסדרת כלים פרקטיים שהרשות תפרסם במסגרת פעולותיה לקידום גישת "אחריותיות לפרטיות" (accountability) בארגונים במשק, ועתיד להצטרף למסמך ההמלצות שפורסם להערות הציבור בנושא מינוי ממונה הגנה על הפרטיות (עליו העיר משרדנו בשיתוף עם גורמים אחרים. ראו מזכרנו בנושא שפורסם ביום 30.11.2020 הזמין לצפייה [באן](#)).

ניתן להעביר לרשות התייחסות לטיוטת המדריך עד ליום ה- 30.9.2021, ואנו נשמח לעמוד לרשותכם לצורך כך וכן על מנת לסייע לארגונכם לעמוד בהוראות דיני הגנת הפרטיות ואבטחת המידע החלים עליו.

להלן נפרט את עיקרי טיוטת המדריך.

בדין הישראלי אין כיום חובה כללית לבצע תסקיר השפעה על פרטיות (המכונה גם Privacy Impact Assessment או Data Protection Impact Assessment), וזאת בניגוד לתחומי שיפוט אחרים (למשל לפי ה- 27 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 and on the free movement of such data ("GDPR"), שם נדרש ביצוע תסקיר בנסיבות מסוימות).

יחד עם זאת, הרשות מוצאת לנכון להציע לציבור את המדריך (אם ולכשיפורסם כמסמך סופי) על מנת לסייע לארגונים בהם נעשה שימוש בטכנולוגיות המשלבות איסוף מידע אישי, להעריך ולמצמם את הסיכונים הכרוכים בתחום הגנת הפרטיות.

מועד ביצוע התזכיר - על פי עמדת הרשות נכון לבצע את התסקיר בשלבים המוקדמים של פרויקט הכרוך בעיבוד של מידע, במקביל לתהליך התכנון והפיתוח של המערכת/הפעילות הרלבנטית, ולפני שהחלו פעולות העיבוד. לאחר אישור התסקיר, יש לשלב את תוצאותיו ומסקנותיו בתכנון הפרויקט או הפעילות הרלבנטית, ולבצע מעקב שוטף אחר מימושו במסגרת תכנית העבודה.

שליבים בביצוע התסקיר. המדריך מונה 7 שלבים עיקריים בביצוע התסקיר –

- 1) קבלת החלטה על ביצוע תסקיר השפעה על הפרטיות. על פי עמדת הרשות נכון לבצע את התסקיר לפני כל שימוש במידע אישי העלול לגרום לסיכון מהותי לפרטיות נושאי המידע, או לשינוי מהותי בזכויותיהם, במיוחד בעת הטמעת טכנולוגיות מידע חדשות, או עיבוד של מידע אישי בהיקף גדול או של מידע בעל רגישות מיוחדת (אם בשל תוכנו או בשל זהות נושאי המידע).
- 2) תיאור פעילויות עיבוד המידע. על פי עמדת הרשות על התסקיר לכלול פרטים על אופי עיבוד המידע, היקף עיבוד המידע, הקשר עיבוד המידע, ומטרות עיבוד המידע.
- 3) התייעצות עם נושאי המידע ועם בעלי עניין נוספים. על פי עמדת הרשות יש לקיים היוועצות עם נושאי המידע ועם כל הגורמים העשויים להיות מושפעים מהפרויקט המתוכנן (למשל עובדים ככל שהמערכת רלבנטית למאגר/י המידע הנוגעים לעובדי הארגון).
- 4) הערכת החוקיות והמידתיות של פעולות עיבוד המידע. בשלב זה נדרש הארגון לפי עמדת הרשות לבחון את הבסיס החוקי לעיבוד ומתן הגישה למידע. כן הארגון נדרש לבחון את מדתיות הפעולות שהוא עתיד לבצע ולבדוק תחולה ספציפית של דינים שונים לפי המקרה¹.
- 5) זיהוי והערכת סיכונים לפגיעה בפרטיות. על פי עמדת הרשות במסגרת שלב זה יש לבחון את ההשפעה הפוטנציאלית על נושאי המידע וכל פגיעה או נזק שעלולים להיגרם להם כתוצאה מעיבוד המידע, כתוצאה מפגיעה באבטחת המידע² או מהפרה של הוראות אחרות של רגולציות הרלבנטיות להגנת המידע. בשלב זה יש לבצע (א) הערכה של סיכוני האבטחה ושל סיכונים אחרים לפרטיות; ו- (ב) מיפוי גורמי האיום/מקורות הסיכון, וההשפעה הפוטנציאלית של התממשות כל מהם.
- 6) זיהוי אמצעים לצמצום הסיכונים שאותרו. ביחס לסיכונים/איומים שאותרו, עמדת הרשות היא שיש לזהות ולתעד את מקורם, ולשקול חלופות לצמצום הסיכון/איום והפחתתו (למשל על ידי החלטה שלא לאסוף את המידע, לצמצם את פעולות העיבוד שנעשות במידע או את בעלי ההרשאה לגשת אליו) ("בקורות מתקנות")³.
- 7) תיקוף ואישור התסקיר. לאחר הטמעת הבקורות המתקנות, יובא התסקיר לאישור הגורם המוסמך בארגון⁴. במידה שמסקנות התסקיר הן שהפעילות מקיימת את הוראות הדין, וכן עומדות בדרישת המידתיות (במקרים מתאימים), ישלב הארגון את תוצאות ומסקנות התסקיר בתוכנית העבודה שלו, תוך קביעת גורם אחראי ליישום האמור בתסקיר וקביעת לוחות זמנים לנושא. לאחר מכן, יש לשוב ולתקף מחדש את התסקיר בהיבטי עיבוד המידע, וזאת על בסיס קבוע, או בעת ביצוע שינויים מהותיים בפרויקט, או במערכות התומכות בו.

1. לדוגמה קיום הוראות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א – 2001 (ככל שמתבצעת העברת מידע מחוץ לישראל), קיום הנחיות סקטוריאליות של רגולטורים ספציפיים (דוגמת משרד הבריאות, הפיקוח על הבנקים, רשות שוק ההון, ביטוח וחשבון) ועוד.
2. "אבטחת מידע", כהגדרתה בסעיף 7 לחוק הגנת הפרטיות, תשמ"א-1981 ("חוק הגנת הפרטיות"), היא "הגנה על שלמות המידע או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדיו".
3. ארגון אשר אינו בטוח האם הסיכון שנתר לאחר מימוש הבקורות המתקנות, מקיים את הוראות חוק הגנת הפרטיות – רשאי לפנות לרשות להגנת הפרטיות בבקשה לקבלת חוות דעת מקדמית.
4. לפי המדריך – הדירקטוריון או חברי הנהלה בכירים.

הגורם שנכון שיבצע את התסקיר. עמדת הרשות היא שניתן לבצע את התסקיר על ידי גורמים פנימיים- תוך ארגוניים, או על ידי יועץ חיצוני, בעלי הכשרה מתאימה לביצוע תהליך מסוג זה, **ובליווי של יעוץ משפטי**. אם קיים בארגון ממונה הגנת פרטיות (Data Protection Officer או Chief Privacy Officer)⁵, ראוי שהתסקיר יערך בניהולו ובאחריותו, או לכל הפחות תוך מעורבות משמעותית שלו.

לקריאת טיוטת המדריך המלאה לחץ [כאן](#).

נשמח לסייע לארגונכם לסייע לכם להגיב לטיטות המדריך ולוודא עמידה בהוראות הגנת הפרטיות ואבטחת המידע החלות עליו.

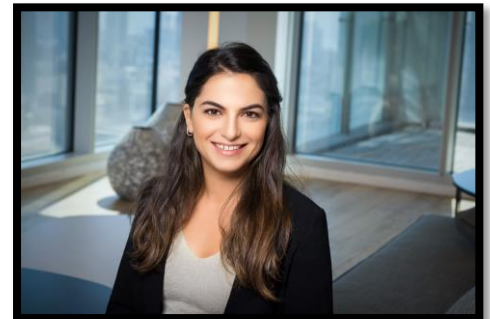
עו"ד אסנת סרוסי פירסטטר
ראש מחלקת הייטק וטכנולוגיה
osnat@agmon-law.co.il
03-6078607



עו"ד סער רוסמן
שותף, מחלקת הייטק וטכנולוגיה
saar@agmon-law.co.il
03-6078607



עו"ד אורן שטרית
מחלקת הייטק וטכנולוגיה
oransh@agmon-law.co.il
03-6078607



המידע האמור לעיל הינו מידע כללי ותמציתי בלבד, הוא אינו מהווה חוות דעת או ייעוץ משפטי ויש לקבל עצה מקצועית נפרדת בטרם נקיטת פעולה משפטית או אחרת בקשר עם הנושאים אותם סקרנו

5. ראו את טיוטת המלצות הרשות להגנת הפרטיות בדבר מינוי ממונה הגנה על הפרטיות בארגון, האמור לעיל.