הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

תסקיר השפעה על פרטיות

מדריך עזר מתודולוגי

(DPIA – DATA PROTECTION IMPACT ASSESSMENT)

1. רקע

תסקיר השפעה על פרטיות (Privacy Impact Assessment), המכונה לעיתים תסקיר השפעה על הגנת מידע (Data Protection Impact Assessment) (להלן: "התסקיר") הוא תהליך אשר נועד לסייע לארגון באיתור, הערכה וניהול של סיכונים לפרטיות בפרויקטים או פעילויות עסקיות וארגוניות אחרות הכוללות עיבוד של מידע אישי.[1]

מדריך זה מפרט המלצות לאופן ביצוע התסקיר.[2] באין חובה כללית כיום בדין הישראלי לעריכת תסקיר השפעה על הפרטיות, הרי שגם מדריך זה אינו יוצר חובה לעריכתו (בהעדר מקור חובה ספציפי אחר) או בנוגע לאופן עריכתו, אלא נועד לשמש ככלי עזר עבור גורם המחליט לערוך תסקיר לצורך הערכה וניהול של הסיכונים לפרטיות.

1.1. שלבי המפתח בביצוע תסקיר השפעה על הפרטיות:

רצוי לבצע את התסקיר בשלבים המוקדמים של הנעת פרויקט הכרוך באיסוף או עיבוד של מידע, במקביל לתהליך התכנון והפיתוח של המערכת, ולפני שהחלו פעולות העיבוד. התסקיר יכלול את השלבים הבאים:

- שלב 1: קבלת החלטה על ביצוע תסקיר השפעה על הפרטיות.
- שלב 2: תיאור כללי של פעילויות עיבוד המידע.
- שלב 3: התייעצות עם בעלי עניין (ככל שרלוונטי).
- שלב 4: הערכת החוקיות, הצורך והמידתיות של פעולות עיבוד המידע.
- שלב 5: זיהוי והערכת סיכונים לפגיעה בפרטיות.
- שלב 6: זיהוי אמצעים לצמצום הסיכונים שאותרו.
- שלב 7: תיקוף ואישור התסקיר.

לאחר אישור התסקיר, יש לשלב את תוצאותיו ומסקנותיו בתכנון הפרויקט או הפעילות העסקית או הארגונית, ככל שאלו כוללים עיבוד של מידע אישי, ולבצע מעקב שוטף אחר מימושן במסגרת תכנית העבודה.

---

[1] להרחבה וחומר רקע ראו: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, המסמך זמין כאן. כן ראו תקן ISO/IEC 29143:2017 אשר מספק קווים מנחים לביצוע תסקירי השפעה על פרטיות, לרבות המבנה והתוכן של דוחות אלה (https://www.iso.org/standard/62289.html).

[2] המדריך הוא עיבוד של מסמך בנושא "How do we do a DPIA?" שפרסמה רשות הפרטיות הבריטית (Information Commissioner's Office), ואשר עבר עריכה והתאמה לדין הישראלי ולתנאי המשק הישראלי. המסמך של רשות הפרטיות הבריטית זמין כאן. כמו כן, מדריך זה מחליף מדריך קודם אשר פורסם על ידי הרשות להגנת הפרטיות בשנת 2015, בעניין תסקיר השפעה על הפרטיות.

התסקיר הוא תהליך גמיש (scalable), אשר ניתן לתכננו כך שיתאים לאופי הארגון, אופי הפרויקט ותהליכי ניהול הסיכונים הנהוגים בארגון, ובלבד שיכלול את שלבי המפתח המפורטים לעיל.

תסקיר אינו פרוצדורה חד-פעמית, אלא תהליך מתמשך. יש לעדכן ולתקף מחדש את התסקיר על בסיס קבוע, או בעת ביצוע שינויים מהותיים בפרויקט או במערכות התומכות בו, בהיבטי עיבוד המידע.

1.2. האחריות לביצוע תסקיר השפעה על הפרטיות ואישורו, ומעורבות הממונה על הגנת הפרטיות

ניתן לבצע תסקיר 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 (Chief Privacy Officer או Data Protection Officer)[3] ראוי שהתסקיר יערך בניהולו ובאחריותו, או לכל הפחות תוך מעורבות משמעותית שלו ובהתייעצות עמו בנושאים הבאים:

- האם קיים צורך בביצוע תסקיר;
- אופן ביצוע התסקיר;
- האם לבצע את התסקיר במיקור חוץ או בתוך הארגון;
- מהם האמצעים והבקרות אותם ניתן ליישם לצמצום סיכונים;
- האם התסקיר בוצע כראוי;
- תוצאות התסקיר והאם ניתן להתחיל בתהליך העיבוד;

את תהליך ההתייעצות עם הממונה רצוי לתעד. כמו כן, במידה שהתקבלה על ידי הארגון החלטה שלא לפעול בהתאם לעצתו, רצוי לתעד את השיקולים והנימוקים להחלטה זו.

את תוצאות התסקיר ומסקנותיו יש להביא לאישור הדירקטוריון או חברי ההנהלה הבכירה, בדרג ובפורום ההולמים את היקף הפרויקט, רגישותו ופוטנציאל הפגיעה בפרטיות הטמון בו.

כשפרויקט עיבוד מידע מבוצע במיקור חוץ, אין מניעה ולעיתים אף רצוי להטיל על הקבלן לערוך את התסקיר הנוגע אליו. עם זאת, גם במקרים אלו האחריות הסופית לביצוע התסקיר ולאישור תוצאותיו, מוטלת על בעל המאגר המזמין.

1.3. גורמים נוספים המעורבים בביצוע התסקיר

מומלץ לערב גם את הגורמים הבאים בעריכת התסקיר:

- מנהל הפרויקט.

[3] ראו המלצות הרשות להגנת הפרטיות בעניין מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו, הזמינות כאן.

- ממונה אבטחת המידע וצוות אבטחת המידע הארגוני.
- ממונה הגנת הפרטיות הארגוני (ככל שקיים בארגון).
- היועץ המשפטי של הארגון.
- מומחים בתחום התוכן של הפרויקט, וככל שרלוונטי גם מומחים בתחומי ידע אחרים שיסייעו בהערכת השפעת הפרויקט על נושאי המידע, כגון פסיכולוגיה, כלכלה התנהגותית או אתיקה.
- ספקי מיקור חוץ המעורבים בתהליך עיבוד המידע.

2. ביצוע תסקיר השפעה על הפרטיות

2.1. שלב 1: קבלת החלטה על ביצוע תסקיר השפעה על הפרטיות

עריכה מוקדמת של תסקיר, או של הליך מתודולוגי דומה, היא פרקטיקה מומלצת העולה בקנה אחד עם האינטרס העסקי והארגוני של יתר בעלי המאגרים במשק.

כמו כן, רבים מרכיבי התסקיר חופפים ממילא לדרישה הקיימת בתקנות 2 ו-5 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן – "**תקנות אבטחת מידע**"), המטילות על כל בעל מאגר מידע במשק להכין "מסמך הגדרות מאגר" ולערוך מיפוי של המערכות הטכנולוגיות המשמשות את המאגר.

מומלץ לבצע תסקיר לפני כל שימוש במידע אישי העלול לגרום לסיכון מהותי לפרטיות נושאי המידע, או לשינוי מהותי בזכויותיהם[4], במיוחד בעת הטמעת טכנולוגיות מידע חדשות, או עיבוד של מידע אישי בהיקף גדול או של מידע בעל רגישות מיוחדת, אם בשל תוכנו[5] או בשל זהות האוכלוסייה עליה הוא נסוב.[6] בכל מקרה של ספק בנוגע לנחיצות בביצוע תסקיר, מומלץ לבצעו.

2.2. שלב 2: תיאור פעילויות עיבוד המידע

על הארגון לתאר כיצד מתוכנן להתבצע השימוש במידע האישי ומדוע מתוכנן שימוש כאמור. על התיאור לכלול פרטים על אופי עיבוד המידע, היקף עיבוד המידע, הקשר עיבוד המידע, ומטרות העיבוד.

---

[4] להשוואה ראו סעיף 35 לרגולציית הגנת המידע האישי של האיחוד האירופי (GDPR), שהפך את ביצוע התסקיר לנורמה מחייבת הנדרשת מכל ארגון הכפוף ל-GDPR, בנסיבות המפורטות בסעיף זה. בין היתר, דורש ה-GDPR לבצע תסקיר במקרים הבאים: כאשר מתבצעת הערכה שיטתית של היבטים אישיים, מבוססת עיבוד אוטומטי, למשל על ידי יצירת פרופיל וקבלת החלטות לגבי נושאי מידע; כאשר נעשה עיבוד קטגוריות מיוחדות של מידע אישי, כגון מוצא אתני, גזעי, דעה פוליטית, דת, אמונה, חברות באיגוד, מידע גנטי, מידע ביומטרי, מידע בריאות, נטייה מינית; כאשר מתבצע מעקב שיטתי באזור ציבורי בהיקף רחב.

[5] למשל מידע רפואי, גנטי, ביומטרי, או מידע על צנעת חייו של אדם או דעותיו הפוליטיות, ושאר סוגי המידע המפורטים בפרט 3(1) לתוספת הראשונה בתקנות אבטחת מידע. ראו גם גילוי הדעת של הרשות להגנת הפרטיות "מהם "מידע" ו"ידיעה על ענייניו הפרטיים של אדם" בחוק הגנת הפרטיות", אשר פורסם להערות הציבור. גילוי הדעת זמין כאן.

[6] למשל קטינים, מטופלים במוסד רפואי, אנשים שנשללה כשרותם המשפטית.

❖ **<u>אופי העיבוד</u> - מה מתכנן הארגון לעשות עם המידע האישי. יש לבחון, בין היתר, את הנושאים הבאים:**

- האופן שבו המידע נאסף ובידי אילו גורמים בארגון;
- האופן שבו המידע מאוחסן;
- אופן השימוש במידע;
- למי יש גישה למידע בתוך הארגון ומחוץ לו;
- שיתוף המידע עם גורמים חיצוניים;
- עיבוד מידע באמצעות ספקי מיקור חוץ;
- פרק הזמן הנדרש או המתוכנן לשמירת המידע;
- אילו אמצעי אבטחה ייושמו לצורך הגנה על המידע;
- האם יבוצע שימוש בטכנולוגיה חדשה לצורך עיבוד המידע;
- האם העיבוד עצמו חדשני;
- מהו הקריטריון שהביא להחלטה על עריכת התסקיר (הסיכון הגבוה לפרטיות נושאי המידע);

❖ **<u>היקף העיבוד</u> – יש לבחון, בין היתר, את הנושאים הבאים:**

- סוג המידע האישי;
- כמות ומגוון מקורות המידע האישי;
- רגישות המידע האישי;
- המידה והתדירות בהן מבוצעות פעולות העיבוד;
- משך זמן העיבוד;
- כמות נושאי המידע המעורבים, והפיזור הגיאוגרפי שלהם;

❖ **<u>ההקשר הרחב של הנסיבות בהן מבוצעות פעולות העיבוד</u>, כולל גורמים פנימיים וחיצוניים נוספים אשר עשויים להשפיע על ציפיות הארגון ונושאי המידע ולהשליך על זכויותיהם. לעניין זה יש לבחון, בין היתר, את הנושאים הבאים:**

- מקורות המידע;
- טיב ומהות מערכת היחסים של הארגון עם נושאי המידע;
- באיזו מידה לנושאי המידע יש שליטה על המידע אודותיהם;
- עד כמה פעולות העיבוד המתוכננות עשויות להיכלל בציפיות הסבירות של נושאי המידע;

- האם עיבוד המידע כולל מידע על קטינים או קבוצות אוכלוסייה רגישות אחרות;
- ניסיון קודם בפעולת עיבוד מסוג זה, לרבות סיכונים או אתגרי אבטחה שיצר סוג העיבוד בעבר;
- התקדמות בתחום הטכנולוגיה או האבטחה הרלוונטיות לסוגי עיבוד כגון זה;
- האם עיבוד המידע מעלה סוגיות המצויות במחלוקת ציבורית או מעוררות עניין ציבורי מיוחד בקשר להגנה על פרטיות הציבור;
- האם חלות על הארגון חובות חוקיות או רגולטוריות נוספות הרלוונטיות לפעולת העיבוד;

❖ **<u>מטרת העיבוד</u> היא הסיבה לשמה מעוניין הארגון לבצע את פעולת עיבוד המידע הספציפית, או להשתמש בטכנולוגיה הקונקרטית. כאן יש לבחון, בין היתר:**

- מהי המטרה העסקית או הארגונית הכללית המבוקשת (יש להגדיר את המטרה באופן ממוקד ובמפורש);
- מהו התוצר או ההישג הקונקרטי המבוקש;
- מהי ההשפעה המצופה על נושאי המידע;

2.3. שלב 3: התייעצות עם נושאי המידע ועם בעלי עניין נוספים

היוועצות עם נושאי המידע ועם כל הגורמים העשויים להיות מושפעים מפרויקט המידע המתוכנן, הינה שלב חשוב בביצוע תסקיר השפעה על הפרטיות, אשר יכול לסייע בהערכת השפעות עיבוד המידע ובהתמודדות עם הסיכונים שיציב לפרטיות. כשהפרויקט מתוכנן בידי רשות ציבורית, רצוי לפרסם שימוע פומבי שיאפשר לציבור המושפע מהפרויקט להביע את עמדתו.[7] לכל הפחות מומלץ לפנות לנושאי מידע כגון לקוחות או עובדים,[8] או לנציגיהם, על מנת לאפשר להם לחוות את דעתם בנוגע לעיבוד המידע המתוכנן וכן לתעד את תגובתם, אלא אם לארגון ישנם טעמים כבדי משקל שלא לבצע את הליך ההיוועצות.
גם החלטה זו יש לתעד כחלק מהתסקיר בליווי הסבר. לדוגמה, פירוט הנימוקים שבעטיים ההיוועצות תפגע בסוד מסחרי, באבטחת המידע, או שהיא איננה מעשית.

[7] להשוואה ראו סעיף 3.1.1.2.4 להנחיית רשם מאגרי מידע מס' 4/2012 - שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן. ההנחיה זמינה כאן.

[8] ראו סעיף 20 וה"ש 20 להנחיית רשם מאגרי מידע מס' 5/17 - שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי עבודה. ההנחיה זמינה כאן.

אם התסקיר מתייחס לתכנית לאסוף מידע אישי על אנשים אשר טרם זוהו או שטרם נוצר איתם קשר, ניתן לקיים הליך התייעצות בעל אופי יותר כללי-ציבורי, או מחקר ממוקד, לדוגמא באמצעות מחקר-שוק בעל מאפיינים דמוגרפיים מסוימים, או לחלופין פנייה לקבוצות צרכנים לקבלת דעותיהם.

אם בסיכום ההיוועצות עם נושאי המידע החליט הארגון לפעול בניגוד לדעתם, יש לתעד את הסיבות לקבלת החלטה זו כחלק מביצוע התסקיר.[9]

התייעצות עם גורמים נוספים

יש לזהות את בעלי העניין הפנימיים הרלוונטיים, להתייעץ עמם בנוגע לפעילויות העיבוד המתוכננות ולתעד את עמדתם, לרבות השפעה על התהליכים שבתחום אחריותם.

ככל שעיבוד המידע מבוצע על ידי ספקים במיקור חוץ, יש לבחון בשלב זה האם נדרש סיוע מצדם בביצוע התסקיר. מומלץ להסדיר את חובות הספק בהקשר זה במסגרת ההתקשרות החוזית עמו.

2.4. שלב 4: הערכת החוקיות והמידתיות של פעולות עיבוד המידע

על הארגון לבחון את השאלות הבאות שהינן מהותיות לשם קביעת מידתיות ביצוע הפרויקט:

- האם עיבוד המידע המתוכנן משיג את המטרות שהארגון הציג לעצמו;
- האם קיימות דרכים נוספות להשגת התוצר הנדרש;

עוד נדרש הארגון לתאר כיצד בכוונתו להבטיח שעיבוד המידע המתוכנן יקיים את הוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן - "**חוק הגנת הפרטיות**") והתקנות שהותקנו מכוחו. זאת מפני שאחד האמצעים המרכזיים להבטיח כי דרישות המידתיות מתקיימות בעת איסוף ועיבוד המידע הוא ציות לחובות החוקיות החלות עליו[10]. יש לפרט, בין היתר:

- מהו הבסיס החוקי לעיבוד המידע (הסכמה או הסמכה בחוק);[11]
- כיצד ימנע הארגון שימוש במידע שלא למטרה שלשמה נמסר או נאסף;[12]
- אופן מסירת המידע הנוגע לפרטיות נושאי המידע;[13]
- כיצד בכוונת הארגון לאפשר ולתמוך בזכותם של נושאי המידע לעיין במידע על אודותיהם ולבקש לתקנו אם המידע אינו נכון, שלם, ברור ומעודכן;[14]

---

[9] להרחבה בנושא החשיבות שבהיוועצות עם הציבור הרלוונטי בעת איסוף או עיבוד מידע רגיש, או בעת איסוף או עיבוד היקף גדול של מידע, ראו סעיף 3.1.1.2.4 להנחיית רשם מאגרי המידע מס' 4/2012 – שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן. קישור להנחיה לעיל ה"ש 7.

[10] ראו שלב 4 במדריך התסקיר של רשות הפרטיות הבריטית (ה"ש 1 לעיל).

[11] סעיף 1 לחוק הגנת הפרטיות.

[12] סעיף 2(9) וסעיף 8(ב) לחוק הגנת הפרטיות.

[13] סעיף 11 לחוק הגנת הפרטיות.

[14] סעיף 13 וסעיף 14 לחוק הגנת הפרטיות.

- הדרך בה מתכוון הארגון לקיים את אחריותו לאבטחת המידע במאגר;[15]
- כיצד יבטיח הארגון שהמידע שהוא שומר איננו רב מן הנדרש למטרות המאגר;[16]
- כיצד הארגון מתכוון לקיים את החובות החלות עליו ביחסיו עם מחזיקים, ספקי מיקור חוץ וגורמים חיצוניים אחרים;[17]
- האם ביצוע עיבוד המידע כרוך במתן גישה למידע מחוץ לגבולות ישראל, וכיצד בכוונת הארגון לקיים את הוראות הדין בעניין העברת מידע מחוץ לגבולות המדינה;[18]
- האם חלה על הפרויקט המתוכנן חקיקה או רגולציה מגזרית נוספת בעניין הגנת מידע, פרטיות או סודיות (בנוסף לחוק הגנת הפרטיות והתקנות שהותקנו מכוחו) וכיצד בכוונת הארגון לקיים את הוראות הרגולציה הנוספת;

2.5. שלב 5: זיהוי והערכת סיכונים לפגיעה בפרטיות

יש לבחון את ההשפעה הפוטנציאלית על נושאי המידע וכל פגיעה או נזק שעלולים להיגרם להם כתוצאה מעיבוד המידע על ידי הארגון – בין אם גופני, נפשי או חומרי. בפרט, יש לבחון האם עיבוד המידע עלול לגרום לתוצאות הבאות:

- אי-יכולת של נושא המידע לממש זכויות (כולל הזכות לפרטיות);
- מניעת יכולת הגישה של נושא המידע לשירותים או הזדמנויות;
- אובדן שליטה בשימוש במידע אישי;
- אפליה;
- גניבת זהות או הונאת זהות;
- הפסד כספי;
- נזק למוניטין או לשם הטוב;
- פגיעה גופנית;
- פגיעה בסודיות;
- זיהוי מחדש של נתונים שהופרדו מהמידע המזהה (פסאודונימיזציה);
- כל חיסרון כלכלי או חברתי מהותי אחר;

---

[15] סעיף 17 לחוק הגנת הפרטיות; תקנות אבטחת מידע. את הבדיקה האם הפרויקט עומד בדרישות אבטחת המידע שמטיל הדין, ניתן לקיים באמצעות הליך ביקורת כאמור בתקנה 16 לתקנות אבטחת מידע. להרחבה בנושא הליך הביקורת ראו "המדריך המלא לתקנות הגנת הפרטיות (אבטחת מידע)" של הרשות להגנת הפרטיות, הזמין כאן.

[16] תקנה 2(ג) לתקנות אבטחת מידע.

[17] ראו תקנה 15 לתקנות אבטחת מידע, וכן הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי. ההנחיה זמינה כאן.

[18] ראו תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א – 2001.

הסיכונים לפרטיות נושאי המידע עשויים לנבוע בין היתר מפגיעה בחובת "**אבטחת המידע**",[19] או מהפרה של הוראות אחרות של רגולציית הגנת המידע, כגון האיסור להשתמש במידע בניגוד למטרה לשמה נאסף ("צמידות המטרה"), והאיסור להשתמש במידע על אודות אדם ללא קבלת הסכמה מדעת, או הסמכה חוקית אחרת.

יש לבצע הערכה של סיכוני האבטחה, אותה ניתן לקיים באמצעות סקר סיכונים ומבדקי חדירות[20] ושל סיכונים אחרים לפרטיות, לרבות מיפוי גורמי האיום או מקורות הסיכון וההשפעה הפוטנציאלית של כל תרחיש (כולל גישה בלתי חוקית, שינוי או אובדן מידע אישי).
על מנת להעריך את רמת הסיכון של התרחישים, יש לבצע שקלול של הסבירות להתממשות הסיכון, וחומרת הנזק וההשפעה האפשריות.
על הארגון לבצע הערכה אובייקטיבית של הסיכונים. כאשר מבצעים הערכה זו, מומלץ להיעזר במטריצה מובנית. ראו בדוגמה שלהלן:

חומרת הנזק				
	גבוה	**סיכון נמוך**	**סיכון גבוה**	**סיכון גבוה**
	בינוני	**סיכון נמוך**	**סיכון בינוני**	**סיכון גבוה**
	נמוך	**סיכון נמוך**	**סיכון נמוך**	**סיכון נמוך**
		נמוכה	**בינונית**	**גבוהה**
		הסתברות לסיכון		

המטריצה שלעיל מציגה שיטה מובנית להערכת סיכונים. ניתן להשתמש גם בשיטה אחרת, בהתאמה לצרכי הארגון, על מנת להשיג את אותה המטרה.
במסגרת הערכת הסיכונים, כדאי לתת את הדעת גם לסיכונים המשפיעים על הארגון עצמו, כדוגמת אי עמידה בדרישות רגולטוריות ופעולות אכיפה, נזק למוניטין, או אובדן אמון הציבור.

[19] "אבטחת מידע", כהגדרתה בסעיף 7 לחוק הגנת הפרטיות, היא "הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין".

[20] ראו תקנה 5 לתקנות אבטחת מידע. להרחבה בנושאים אלו, ראו "המדריך המלא לתקנות הגנת הפרטיות (אבטחת מידע)" של הרשות להגנת הפרטיות. ראו קישור למדריך בה"ש 14 לעיל.

2.6. שלב 6: זיהוי אמצעים לצמצום הסיכונים שאותרו

לגבי כל אחד מהסיכונים שאותרו, יש לזהות ולתעד את מקורו, ולשקול חלופות לאמצעים לצמצום הסיכון והפחתתו (להלן – "**בקרות**"). להלן רשימה לא ממצה של דוגמאות לאמצעים אפשריים לצמצום הסיכונים, הן בתחום אבטחת המידע והן בתחומים משפטיים, עסקיים, וארגוניים אחרים:

- החלטה שלא לאסוף כלל מידע מסוגים מסוימים;
- צמצום היקף העיבוד או מספר מורשי הגישה;
- צמצום תקופת שמירת המידע;
- נקיטה באמצעי אבטחה טכנולוגיים נוספים;
- הדרכת העובדים לזיהוי מוקדם של הסיכונים ולהתמודדות עימם;
- אנונימיזציה[21] או פסאודונימיזציה[22] של הנתונים, במקרים בהם הדבר רלוונטי;
- גיבוש הנחיות או נהלים פנימיים להתמודדות עם סיכונים ספציפיים;
- בחירה בטכנולוגיה אחרת לביצוע עיבוד המידע;
- תיקון והבהרה של ההסכמים עם שותפים עסקיים, או עם ספקי מיקור חוץ;
- העצמת יכולת השליטה וההשפעה של נושאי המידע. למשל, באמצעות התניית עיבוד המידע בהסכמה אקטיבית (Opt-in) של נושא המידע, מתן זכות סירוב (Opt-out) או חזרה מהסכמה, או שיפור השקיפות כלפי נושא המידע והרחבה של האינפורמציה המסופקת לו על השימוש במידע אודותיו;
- הטמעת טכנולוגיות או פרוצדורות ארגוניות המסייעות להעצמת נושא המידע במימוש זכויותיו על פי חוק, ויכולת ההשפעה שלו על עיבוד המידע אודותיו;

רשימה זו איננה ממצה, וייתכנו דרכים אחרות לצמצום או מניעת הסיכונים.

לאחר שנבחר אמצעי לצמצום סיכון מסוים לפרטיות, יש לבחון האם הסיכון אכן הצטמצם או נמנע, ולהעריך מחדש את רמת הסיכון לאחר מימוש הבקרה (להלן - "**סיכון שיורי**"). בעת קבלת החלטה על מידת ההתאמה של הבקרה המוצעת יכול הארגון לשקול גם את העלויות וכן המורכבות הטכנולוגית והתפעולית הכרוכות במימושה. עם זאת, אין בכוחם של שיקולים אלו לפטור ארגון מקיום הוראותיהן של תקנות אבטחת מידע, או מדרישות חוק הגנת הפרטיות.

[21] אנונימיזציה (התממה) היא תהליך שמטרתו הפיכת מידע אישי לבלתי ניתן לקישור לאדם מזוהה.

[22] פסאודונימיזציה הוא תהליך שמטרתו הפיכת מידע אישי לבלתי ניתן לקישור לאדם מזוהה, בהעדר מידע נוסף לגבי אותו אדם. זאת, בדרך כלל באמצעות הסרה של מזהים ישירים.

2.7. שלב 7: תיקוף ואישור התסקיר

בשלב זה, יש לתעד את הפרטים הבאים:

- האם כל סיכון וסיכון שאותר הוסר, צומצם או הוגדר כלגיטימי;
- האמצעים והבקרות הנוספים לצמצום סיכוני הפרטיות, בהם מתכוון הארגון לנקוט בעקבות עריכת התסקיר;
- רמת "הסיכון השיורי" שנותר לאחר הנקיטה באמצעים נוספים;

לאחר שתיעוד התסקיר הסתיים, יש להביאו לתיקוף ואישור של הגורם המוסמך בארגון. על הגורם המאשר לבחון ולתקף את הערכת הסיכונים אשר בוצעה בתסקיר, וכן לאשר את רמות הסיכון השיורי שנותר ואת הבקרות המתקנות אשר הוצעו במסגרת התסקיר. כאשר מדובר בפרויקטים גדולים או רגישים רצוי לערב גורם אשר יבצע בקרה על אופן עריכת התסקיר.

במידה שמסקנות התסקיר מקיימות את הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו, וכן עומדות בדרישת המידתיות (רלוונטי לגופים הכפופים לדרישת המידתיות) - הארגון אינו מחויב למנוע לחלוטין או לצמצם לרמה זניחה את כל הסיכונים שאיתר במסגרת התסקיר. ארגון אשר איננו בטוח האם הסיכון השיורי שנותר לאחר מימוש הבקרות מקיים את הוראות חוק הגנת הפרטיות ועומד בדרישת המידתיות - רשאי לפנות לרשות להגנת הפרטיות בבקשה לקבלת חוות דעת מקדמית, בהתאם לנוהל הרשות בנושא.[23]

2.8. מה קורה לאחר מכן?

יש לשלב את תוצאות ומסקנות התסקיר בתכניות העבודה של הארגון, תוך קביעת גורם אחראי לכל בקרה מתקנת ולוחות זמנים ומעקב להבטיח את ביצועה.

מטעמים של שקיפות ואחריותיות, רצוי לבחון אפשרות לפרסם את תוצאות התסקיר. הפרסום עשוי לתרום לתחושת האמון של נושאי המידע בפעולות העיבוד, ולשפר את יכולתם לממש את זכויותיהם. במקרה של חשש כי הפרסום עלול לגלות מידע בעל רגישות מסחרית, לפגוע באבטחת המידע, או לגרום לסיכונים נוספים, יש לשקול האם ניתן לפרסם גרסה מצומצמת אשר תפחית סיכונים מסוג זה.

נזכיר שוב כי התסקיר אינו פעילות חד פעמית, אלא תהליך מתמשך. יש לעדכן ולתקף מחדש את התסקיר על בסיס קבוע, או בעת ביצוע שינויים מהותיים בפרויקט, או במערכות התומכות בו, בהיבטי עיבוד המידע.

[23] ראו נוהל מתן חוות דעת מקדמיות בידי הרשות להגנת הפרטיות, הזמין כאן.