תסקיר השפעה על הפרטיות

תקציר

תסקיר השפעה על הפרטיות, (להלן - **התסקיר**) הוא כלי שנועד לשמש את הארגון לזיהוי וצמצום הסיכון לפרטיות במהלך הקמה וניהול של פרויקטים חדשים אשר יש להם השפעה על הפרטיות. השימוש בתסקיר יבטיח זיהוי מכשולים להגנת הפרטיות בשלב מוקדם, כך שהפתרון יהיה פשוט יותר, יעיל יותר ובדרך כלל, בעלות כספית נמוכה יותר. ביצוע תסקיר מיטיב הן עם הארגון והן עם האנשים שהמידע הוא על אודותיהם (להלן - **נושאי המידע**).

מהו תסקיר השפעה על הפרטיות

התסקיר הינו הליך שמבוצע על ידי הארגון בשלב מוקדם של תכנון מערכת המידע (להלן - **המערכת**), על מנת לזהות במערכת סיכונים לפגיעה בפרטיות ולהגנת המידע האישי, ולעצבה בדרך שתמזער את הסיכונים האפשריים ואף תמנע אותם. תסקיר אפקטיבי מבוצע כבר בשלב התכנון והיישום הראשוני של המערכת, כחלק מתהליך " תכנון לפרטיות" (Privacy By Design או PBD).

PBD פירושו עיצוב הטכנולוגיה כך שתגן על הפרטיות באופן אופטימלי מלכתחילה, ולא בדיעבד, כשיתברר שיש בעיה. לשם כך, יש להטמיע שיקולי פרטיות ואבטחת מידע לתוך מערכות ממחושבות בכל שלבי החיים שלהן, החל משלב העיצוב, דרך שלב השימוש ועד לשלב שבו מפסיקים להשתמש בהן. התסקיר מאפשר לארגון לנתח באופן שיטתי כיצד מערכת מידע תשפיע על הפרטיות של נושאי המידע. מטרת התסקיר להבטיח כי הסיכון לפרטיות במערכות המידע יהיה מינימלי ככל האפשר. מומלץ לבצע את התהליך כך שעובר לכל החלטה עסקית תבוצע בדיקה של השלכותיה על עקרונות דיני הפרטיות. המטרה היא שהעיצוב ישרת את התכליות העסקיות, בד בבד עם מזעור הסיכונים לפרטיות והשקעת משאבים באמצעי ההגנה הנדרשים.

עוד נועד התסקיר להציג את האופן שבו הנהלת הארגון מימשה את חובותיה ואחריותה בהתאם להוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן - **החוק**) והתקנות המותקנות לפיו. בהתאם לכך, נועד התסקיר לשקף את הליך הבחינה הפנימי של היבטי הפרטיות בפעילות המערכת, של הסיכונים הנובעים ממנה ושל האמצעים שננקטו כדי להתמודד עמם.

מהי פרטיות במידע

הזכות לפרטיות היא זכות חוקתית המעוגנת בחוק יסוד: כבוד האדם וחירותו. הזכות לפרטיות מתפרסת על תחומים רבים בחיי היומיום.

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

נדבך אחד שבו עוסקת הזכות לפרטיות הוא הזכות לפרטיות במידע, דהיינו – זכותו של אדם לשלוט, לערוך, לנהל ולמחוק מידע על אודותיו, להחליט עם מי לחלוק את המידע וכיצד. פגיעה בפרטיות המידע יכולה ללבוש מספר צורות כגון איסוף מידע ללא בסיס חוקי, גילוי מידע על אודות אדם ללא הסכמתו ושימוש במידע אודות אדם שלא למטרה שלשמה הוא נמסר.
הזכות לפרטיות במידע מעוגנת בפרק ב׳ לחוק, שעניינו הגנה על הפרטיות במאגרי מידע, אשר מסדיר הן את זכויות נושאי המידע והן את חובותיהם של בעל מאגר המידע, המחזיק במאגר המידע, מנהל מאגר המידע והמשתמש במידע שבמאגר.

תסקיר השפעה על הפרטיות נועד בראש ובראשונה להתמודד עם הזכות לפרטיות במידע ולהקטין את הסיכון לפגיעה בפרטיות במידע למינימום הכרחי. להלן דוגמאות לדרכים שבהן מתממש הסיכון לפרטיות:

- מוחזק מידע לא מדויק, לא מספיק, או לא מעודכן.
- מוחזק מידע עודף, או לא רלוונטי.
- המידע מוחזק לזמן רב מדי.
- גילוי מידע לצדדים שלישיים, ללא הסכמתו של נושא המידע.
- שימוש במידע שלא למטרה שלשמה הוא נמסר.
- שימור מידע באופן לא מאובטח.

כאשר הסיכון לפרטיות במידע מתממש, נגרם נזק. לפעמים הנזק מוחשי וניתן לכימות, כמו הפסד כלכלי, ולעיתים הנזק בלתי מוחשי ו/או בלתי ניתן לכימות. יודגש כי בעידן המידע והרשתות הדיגיטליות, יכולת הצלבת המידע והפצתו גדולה מאי פעם וגדלה כל העת, ולכן מידע שמתגלה לא ניתן שוב להסתיר, למחוק או להסיר, כך שבדרך כלל, הנזק הוא בלתי הפיך.
יתרה מזאת, הנזק הנגרם משימוש במידע אישי יכול להיות חסר חשיבות או זניח בעיני האדם, אך מצטבר ומשמעותי בהשפעתו על החברה. לפיכך נודעת חשיבות ראשונה במעלה לביצוע תסקיר השפעה על הפרטיות מבעוד מועד ובאופן תדיר, על מנת להפחית את הסיכון לפגיעה בפרטיות במידע למינימום הכרחי.

היתרונות של תסקיר השפעה על הפרטיות

הרשות למשפט, טכנולוגיה ומידע (להלן - **רמו״ט**) מקדמת את ביצוע התסקיר על מנת לעזור לארגונים לוודא שמערכות המידע בארגון תואמות לדרישות החוק והתקנות על פיו, בכל הקשור להיבטי פרטיות ואבטחת המידע. רמו״ט עשויה לבקש מארגון לבצע תסקיר, משום שזו הדרך היעילה ביותר לוודא כי תהליכים פנים-ארגוניים הקשורים במידע אישי עומדים בדרישות חוקיות.

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל׳: 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

ביצוע תסקיר השפעה על הפרטיות מיטיב הן עם הארגון והן עם נושאי המידע. נושאי המידע יכולים לחוש יותר ביטחון ואמון לגבי הטיפול במידע האישי שלהם, ביודעם שהארגון נקט ונוקט צעדים להבטיח כי הסיכון לפגיעה במידע האישי שלהם הוא מינימלי. זאת ועוד, שקיפות התהליך משפרת את הבנת נושאי המידע לגבי האופנים שבהם משתמש הארגון במידע על אודותיהם.

ארגון המבצע תסקיר השפעת פרטיות יוצא א, הוא נשכר. ביצוע התסקיר כהלכה מבטיח כי הארגון עומד בדרישות החוקיות, מקטין את הסיכון לפגיעה בפרטיות במידע, מאפשר זיהוי בעיות בשלב מוקדם ומאפשר פתרון פשוט וזול.

באופן כללי, שימוש תדיר בתסקיר השפעה על הפרטיות מגדיל את המודעות לפרטיות ולאבטחת מידע בארגון, ומבטיח כי נושאי פרטיות יעלו כבר בשלב המוקדם של כל החלטה עסקית.

מקרים שבהם רצוי לבצע תסקיר השפעה על הפרטיות

העקרונות הכלליים שנבחנים בתסקיר יכולים לשמש בכל פרויקט המערב שימוש במידע אישי, ובכל פעילות עסקית אשר יש לה השפעה על פרטיותם של אנשים. להלן דוגמאות למקרים שבהם רצוי לבצע תסקיר השפעה על הפרטיות:

- מערכת מידע חדשה אשר שומרת או מעבדת מידע אישי.
- פרויקט שיתוף מידע אישי בין ארגונים.
- הצעה לזהות קבוצת אנשים לפי קריטריון משותף על מנת להניע פעולה.
- שימוש במידע קיים לפרויקט חדש או למטרה חדשה.
- שימוש בנתוני מעקב, כגון מצלמות ונתוני מיקום.
- הקמת מאגר מידע חדש שיקלוט לתוכו מידע המוחזק בחלקים שונים של הארגון.
- גיבוש מדיניות, אסטרטגיה ו/או נהלים בנושאי שימוש ו/או גילוי מידע אישי.

על מנת שהתסקיר יהיה אפקטיבי, יש לבצע אותו עבור כל פרויקט בנפרד, ולבצעו בשלב שבו יש לו יכולת להשפיע על הפרויקט. לפיכך, תסקיר השפעה על הפרטיות יבוצע לרוב לגבי פרויקטים חדשים, או לצורכי ביקורת על פרויקטים קיימים.

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

תוכן עניינים

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

1. ניתוח תהליכי איסוף ועיבוד המידע

1.1 הגדרות

1.1.1 "**מידע אישי**" - מידע על אודות אדם, מידע מזוהה או ניתן לזיהוי. הגדרת המידע כאישי מהווה הבסיס לתסקיר, וביחס אליו יש לתאר את מכלול התהליכים;

1.1.2 "**נושא המידע**" - זהו האדם שהפרטים על אודותיו מעובדים במערכת. בטרמינולוגיה של התסקיר יש להבחין בין "לקוחות" המערכת, כלומר משתמשים או גורמים המקבלים ממנה מידע, ובין נושאי המידע;

1.1.3 "**מידע מזהה**" - יש להבהיר מה נכלל ב"מידע מזהה" (למשל: מידע מזהה יכול לכלול שם, מספר זהות, כתובת, מספר כרטיס אשראי, מספר טלפון וכדומה). לפירוט נוסף, ניתן לפנות להגדרות "מידע" ו"מידע רגיש" לפי החוק, וכן לפסיקה הרלוונטית אשר מבחינה בין סוגי המידע השונים והמפורטת בסילבוס של רמו"ט באתר Ilita.Justice.gov.il.

1.1.4 "**מאגר מידע**" - כהגדרתו בסעיף 7 לחוק.

1.2 תיאור תהליך זרימת המידע במערכת

1.2.1 פירוט של כל פריטי המידע שנאסף ונשמר במערכת הממוחשבת, במאגרי המידע שבה והקשורים אליה (להלן - **המערכת**). הפירוט יכלול גם את המידע האישי הניתן לזיהוי. (למשל: שם, תאריך לידה, כתובת דואר אלקטרוני, מספר טלפון, מספר זהות, כתובת, מיקוד, שם נעוריה של האם, מספר חבר בקופת חולים, מספר חשבון בנק, רישיון נהיגה, מצב משפחתי וכדומה);

1.2.2 במקרה שבמסגרת השימוש במערכת נוצר מידע נוסף, יש לתאר את אופן יצירת המידע ומטרתו;

1.2.3 במידה שהמערכת מקבלת/מוסרת מידע מ/אל מערכות אחרות (כגון תשובה לאימות מידע) יש לתאר את המערכת שממנה נלקח המידע, המידע שמוחזר וכיצד נעשה בו שימוש;

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

1.2.4 במקומות ובתהליכים שבהם נשמר מידע ללא מידע מזהה, לא בהכרח נובע מכך שהמידע אינו ניתן לזיהוי, על ידי שחזור הזהות בהצלבת המידע עם מידע אחר. לכן, יש לתאר את הסיכון לזיהוי בהנדסה חוזרת והדרכים להתמודד עמו;

1.3 תיאור תהליך איסוף ועיבוד המידע

במסגרת השירותים שתיתן המערכת, על מכלול התחנות שהמידע עובר בהן, נדרש להתייחס לפרמטרים הבאים:

1.3.1 יש לתאר את מחזור החיים של המידע מעת שהוא נקלט במערכת ועד שהוא מועבר למערכת אחרת, במקרה שישנה העברה של המידע. מובן כי יש לסקור היבטים נוספים חשובים, ככל שישנם, להבנה או לתיאור תהליך העבודה של המערכת. אולם, חשוב להבהיר כיצד תיאורים אלה משרתים את המטרה, שהיא הבנת זרימת המידע במערכת;

1.3.2 תיאור תהליכי עיבוד המידע, החל מקבלת המידע ממקורות המידע ועד להעברתם למזמין המידע, במקרה שישנה העברה של המידע;

1.3.3 במקרה שישנה העברת מידע, יש לציין ליד כל פריט מידע את הזיקה בין המידע המועבר ובין מטרת המערכת, וכן את האסמכתא החוקית להעברת המידע (למשל - הוראות החוק);

1.3.4 לצד תהליך עיבוד המידע, יש לציין את הזיקה בין התהליך ובין מטרות המערכת;

1.3.5 בהתאם לכך, יש לתאר את מקורות איסוף המידע המועבר או הנשמר במערכת, המטרות לשימוש בו והאסמכתא החוקית לאיסוף זה;

1.3.6 תיאור קבוצות איסוף סוגי המידע; האם נאספים ישירות, מגיעים ממאגר מידע אחר או שהמידע נוצר כחלק מתהליכי המערכת. יש לפרט לגבי כל פריט מידע המפורט לעיל;

1.3.7 במקרה שמידע נאסף ממקורות נוספים פרט לנושאי המידע עצמם, ובכלל זה מערכות IT אחרות, מאגרי מידע, ספקי תוכן עסקיים או משרדים ומחלקות אחרות, יש לציין את מקור המידע, מטרת איסופו והסבר לכך שהמידע נאסף בדרך זו ולא ישירות מנושאי המידע;

1.4 תיאור הרכיבים הטכנולוגים המשתתפים בתהליך

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

1.4.1 יש לפרט אם מתבצעים ניתוחים טכנולוגים במידע שנאסף לצורך זיהוי דפוסים או אנומליה, ובמקרה שכן, אילו שימושים יעשו במידע המתקבל;

1.4.2 האם ייעשו השלמות מידע שחסר על סמך אלגוריתמים טכנולוגיים לצורך הוספת מידע שלא נמסר באופן ישיר, או על ידי הצלבה ממקורות מידע נוספים;

1.4.3 יש להסביר כיצד ומדוע נעשה שימוש בפריטי המידע במערכת;

1.4.4 יש לפרט כל שימוש שנעשה בפריטי המידע שנאספים או מתוחזקים. יש לתאר כיצד ומדוע ייעשה שימוש ברכיבי המידע השונים;

1.4.5 התייחסות לסוגי מידע נוספים, שאינם מידע אישי, ככל שהדבר נדרש לתיאור היבטי פרטיות ואבטחה. מאחר שמדובר במסמך בעל אופי אבטחתי, עליו לתאר סוגי מידע נוספים כגון מידע בעל ערך אבטחתי (למשל - בהתאם לשיטת הסיווג בתקן-ISO 27001). אולם, חשוב להבחין בין מידע זה ובין מידע אישי על אדם ולהשתמש בהגדרות ובמינוחים אחידים;

1.5 תיאור אופן הבקשה לאיסוף המידע

1.5.1 כיצד מודיעים לנושאי המידע טרם איסוף המידע; אם ישנם מקרים שבהם לא נמסרת הודעה על האיסוף (להלן - **ההודעה**), יש לפרט את הסיבה לכך;

1.5.2 יש לתאר כיצד מתבצע תהליך ההודעה לנושאי המידע טרם איסוף המידע לצורך מערכת זו. האם קיימת מדיניות פרטיות כתובה הנגישה לנושאי המידע וללקוחות (אם כן, יש לצרפה לתסקיר);

1.5.3 מה מידת הבהירות והקוהרנטיות של ההודעה שנשלחת ללקוחות;

1.5.4 אלו אפשרויות עומדות בפני נושאי המידע להגביל או למנוע את השימוש במידע על אודותיהם במערכת;

1.5.5 האם אדם יכול לסרב להעברת המידע (הן בעצמו והן על ידי הגופים האחרים שמהם נאסף המידע על אודותיו); אם כן, מה ההשלכות של סירובו זה, האם בעקבותיו תיפגע יכולתו להשתמש בשירותי המערכת;

1.6 תיאור אופן השליטה בשימוש במידע

1.6.1 כיצד יתבצע הפיקוח על כך שהשימוש במידע יהיה אך ורק למטרה שלשמה נאסף;

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

1.6.2 כיצד יתבצע הפיקוח על כך שהשימוש במידע והנגישות אליו יוגבלו רק למורשה הגישה;

1.6.3 כיצד יתבצע הפיקוח על כך שהעברות המידע מהמערכת החוצה לפי הכללים המותרים, מתבצעות בהתאם למתווה הפרטיות הרצוי, הן מהבחינה המשפטית והן מהבחינה הטכנולוגית;

1.7 שמירת המידע

1.7.1 האם קיימת חובת שמירת מידע במערכת;

1.7.2 האם כל המידע שנאסף נשמר; האם חלק מסוים מהמידע נשמר;

1.7.3 אם כן, יש לפרט את מהות החובה לשמירת המידע לגבי כל מאגר או לגבי כל קבוצה של מידע במאגר (מכוח הוראות חוק/תקנות) ואת משך זמן השמירה;

1.7.4 אילו סיכונים יכולים לנבוע משמירת המידע לתקופה זו; כיצד הופחתו הסיכונים הנ"ל;

1.7.5 מהו התהליך לעדכון מידע שמור במקרה שיש בו טעות; כיצד מתבצע תהליך העדכון; מי מבצע את העדכון;

1.7.6 האם המידע נמצא בתוך מערכת סגורה בלבד; האם הוא נגיש לרשת נוספת; האם הוא מחובר לאינטרנט; האם המידע יועבר באמצעים ניידים;

1.8 תיאור תהליכי העברת מידע

1.8.1 מאגרי מידע חיצוניים (במקרה שקיים)

יש לבצע את הבדיקה לכל מאגר מידע חיצוני בנפרד:

1.8.1.1 איך מתבצע החיבור למאגר המידע החיצוני; האם קיימת גישה חופשית למאגרי המידע החיצוניים/לחלקים מהם או שמדובר בשאילתות ספציפיות;

1.8.1.2 על פי אילו מזהים נעשה האימות של מורשי הגישה לחיבור;

1.8.1.3 האם ישנו מעקב אחרי הלוגים של מורשי הגישה;

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

1.8.1.4 מהו תוצר החיבור ואילו ערכים מתקבלים מהחיבור; תשובה של True/False (Boolean variable), צפייה במידע, קבלת ערכים עם יכולת שמירה או העתקה וכדומה;

1.8.1.5 האם נעשה שימוש במקורות מידע נוספים; האם נאסר על שימוש במקורות מידע נוספים;

1.8.1.6 האם קיים רישום למקורות המידע מהמאגרים החיצוניים שאוספים את המידע ומעבירים אותו למערכת דנן; כיצד מתבצע אימות המידע המתקבל מגורמים אלה; מהי מידת הוודאות הנדרשת לצורך שימוש במידע שנאסף ממקורות אלה;

1.8.2 כיצד מתבצעת העברת המידע בין הגופים השונים; באמצעות עדכון ישיר למאגר הנתונים, באמצעות Web Services וכו';

1.8.3 אילו אמצעי אבטחה ננקטים על מנת שהמידע לא ייורט בדרך;

1.8.4 אילו אמצעים ננקטים על מנת לאבטח את העברת המידע;

1.8.5 כיצד מזוהות נקודות הקצה לעניין העברת המידע; איזה תהליך ננקט כדי לוודא שמדובר בתחנת קצה לגיטימית;

1.9 הרשאות גישה

1.9.1 תיאור הטיפול בהרשאות גישה ותיאור השימוש בהתממה (אנונימיזציה) או טשטוש (פסבדונימיזציה) של מידע;

1.9.2 זיהוי מורשי הגישה למידע בכל שלב: תיאור הגישה שלהם למידע בכל שלב והסביבה שבהם הם פועלים;

1.9.3 הגדרה חד-ערכית וברורה לכל אחד מסוגי בעלי ההרשאות; הסבר לגבי הצורך בגישה ביחס למטרות המערכת והאסמכתא לכך;

1.9.4 הרחבה לעניין מאפייני השימוש ולעניין הנחות עבודה לגבי היבטי האבטחה והפרטיות של סביבת המשתמש ולגבי האתר שבו ניתנת גישה למערכת;

1.9.5 תיאור תהליכי רישום משתמש, זיהוי ואישור;

1.10 תיאור תהליך מחיקת מידע

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

כיצד מבוצעת מחיקה של פריטי מידע; לאחר איזה פרק זמן; מי האחראי על כך;

1.11 תהליכי גיבוי ואחזור מידע

היכן נמצאים שרתי הגיבוי; כיצד מתבצעת פעולת הגיבוי ואחזור המידע;

1.12 תיאור גרפי של התהליכים העסקיים

בכל מקרה שבו קיים תהליך הקשור בניהול מידע והמכיל תהליכים הנוגעים לאלמנטים בתהליך כזה, יש לשרטט דיאגרמת זרימת מידע שתתאר כיצד המידע זורם בארגון כתוצאה מהתהליכים העסקיים;

1.13 פיתוח תרשימי זרימה מפורטים למידע האישי

נוסף לתיאורים המפורטים לעיל, יש לצרף Use Cases לפעולות אשר מעורב בהן מידע אישי ברמת המשתמשים, האפליקציה, מאגר הנתונים, שאר רכיבי המערכת והתוצאה המתקבלת מפעולה זו; דוגמא לפירוט תיאור כאמור לעיל על ידי שימוש בטבלאות:

תיאור סוג המידע	שם פריט מידע	נאסף בידי	אופן איסוף מידע	מטרת האיסוף	היכן נשמר פריט המידע[1]	כיצד נעשה שימוש בפריט המידע	האם המידע מאפשר זיהוי האדם	האם המידע משותף עם גורמים	מי יכול לגשת למידע[2]	לאן, למי וכיצד מועבר המידע	אופן גישה למידע (ברמת תקשורת)

[1] אם במסד הנתונים, יש לציין שם מסד וטבלה, אם בקובץ – שם הקובץ וכו'.
[2] תיאור תפקיד ומספר צפוי של בעלי תפקידים כאמור.

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

2 ניהול סיכונים ביחס למידע וניהול סקרי אבטחת מידע

2.1 רקע כללי לעניין הערכת סיכונים

2.1.1 ביחס למידע שנאסף כמפורט לעיל, יש לבצע תהליך של הערכת סיכוני אבטחת מידע במערכות המידע והממשקים;

2.1.2 "**סקר סיכונים ומבדק חוסן**" הינו סקר הנערך בידי בעל הכשרה מתאימה, במטרה לזהות ולדרג את רמת החשיפה לסיכון הקיימת בכל אחת ממערכות המחשוב שבמאגר המידע, על סמך מאפייני סיכון שייקבעו;

2.1.3 הערכת הסיכונים תגדיר את רמת הרגישות של המערכות, ותתייחס למכלול סיכוני אבטחת המידע הפוטנציאלים הנובעים ממערכות המידע ומההתנהלות העסקית השוטפת של הארגון. סיווג רמת הרגישות של כל מערכת תיקבע לפי המידע בעל הרגישות הגבוהה ביותר שבו היא מטפלת;

2.1.4 תהליך זה יתבסס על סיווג הנכסים, אופי העבודה באגפים השונים בארגון והאופי העסקי של הארגון;

2.1.5 הארגון יעדכן את הערכת הסיכונים עם שינויים משמעותיים בתהליכים העסקיים, במערכות המידע או באיומי אבטחת מידע;

2.1.6 תוצרי הערכת הסיכונים ינחו את הנהלת הארגון בהפניית משאבים נאותים להטמעת אמצעי אבטחת מידע ולמיקוד בסקרי סיכוני אבטחת המידע במערכות השונות בארגון;

2.1.7 תוצר הערכת הסיכונים, המתבסס בין היתר על סיווג נכסי המידע, יספק מדרג רגישות של מערכות שונות בארגון;

2.1.8 מערכות המכילות מידע שסווגו בסיווג גבוה, לפי סיווג נכסי מידע, יסווגו כמערכות בעלות סיכון גבוה;

2.2 סקרי סיכוני אבטחת מידע ומבחני חדירה מבוקרים

2.2.1 בעת עיצוב מעטפת אבטחת המידע, יש לשלב ביצוע סקרי אבטחת מידע ומבדקי חוסן של מערך טכנולוגיית המידע של הארגון, בהתאם לכללים הבאים; מערכות בעלות סיכון גבוה ייסקרו לפחות אחת ל-18 חודשים או לאחר ביצוע שינויים בתשתיות או

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

במערכת עצמה, וכן בעת פרסום של פרצת אבטחה חדשה המסכנת את המערכת והתשתיות;

2.2.2 הסקרים ומבדקי החוסן יבחנו את נושאי הניהול ואת יעילות אמצעי ההגנה (כולל אמצעים פיזיים ולוגיים) שיושמו בארגון. כמו כן, הסקרים ומבדקי החוסן יבחנו את הגדרות אבטחת המידע במערכות המידע הן ברמת התשתית (ציוד ותווך תקשורת, מערכות הפעלה, בסיסי נתונים) והן ברמת האפליקציה (ברמת קוד מקור או חבילות תוכנה);

2.2.3 הארגון יערוך סקרי אבטחת מידע לפני הטמעת שינויים משמעותיים במערכות שהוגדרו על ידי הארגון כבעלות סיכון גבוה או לפני הכנסת מערכות אלו לשימוש תפעולי (Production);

2.2.4 מנהל אבטחת המידע יזום מבחני חוסן (Penetration Tests) הן ברמת התשתית והן ברמת היישום (אפליקציה), המדמים ניסיונות פריצה על ידי תוקף מתוך ומחוץ לארגון, הן כמשתמש קיים והן כגורם זר. תדירות מבחני החוסן תביא בחשבון את רגישות המערך בהתאם להערכת סיכוני אבטחת מידע; מערכות מידע הפתוחות לתווך תקשורת ציבורי, יעברו מבחני חדירה לכל הפחות אחת ל-18 חודשים, או לאחר ביצוע שינויים בתשתיות או במערכת עצמה, וכן בעת פרסום של פרצת אבטחה חדשה המסכנת את המערכת והתשתיות;

2.2.5 סקרי אבטחת המידע ומבחני החוסן התקופתיים ייערכו על ידי גורם מקצועי, עצמאי, בלתי תלוי וחיצוני לארגון;

2.2.6 הנהלת הארגון תקיים דיונים על תוצאות סקרי אבטחת המידע ומבחני החוסן, ותפעל למימוש ההמלצות שיתקבלו תוך פרק זמן סביר;

2.3 הגדרת נהלים לניהול סיכונים

2.3.1 לכל תהליך הנוגע לניהול, הכנסה, תפעול, תחזוקה והוצאה של מידע בארגון, כולל מערכות המכילות זיכרון נייד כדוגמת מחשבים ניידים וסייען דיגיטלי (Personal Digital Assistant), ייכתב נוהל אבטחת מידע מפורט; לכל הפחות, ייכתבו נהלים לכל הנושאים המפורטים לעיל;

2.3.2 נהלים אלה ייגזרו ממדיניות אבטחת המידע ומצורכי אבטחת המידע בארגון;

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

2.3.3 ההנהלה תאשר את הנהלים עם כתיבתם או את השינויים המהותיים בהם, ותפעל להטמעתם;

2.3.4 הנהלים יעברו תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בסביבה הטכנולוגית או לאחר אירוע אבטחת מידע, ולכל הפחות אחת ל-24 חודשים;

3 עיצוב לפרטיות ותיאור פתרונות

3.1 בבחירת החלופות העיצוביות של המערכת לצורך ההתמודדות עם הסיכונים, יש לתאר את הסיכונים לפרטיות הנובעים משיקולי אבטחת מידע ופרטיות כמתואר לעיל;

3.2 בחירת הפתרונות תתבסס על המסקנות העולות מתוך סקר הסיכונים;

3.3 במסגרת הדיון הכולל בסיכונים ובהחלטות העיצוביות יש להתייחס, בין היתר, גם לנושאים הבאים:

3.3.1 בחירה ברכיבים:

3.3.1.1 תיאור הסיכונים הנשקפים מהרכיבים השונים;

3.3.1.2 מידת אבטחת המידע הבסיסית של רכיבים אלה ואופן ההתמודדות עם ההקשחה שלהם במערכת;

3.3.1.3 במיפוי הסיכונים של מרכיבים אלה יש להתייחס לשאלות הבאות, בהתאם לסדר הבא:

3.3.1.3.1 האם ניתן להתמודד עם הסיכונים על בסיס התכונות והיכולות של הרכיב;

3.3.1.3.2 במקרה שלא, האם מוטמע רכיב טכנולוגי שנועד להתמודד עם הסיכונים, כמעגל הגנה חיצוני נוסף;

3.3.2 עיצוב הממשקים, הסיכונים הנובעים מהם והפתרונות לכך;

3.3.3 שימוש בהצפנה ואנונימיזציה של מידע:

3.3.3.1 מהן שיטות ההצפנה במידע, כיצד יוטמעו ומה המגבלות החלות עליהן;

3.3.3.2 היכן תבוצע ההצפנה;

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il

3.3.3.3 איזה רכיב ואיזה בעל הרשאה רשאים לבקש פענוח מידע שהוצפן ;

3.3.3.4 כיצד תבוצע אנונימיזציה ;

3.3.3.5 מה הסיכון לדה-אנונימיזציה של מידע אנונימי ;

4 סיכום והנחיות להמשך

תסקיר השפעה על הפרטיות, כפי הצגתו המפורטת לעיל, הוא כלי לשימוש הארגון על מנת לזהות ולהקטין את הסיכון לפרטיות בהקמה וניהול של פרויקטים חדשים אשר יש להם השפעה על הפרטיות.[3]

עורך התסקיר יתאר את עמידת המערכת בדרישות של תהליכי תכנון לפרטיות ואבטחת המידע, כמתואר לעיל. כמו כן, עורך התסקיר יעמוד על הוראות נוספות לעניין אופן העדכון של התוצרים מהתסקיר, וכן לעניין נושאים שאינם מטופלים בתסקיר ועשויים לשאת השלכות לגבי פרטיות במידע.

[3] להרחבת מקורות הידע בנושא, ראה המדריך לתסקיר ההשפעה על הפרטיות של הרשות הבריטית להגנת המידע, בלינק להלן: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

קרית הממשלה, ת.ד. 7360, תל אביב 6107202. טל': 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 6107202 Israel. Tel: 03-7634050 Fax: 02-6467064
Email: ilita@justice.gov.il | Web: ilita.justice.gov.il