



מחזור חיי המידע

מדריך הגנת פרטיות: תפקיד ה- PQMS במחזור חיי מידע אישי

1. תכנון מוקדם

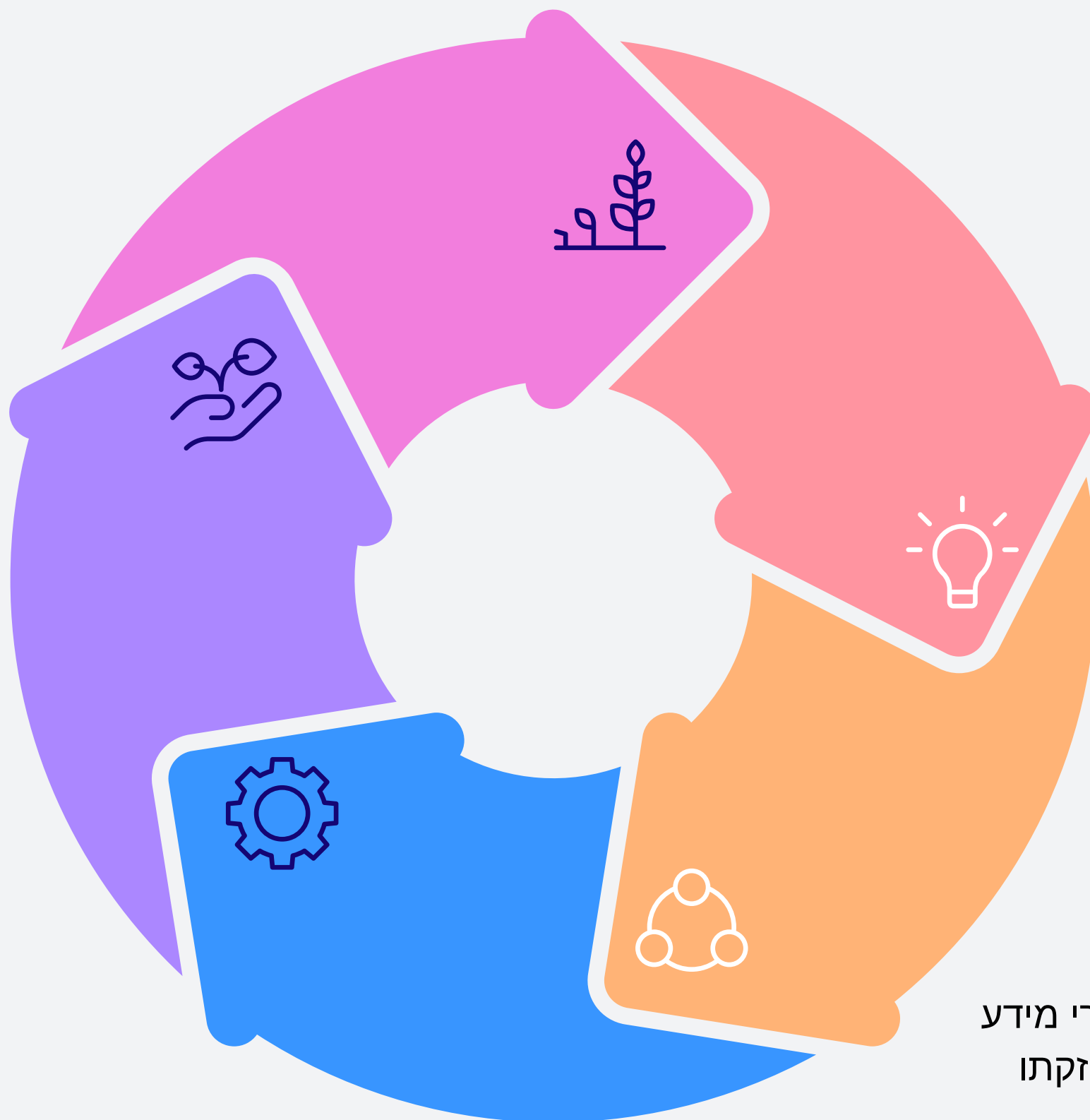
שלב מקדמי לשלב איסוף המידע שנועד להיות מיושם בטרם השקה ושימוש במערכת טכנולוגית חדשה או התחלת ביצוע תהליך טכנולוגי הכרוכים בעיבוד מידע אישי

2. איסוף מידע

שלב האיסוף בפועל של המידע האישי

3. אחסון מידע אישי

שלב קבלת המידע ושמירתו במאגרי מידע מרגע איסופו ולאורך כל תקופת החזקתו על-ידי הארגון



5. סיום חיי המידע האישי

שלב סיום השימוש וההחזקה של מידע אישי

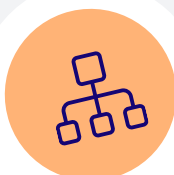
4. עיבוד מידע אישי

שלב ביצוע פעולות על ובמידע האישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו או מתן גישה אליו



תכנון מוקדם

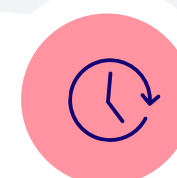
צומח



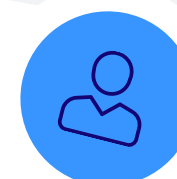
תסקיר השפעה על
פרטיות =
שאיס מרכזיים



מה צריך לדעת?



הגדרה ומטרה





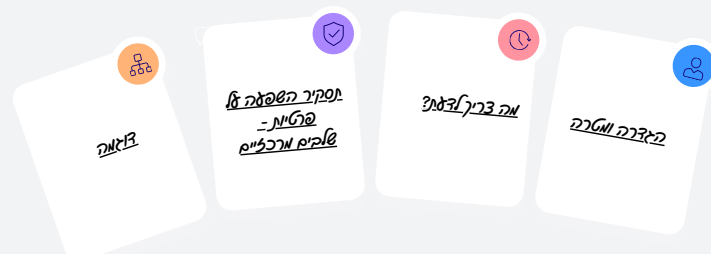
הגדרה ומטרה

שלב התכנון המוקדם הוא שלב מקדמי לשלב איסוף המידע, והוא נועד להיות מיושם בטרם השקה ושימוש במערכת טכנולוגית חדשה, או התחלת ביצוע תהליך טכנולוגי הכרוכים בעיבוד מידע אישי.

בשלב התכנון המוקדם אמורים ארגונים לתכנן את הליך איסוף המידע ועיבודו בתלות במוצר או בשירות. שלב זה מאופיין, בין היתר, בביצוע התהליכים הבאים:

- תכנון תהליך איסוף, עיבוד ואחסון המידע;
- זיהוי וקביעת בסיס המידע החוקי לאיסוף המידע ועיבודו;
- הגדרת מטרות איסוף המידע;
- הגדרת פרק זמן השימוש במידע;
- זיהוי קהל היעד הרלוונטי;
- קביעת היקף וסוג המידע האישי הנחוצים להשגת מטרות איסוף המידע, ואופי עיבוד המידע;
- התייעצות עם גורמי מקצוע נדרשים (כגון ייעוץ משפטי, ממונה על הגנת הפרטיות, ממונה אבטחת מידע וכו') וגורמים בעלי עניין;
- בחינת וקבלת החלטות בדבר הטכנולוגיות בהן ייעשה שימוש לאיסוף ועיבוד המידע;
- ביצוע הליך הערכת סיכונים, ועוד.

תכנון מוקדם





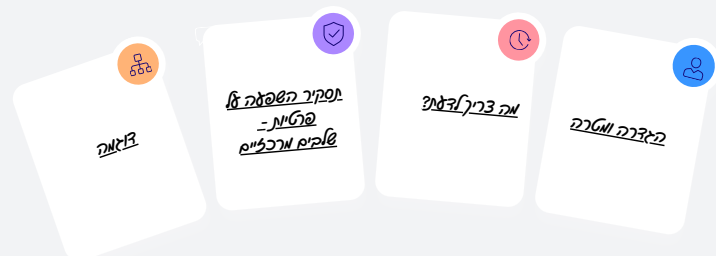
מה צריך לדעת?

סעיף 17ב(ב) לחוק הגנת הפרטיות קובע כי על ארגונים המחויבים במינוי ממונה על הגנת הפרטיות לוודא כי הממונה יהיה "מעורב כראוי בכל נושא הנוגע לדיני הגנת פרטיות".

לפיכך, ממונה על הגנת הפרטיות צריך להיות מעורב באופן משמעותי בשלב התכנון המוקדם, כבר מראשיתו, ככל שמדובר בתהליך תכנון של הטמעת טכנולוגיה חדשה או כל יישום אחר בעל השפעה על פרטיות.

להרחבה – "גילוי דעת בנושא מינוי ממונה על הגנת הפרטיות בארגון (DPO) לפי דרישות תיקון 13 לחוק הגנת הפרטיות".

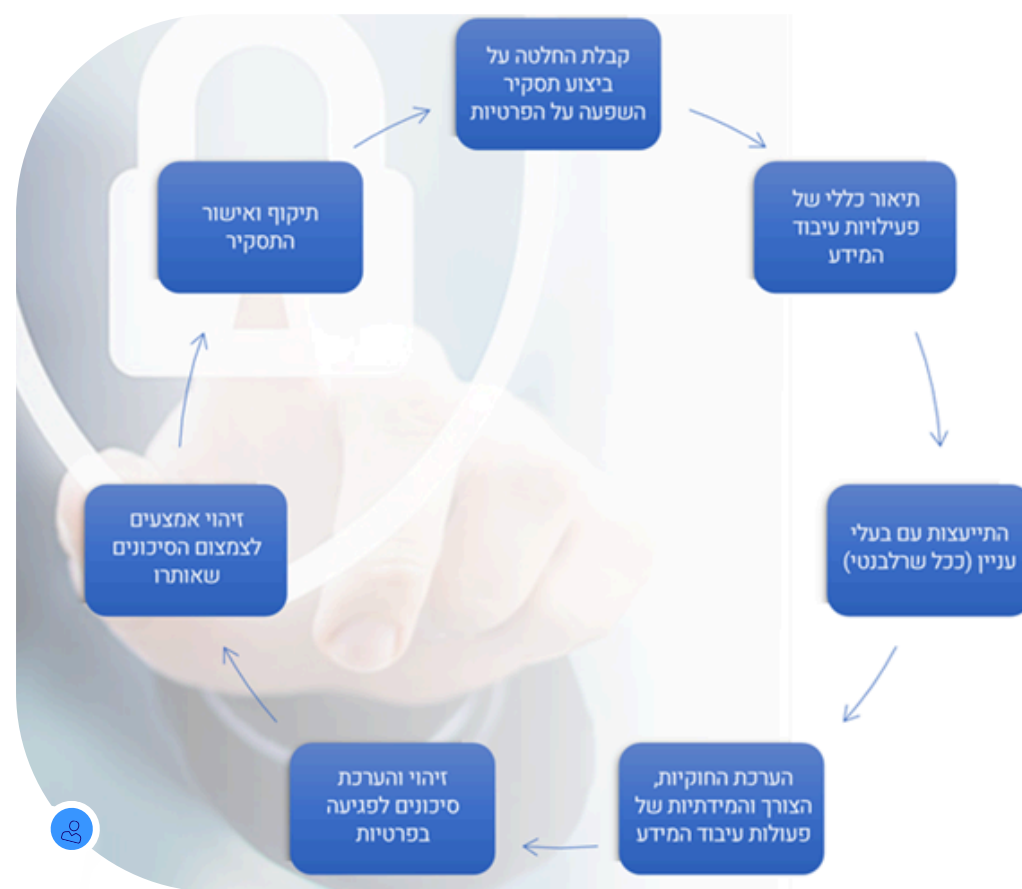
תכנון מוקדם





בשלב זה, ובין השאר לפי מסקנות התסקיר, מומלץ גם לבחון שימוש בטכנולוגיות מגבירות פרטיות שהן אוסף של שיטות, תהליכים וכלים דיגיטליים שנועדו לסייע בהגנה על מידע אישי ולהקטין את הסיכון לחשיפתו, (בין היתר באמצעות ערפול המידע וצמצום הפירוט שלו), וכן להביא לחיזוק השקיפות והשליטה של נושא המידע במידע על אודותיו.

להרחבה ראו "מדריך לטכנולוגיות מגבירות-פרטיות".



תכנון מוקדם

הזדמנות

יסקיר השפעה על פרטיות - שלבים מרכזיים

מה צריך לדעת?

הזדמנות



תסקיר השפעה על פרטיות - שלבים מרכזיים

בשלב התכנון המוקדם מומלץ מאד לבצע תסקיר השפעה על פרטיות שנועד, בין היתר, לסייע לארגונים לאתר מראש סיכונים אפשריים לפרטיות ולצמצמם מבעוד מועד.

תסקיר השפעה על הפרטיות הוא תהליך המנתח באופן מקיף ושיטתי את השפעת עיבוד המידע האישי והטכנולוגיות המשמשות אותו על פרטיות נושאי המידע.

התסקיר מזהה את מכלול הסיכונים לפרטיות, בוחן חלופות ומציע את הדרך לצמצם את הסיכונים למינימום. התסקיר נועד לשמש ארגונים במהלך הקמה וניהול של פרויקטים חדשים אשר יש להם השפעה על הפרטיות, ובפרט מערכות טכנולוגיות חדשות ופרויקטים הכרוכים באיסוף ובעיבוד של מידע אישי.

להרחבה – "מדריך עזר מתודולוגי לעריכת תסקיר השפעה על הפרטיות"; עיצוב לפרטיות (Privacy By Design).



תכנון מוקדם

המנהל

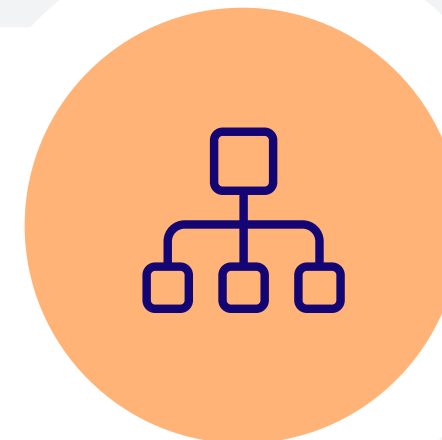
מפקד השטח
פיקוח -
שליטת מרכזים

מנהל צרכנות

המנהל המרכזי

בסיום התהליך, החברה מצאה כי בנסיבות המקרה קיימת הצדקה למעבר למערכת ביומטרית לבקרת נוכחות. עם זאת, כדי לצמצם את הפגיעה בפרטיות, הוחלט שהמידע הביומטרי יישמר רק על גבי הכרטיסים בשימוש העובדים, ולא במאגרי המידע של החברה. כמו כן נמצא כי קיימת חובה ליידוע העובדים וקבלת הסכמתו של כל עובד. לשם כך הוחלט על ניסוח מדיניות שימוש מפורטת בטכנולוגיה ושליחתה לכל העובדים. בנוסף, הוחלט כי השימוש במערכת יהיה וולונטרי בלבד. עובדים שיבחרו לא להשתמש בזיהוי באמצעי ביומטרי יוכלו להמשיך להשתמש בכרטיס רגיל – אך יידרשו להעבירו פעם נוספת במהלך היום.

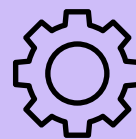
להרחבה על הנושא ראו מסמך המדיניות של הרשות להגנת הפרטיות "מדיניות בנושא איסוף ושימוש במידע ביומטרי במקום העבודה".



רצאה

בחברת היי-טק גדולה עם אוריינטציה ביטחונית התגלו מקרים רבים של דיווחי נוכחות כוזבים מצד עובדים. בעקבות זאת, הנהלת החברה שקלה לעבור לשימוש במערכת ביומטרית מבוססת זיהוי טביעת אצבע לצורך דיווח ובקרת נוכחות. הנהלת החברה פנתה להתייעצות עם הייעוץ המשפטי ועם הממונה על הגנת הפרטיות בארגון. אלו המליצו שלא למהר ביישום הטכנולוגיה, אלא תחילה לבצע תסקיר השפעה על פרטיות. במסגרת התסקיר, נבחנו ההיבטים המשפטיים והמעשיים של השימוש בטכנולוגיה לצורך דיווחי נוכחות במקום העבודה:

- נבחן והוגדר הבסיס החוקי לאיסוף מידע ביומטרי לצרכי נוכחות;
- תוארו אופן עיבוד המידע, מטרותיו, היקפו והקשרו;
- נבחנה חוקיות איסוף המידע, מידת הצורך בשימוש בטכנולוגיה, ומידת הפגיעה האפשרית בפרטיות, כתלות גם ברגישות המידע;
- נבחנו חלופות שונות לשימוש באמצעים ביומטריים;
- נערכה התייעצות עם נציגות העובדים;
- זוהו הסיכונים לפרטיות (כגון החשש לדלף המידע וכן פגיעה בתחושת השליטה של עובדים ובאוטונומיה שלהם), והאמצעים לצמצומם;
- נבחנו שיטות ואמצעים טכנולוגיים שונים המאפשרים זיהוי ביומטרי לצרכי דיווח ובקרת נוכחות.



הגדרה ומטרה

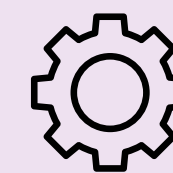


מה כדאי ללמוד



רזומה

איסוף מידע אישי



הגדרה ומטרה

שלב איסוף המידע הוא השלב בו מתבצע האיסוף בפועל של המידע האישי. בשלב זה על ארגונים להקפיד כי תהליך איסוף המידע ייעשה בהתאם להוראות הדין, ובכלל זה:

- לוודא שהמידע נאסף על בסיס חוקי – קרי מכח סמכות בדין או הסכמה תקפה של נושא המידע;
- לעמוד בחובת היידוע הקבועה בסעיף 11 לחוק הגנת הפרטיות (להרחבה – "חובת יידוע במסגרת איסוף ושימוש במידע אישי");
- להקפיד על כך שהמידע הנאסף אינו חורג מהנדרש או ממה שנושא המידע הסכים לו;
- לוודא כי איסוף המידע נעשה בצורה מוגנת, מאובטחת, ועל-פי כללי אבטחת המידע המחייבים.

הגדרה ומטרה

אם כדאי לדעת

במצב

איסוף מידע אישי



שימו לב: הפונה לאדם לקבלת מידע אישי לשם עיבוד המידע במאגר מידע ומוסר לו פרטים לא נכונים, בניגוד להוראות סעיף 11 לחוק הגנת הפרטיות בכוונה להטעותו באשר למסירת המידע האישי, דינו – מאסר שלוש שנים.



שימו לב: במקרים של פגיעה בפרטיות שלא על יסוד הסכמה או מתוקף סמכות בדין – על ארגון המבקש להסתמך על הגנות סעיף 18 לחוק לעמוד בעניין זה בדרישת המידתיות (סעיף 20(ב) לחוק הגנת הפרטיות), בכלל זה, עליו להיות מסוגל להצביע על הסיבות והאינטרסים הלגיטימיים המצדיקים, לגישתו, את פגיעתו בפרטיות נושא המידע (להרחבה – טיוטת "גילוי דעת הסכמה בדיני הגנת פרטיות").



מה כדאי לדעת

במקרה של איסוף מידע על יסוד הסכמת נושא המידע: על ארגון להקפיד כי הסכמת נושא מידע ניתנת מדעת, מתוך רצון חופשי, במפורש או באופן משתמע (להרחבה – טיוטת "גילוי דעת הסכמה בדיני הגנת פרטיות");

לממונה על הגנת הפרטיות מומלץ לבחון דרכים לחיזוק הליך ההסכמה ושליטת נושא המידע במידע על אודותיו, כגון: העדפת הסכמה מפורשת על פני הסכמה משתמעת; העדפת מנגנון של הסכמה אקטיבית ולא פסיבית; העמדת אפשרות לחזרה מהסכמה (להרחבה – טיוטת "גילוי דעת בנושא הסכמה בדיני הגנת פרטיות").

במידה שהשירות מיועד בעיקרו לאוכלוסיות מיוחדות (קטינים, אנשים עם מוגבלות) – מומלץ להתאים את תוכן ההסכמה ואת אופן הצגתה למאפיינים הייחודיים של האוכלוסייה.

הזכרת מידע

מה כדאי לדעת

הזכרת מידע

איסוף מידע אישי



לאור האמור הממונה פנתה להנהלת החברה, התריעה על הכשלים והבעיות שבהליך איסוף המידע, וייעצה לתקן את מנגנוני היידוע וההסכמה לשם עמידה בדרישות הדין ולשם חיזוק שליטתם של המשתמשים במידע על אודותיהם. הממונה המליצה על התיקונים הבאים:

- פישוט וקיצור מסמכי מדיניות הפרטיות ותיקון הקישורים ה"שבורים";
- תיקון מסמכי מדיניות הפרטיות והוספת הבהרה בדבר סוג המידע הנאסף ומטרות האיסוף ועיבוד המידע;
- שיפור נגישות עמוד הגדרות הפרטיות באפליקציה;
- שינוי מנגנון איסוף נתוני המיקום – ממנגנון של "ברירת מחדל" (Opt-out) למנגנון של הסכמה אקטיבית (Opt-in);
- הוספת נתונים ליידוע משתמשים עם התחלת השימוש ב"בוט" האפליקציה.



ממונה על הגנת הפרטיות אשר נכנסה לאחרונה לתפקידה בחברה המספקת שירותי אימוני כושר מקוונים ומשווקת מוצרי בריאות לספורטאים חובבנים, החלה בבחינת אופן איסוף המידע בארגון.

במהלך הבדיקה התברר לממונה כי מסמכי מדיניות הפרטיות ותנאי השימוש של החברה הם ארוכים, מנוסחים בצורה לא ברורה, וכוללים קישורים "שבורים" שאינם פעילים. כמו כן, התברר לה כי המסמכים אינם מציינים בצורה ספציפית אילו סוגי מידע עשויה החברה לאסוף, ולאילו מטרות.

בנוסף, בבדיקתה את האפליקציה של החברה, מצאה הממונה כי הגדרות הפרטיות אינן נגישות למשתמשים, באופן המקשה עליהם לשלוט באיסוף המידע עליהם. כמו כן, בהגדרות הפרטיות נמצא כי האפליקציה אוספת נתוני מיקום של משתמשים במתכונת של "ברירת מחדל", כך שמי שמבקש להימנע מאיסוף זה צריך לפעול באופן יזום ולבקש שהנתונים לגביו לא יאספו (Opt-out).

בנוסף, במהלך הבדיקה התברר לממונה כי החברה גם אוספת מידע אישי ממשתמשים פוטנציאליים המתנסים לראשונה באפליקציה (כגון גיל, משקל וכתובת) באמצעות 'בוט', וזאת מבלי להציג בפניהם את המידע הנדרש לצורך יידועם, כנדרש על-פי הוראות סעיף 11 לחוק הגנת הפרטיות והנחיות הרשות להגנת הפרטיות בנושא.

הזכרת מידע

אם כדאי לדעת

המידע

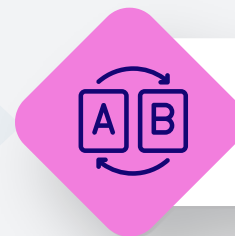
איסוף מידע אישי



אחסון מידע



הגדרה



מה כדאי לשלוח?



רצחנה



הגדרה



שלב אחסון המידע מיוחס לשלב קבלת המידע ושמירתו במאגרי מידע, וזאת מרגע איסופו ולאורך כל תקופת החזקתו על-ידי הארגון.

בשלב זה על הארגון להקפיד, בין היתר:

- על שמירת המידע האישי במאגרי מידע בהתאם למטרות המאגר;
- על אבטחתו של המידע בהתאם לדרישות הדין;
- על בדיקה עיתית בדבר קיומו של מידע עודף במאגר;
- על העמדת זכות העיון וזכות התיקון לנושאי המידע, בהתאם לקבוע בהוראות הדין.



הגדרה

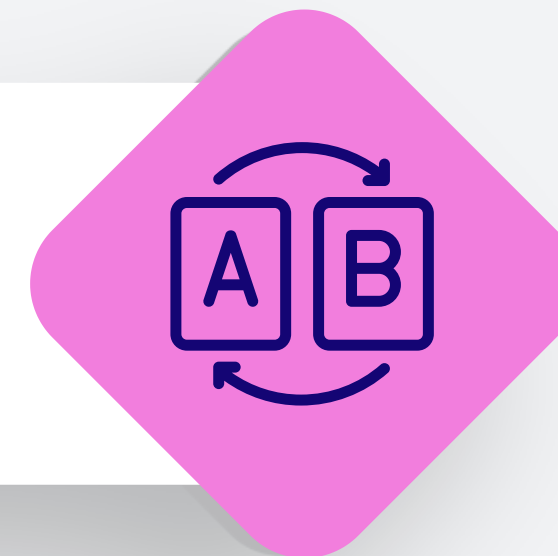
אחסון מידע



מה כדאי לדעת?



דגימה



מה כדאי לדעת? #1

על ארגון המחויב ברישום מאגרי מידע לפעול לרישום המאגרים שבשליטתו, או לחלופין למסירת הודעה לרשות על מאגר מידע שבו מידע בעל רגישות מיוחדת על 100,000 איש ומעלה, והכל בהתאם לנסיבות ולהוראות סעיף 8א לחוק הגנת הפרטיות (להרחבה: "רישום מאגר מידע" ; "שליחת הודעה לרשות על מאגר מידע" – באתר הרשות להגנת הפרטיות).

עם איסוף המידע, ולאורך כל תקופת החזקתו, על ארגון לוודא כי מאגרי המידע מוגנים ומאובטחים בהתאם לדרישות תקנות אבטחת מידע, התשע"ז-2017 (להרחבה – "מדריך אבטחת מידע");

על ארגון לדווח מידית לרשות להגנת הפרטיות מיד עם קרות אירוע אבטחה חמור, כהגדרתו בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להרחבה ראו אתר הרשות להגנת הפרטיות);

על ארגון לבחון, לפחות אחת לשנה, אם אין הוא מחזיק מידע עודף, כלומר שהמידע שהוא שומר במאגר אינו רב מן הנדרש למטרות המאגר (תקנה 2(ג) לתקנות אבטחת מידע, התשע"ז-2017). (להרחבה – טיוטת "מסמך מדיניות בנושא צמצום מידע (Data Minimization)").



הגדרה

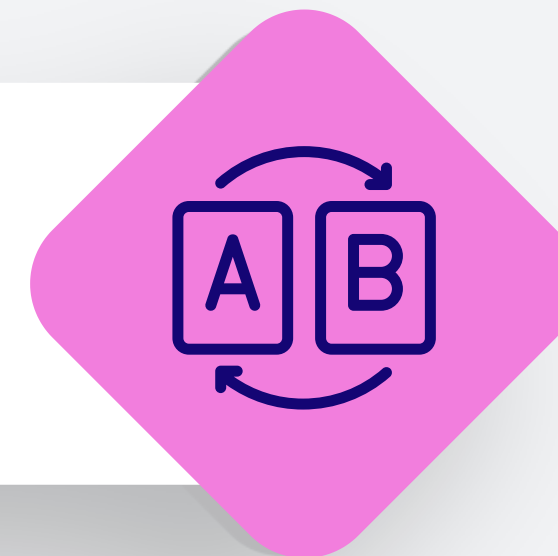
אחסון מידע



מה כדאי לדעת?



דגימה



מה כדאי לדעת #2

על ממונה על הגנת הפרטיות להכין תוכנית לבקרה שוטפת על העמידה בהוראות חוק הגנת הפרטיות לגבי מאגרי מידע, לוודא כי היא מבוצעת, לדווח להנהלת החברה על ממצאיו ולהציע הצעות לתיקון הליקויים (סעיף 17ב2(א)(2) לחוק הגנת הפרטיות).

על ממונה על הגנת הפרטיות לוודא קיומם של נוהל אבטחת מידע ומסמך הגדרות מאגר (סעיף 17ב2(א)(3) לחוק הגנת הפרטיות).

על ארגון לפעול להעמדת זכות העיון במידע אישי והזכות לבקש תיקון מידע בהתאם לקבוע בהוראות הדין (סעיפים 13 ו-14 לחוק הגנת הפרטיות).

על ממונה על הגנת הפרטיות לוודא טיפול בפניות של נושאי מידע שמידע אישי על אודותיהם נמצא במאגר המידע (סעיף 17ב2(א)(4) לחוק הגנת הפרטיות).

בשלב אחסון המידע מומלץ לעשות שימוש בטכנולוגיות מגבירות פרטיות לשם ערפול המידע האישי הנשמר וצמצום רמת הפירוט שלו (בין היתר על ידי הסרת פרטים מזהים, שינוי הנתונים, טשטוש הערכים המדויקים או הוספת "רעש"), וכן למניעת נגישות למידע ללא הרשאה, וחיזוק הליכי התייעוד והשקיפות בנושא (להרחבה ראו "מדריך לטכנולוגיות מגבירות-פרטיות").



הזכרה

אחסון מידע



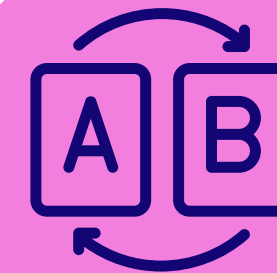
מה כדאי לדעת?



דואמה



מה כדאי לדעת? #3



שימו לב: על דירקטוריון הארגון לוודא גיבוש, אימוץ ויישום של מדיניות בדבר אופן ביצוע דרישות החוק והתקנות בארגון, לרבות חובת הדיווח המיידית לרשות להגנת הפרטיות על קרות אירועי אבטחת מידע חמור.



בנוסף על הדירקטוריון לקיים דיון במסמך הגדרות המאגר, בעקרונות המרכזיים של נוהל אבטחת המידע הארגוני, בתוצאות סקר הסיכונים ומבדקי החדירות שהארגון ביצע ובפעולות הנדרשות לתיקון, באירועי אבטחת המידע שהתרחשו בארגון, ובתוצאות הביקורת התקופתית בנוגע לעמידה בתקנות.

(להרחבה ראו הנחית הרשות להגנת הפרטיות מס' 1/2024 "תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע)").



הגדרה

אחסון מידע



מה כדאי לדעת?



דגימה



צוואה



לאחר כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות התקבלה במשרדי חברת השמה בקשה של אדם לעיין במידע על אודותיו השמור במאגרי המידע של החברה.

הפנייה הגיעה לידיעתו של הממונה על הגנת הפרטיות בחברה, אשר דאג כי היא תטופל. לאחר שקיבל את המידע פנה הפונה שוב לחברה וביקש את מחיקתו של המידע על אודותיו ממאגרי המידע בטענה שהוא לא מעודכן, ובהתאם להנחית הרשות להגנת הפרטיות מס' 2/2012 בנושא "תחולת הוראות חוק הגנת הפרטיות על הליכי מיון לקבלה לעבודה ופעילות מכוני מיון". לאחר קבלת הבקשה ובחינתה פנה הממונה על הגנת הפרטיות לגורם הרלוונטי בחברה וייעץ למחוק את המידע.

לאור הפנייה ערך הממונה בדיקה כוללת בעניין מדיניות החברה בנושא מידע עודף. במסגרת הבדיקה התברר לממונה כי החברה אינה מקפידה על יישום הנחיות הרשות בנושא, וכלל אינה בוחנת האם היא מחזיקה מידע עודף במאגריה.

לאור האמור ביקש הממונה להציג בפני הנהלת החברה את הנחיות הרשות בנושא, וחידד בפניהם את החובה המוטלת על ארגונים לבחון ולוודא, אחת לשנה, כי הם אינם מחזיקים מידע עודף במאגריהם. בנוסף, הממונה עדכן את תוכנית הבקרה השוטפת של התנהלות החברה בנושא תוך שהוא מדגיש את הנחיות הרשות ודרישות הדין בעניין זה, וכן כלל את הנושא במסגרת תוכנית ההדרכה לעובדי החברה.



האזרה

אחסון מידע



מה כדאי לדעת?



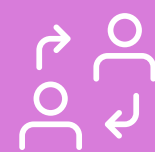
צוואה



עיבוד מידע



דוגמה



מה כדאי לעשות?



הגדרה ומטרה



הגדרה ומטרה

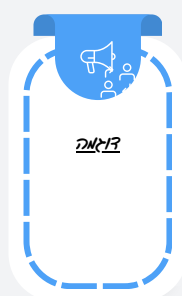
עיבוד מידע אישי הוא "כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו או מתן גישה אליו" (סעי' 3 לחוק הגנת הפרטיות).

שלב עיבוד המידע הוא השלב בו המידע האישי עובר תהליכים של עיבוד, ניתוח, וארגון בהתאם למטרות שנקבעו מראש והוצגו על-ידי הארגון. תהליך עיבוד המידע יכול לכלול, בין היתר, פילוח קהלי יעד, הפקת תובנות עסקיות, וכן העברת המידע לצדדים שלישיים.

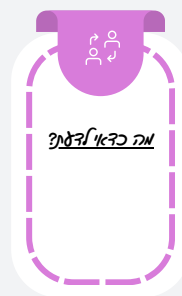
יובהר כי כללי אבטחת המידע חלים גם על שלב זה.



עיבוד מידע



קליטה



מה כדאי לדעת?



הגדרה ומטרה



מה כדאי לדעת?

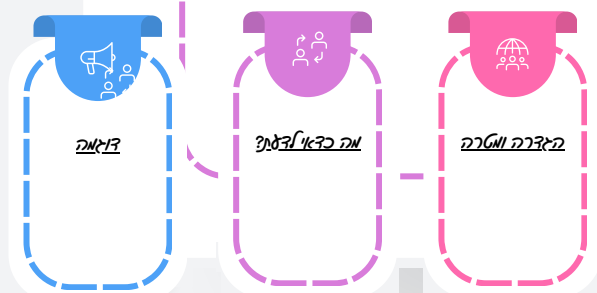
חל איסור לעבד מידע אישי ממאגר מידע ללא הרשאה מאת בעל השליטה במאגר או בחריגה מהרשאה שכזו (סעיף 8(ג) לחוק הגנת הפרטיות).

ארגון רשאי לעבד מידע אישי במאגר מידע רק למטרה החוקית לשמה נאסף המידע מלכתחילה (סעיפים 2(9) ו- 8(ב) לחוק הגנת הפרטיות).

העברת מידע לגורם מחוץ לארגון – אפשרית רק בהתאם להסכמת נושא המידע או מתוקף סמכויות וחובות שמכח הוראות הדין, כולל הגנות סעיף 18 לחוק הגנת הפרטיות.

על ארגון חל איסור לעבד מידע אישי או לתת הרשאה לאחר לעבד מידע אישי, אם המידע התקבל, נצבר או נאסף בניגוד להוראות חוק הגנת הפרטיות או להוראות כל דין אחר המסדיר עיבוד מידע (סעיף 8(ד)(1) לחוק הגנת הפרטיות).

עיבוד מידע





מה כדאי לדעת?

#2

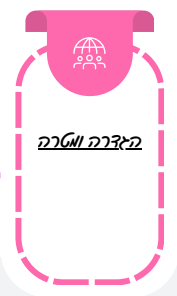
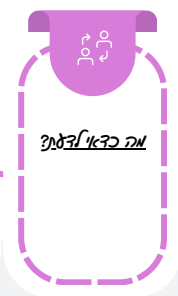
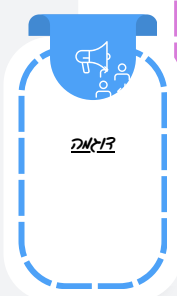
היעזרות בנותני שירותים חיצוניים דרך מיקור חוץ (ספקים) – צריכה להתבצע בהתאם להוראות תקנה 15 לתקנות אבטחת מידע, התשע"ז-2017. להרחבה: מדריך פעולה להתקשרות עם ספקי מיקור חוץ - תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע).

מומלץ לעשות שימוש בטכנולוגיות מגבירות פרטיות לשם צמצום החשיפה של המידע האישי במהלך עיבודו, כדוגמת טכנולוגיות בתחום ההצפנה ההומומורפית וחישוב רב-משתתפים. להרחבה ראו "מדריך לטכנולוגיות מגבירות-פרטיות".

על ממונה הגנת פרטיות להכיר את תהליכי העבודה הארגוניים ובכלל זאת להבין איך העובדים בארגון ניגשים למידע אישי במאגר ומבצעים בו פעולות שונות.

בקשת נושא מידע לחזרה מהסכמה עשויה, במקרים מסוימים, לחייב את הארגון לקבל את הבקשה, ולהביא להפסקת עיבוד המידע על אודותיו. להרחבה: טיוטת "גילוי דעת בנושא הסכמה בדיני הגנת פרטיות".

עיבוד מידע



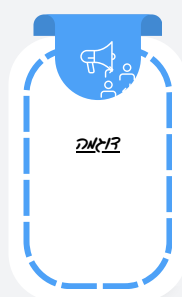


מה כדאי לדעת?
#3

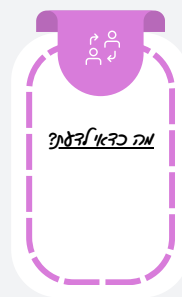
שימו לב: שימוש במידע בניגוד למטרה לשמה נמסר; גילוי מידע לאחר והפרת חובת הסודיות של עובד, מנהל או מחזיק; עיבוד מידע ללא הרשאה מבעל המאגר; ומסירת מידע מעובד של גוף ציבורי לעיבוד ע"י גורם לא מוסמך, מהווים עבירות שסנקציה פלילית בצידן.

שימו לב: כאשר יש לרשות להגנת הפרטיות יסוד סביר להניח כי מתבצעת או עומדת להתבצע במאגר מידע הפרה של הוראות לפי סעיפים 2(9), 8(ב), (ג), (ד), 17 או 23ב, רשאית היא לבקש מבית המשפט לעניינים מינהליים להוציא נגד הארגון צו להפסקת פעולות עיבוד המידע האישי הגורמות להפרה או שיש חשש שיגרמו להפרה, כולל צו למחיקת המידע (להרחבה ראו סעיף 23מט לחוק הגנת הפרטיות).

עיבוד מידע



דאטה



מה כדאי לדעת?



האזרה ומערכה



צהל

חברה המעניקה שירותי תיווך מפרסמת באתר האינטרנט שלה המלצות מטעם לקוחות מרוצים. ההמלצות, הכוללות פרטים אישיים של לקוחות (כגון שמם, כתובתם ותמונותיהם) מפורסמות באתר החברה בהסכמת הלקוחות.

לאחר פניית לקוחה לחברה, בה היא הביעה חשש כי חברה המבצעת "כריית מידע" מהרשת (Scarping) משתמשת במידע מההמלצות לשם פרסום ממוקד ושיווק מוצרים, המליצה הממונה על הגנת הפרטיות בחברה להוסיף הבהרה באתר האינטרנט ובמסמך תנאי השימוש כי המידע מפורסם באתר רק למטרת הצגה של חוות דעת לקוחות, וכי אין לעשות במידע כל שימוש למטרות אחרות. להרחבה בנושא ראו טיוטת הנחיית הרשות להגנת הפרטיות בנושא "תחולת חוק הגנת הפרטיות על מערכות בינה מלאכותית" (סעיף 6.3.5 להנחיה).

בנוסף, במסגרת הטיפול בפנייה התברר לממונה כי חברת התיווך העבירה במשך שנים מידע על אודות לקוחותיה לחברה לשיווק רהיטים, מבלי לקבל את הסכמת הלקוחות לכך, כחלק מהתקשרות עסקית בין החברות. מיד כשנודע לה על כך פנתה הממונה להנהלת החברה וייעצה לה להפסיק את העברת המידע או לפנות ללקוחותיה בבקשה לקבלת הסכמתם לכך.

עיבוד מידע



צהל



ועד כדאי לדעת?



האזרה ושמירה



סיום חיי המידע



רזימה



מה כדאי לדעת?



הגדרה ומטרה



הגדרה ומטרה

שלב סיום חיי המידע מיוחס לשלב סיום השימוש וההחזקה של מידע אישי. שלב זה עשוי להתקיים במגוון נסיבות, כגון:

- כאשר המידע האישי (כולו או חלקו) אינו נדרש עוד למטרות שלשמן נאסף;
- כאשר הסתיים התוקף החוקי להחזקתו של מידע אישי (אם היה כזה);
- כאשר הארגון החליט למחוק את המידע בעקבות בקשת נושא המידע לתיקון או למחיקת המידע לפי סעיף 14 לחוק הגנת הפרטיות;
- כאשר הוחלט על גריסה ו"סיום חיים" של כלי טכנולוגי המכיל מידע אישי;
- כאשר התקבלה הוראה חוקית המחייבת את הארגון במחיקת המידע.
- בהתאם לנסיבות, בשלב זה עשוי הארגון למחוק את המידע (כולו או חלקו) ממאגרי המידע (לרבות גיבויים), או לנקוט באמצעים טכנולוגיים לצמצומו וערפולו.

סיום חיי המידע



צמצום



מה בדאי לצאת?



הגדרה ומטרה



מה כדאי לדעת?

שימו לב: כאשר יש לרשות להגנת הפרטיות יסוד סביר להניח כי מתבצעת או עומדת להתבצע במאגר מידע הפרה של הוראות לפי סעיפים 2(9), 8(ב), (ג), (ד), 17 או 23ב, רשאית היא לבקש מבית המשפט לעניינים מינהליים להוציא נגד הארגון צו למחיקת המידע האישי שבמאגר המידע במלואו (להרחבה ראו סעיף 23מט לחוק הגנת הפרטיות).

בהתאם לנסיבות מומלץ להשתמש בטכנולוגיות מגבירות פרטיות לשם ערפול המידע האישי שנדרש להישמר במאגרי המידע גם לאחר סיום השימוש בו, לדוגמה באמצעות התממתו.

להרחבה ראו "מדריך לטכנולוגיות מגבירות-פרטיות".

סיום חיי המידע



צאמה



מה כדאי לדעת?



ביצירה ומארה



רצח

בעקבות פניית הממונה הכון הוצא מהמכשיר ונשלח לגורם מוסמך לביצוע השמדה מאובטחת של מדיה מגנטית, וזאת לאחר וידוא כי המידע עצמו נשמר, בהתאם להוראות הדין, במאגרי המידע הדיגיטליים של בית החולים. התהליך תועד בפרוטוקול מסודר, כולל מספר סידורי של הכון, תאריך ביצוע, חתימת הגורם המבצע, והעתק אישור השמדת המידע.

רק לאחר "ניקוי" המכשיר ממידע אישי, הועבר המכשיר לידי הקליניקה הפרטית.

בבית חולים במרכז הארץ הוחלט להוציא מכלל שימוש מכשיר דימות (מערכת שיקוף רנטגן דיגיטלית) ששירת את המחלקה האורתופדית בבית החולים במשך יותר מעשור. המכשיר תיעד מאות אלפי צילומים רפואיים, אשר חלקם עדיין נשמרו בכון הקשיח הפנימי שלו, לצד פרטים מזהים של מטופלים כגון שמות, מספרי תעודות זהות, תאריכי לידה ואבחנות רפואיות.

בית החולים תכנן למכור את מכשיר הדימות לקליניקה פרטית. המקרה הגיע לידיעתו של ממונה הגנה על הפרטיות בבית החולים מספר שעות בלבד לפני פירוקו הפיזי של ציוד הרנטגן הישן והעברתו. ממונה הגנת הפרטיות ביקש את דחיית ביצוע הפעולה עד לטיפול במידע האישי שבכון המכשיר.

סיום חיי המידע



רצח



מה כדאי לדעת?



ביצירה ומערכה