

הגנת הפרטיות
הגדרת מידע אישי

1 מתוך 10

הוראת עבודה: הגנת פרטיות <> הגדרת מידע אישי

מהדורה: 1

נרשם ע"י: גבי בר יוסף	תאריך: יולי 2020
עודכן: גל יצחק, CISO	תאריך: יולי 2023

1. תוכן

1	תוכן	1
2	מטרה	2
2	מסגרת	3
2	אחריות	4
2	מסמכים מקושרים	5
3	מונחים והגדרות (על פי החוק הישראלי להגנת פרטיות)	6
4	הגדרת מידע אישי	7
4	מה הבסיס להגדרה של מידע אישי?	4
5	מהי ההגדרה המדויקת של מידע אישי?	5
5	"מידע" "מידע אישי" "מידע אישי רגיש" ?	5
5	על מה בא החוק להגן?	5
6	הגדרת החוק האירופי למידע אישי (GDPR)	8
7	דוגמאות למידע אישי ומידע אישי רגיש	9
8	הגדרת מידע אישי – מורכבות ושיקול דעת	10
9	הנחיות וכללים באיסוף מידע אישי	11
10	זכויות נושאי המידע	12
10	סיכום	13

הגנת הפרטיות הגדרת מידע אישי

2 מתוך 10

הוראת עבודה: הגנת פרטיות <> הגדרת מידע אישי

מהדורה: 1

2. מטרה

מסמך זה הוא חלק ממכלול הנהלים של אוניברסיטת תל אביב, הבאים להגדיר את חובות הארגון ואת האמצעים הנדרשים על מנת לאבטח מידע אישי הנמצא ברשות הארגון בהתאם לחוקי הגנת הפרטיות.

חוקי הגנת הפרטיות נועדו, בין היתר, להגן על מידע אישי של אזרחים אשר אינו נמצא ברשותם. בעידן הדיגיטלי של ימינו מידע אישי אשר נמצא, נשמר ומועבר במערכות מידע, מחייב עמידה בדרישות חוק הגנת הפרטיות ובתקנות הגנת הפרטיות (אבטחת מידע).

כדי לעמוד בדרישות החוק יש להגן על "מידע אישי".

מטרת מסמך זה היא להגדיר באופן ברור ומפורט מה המשמעות של "מידע אישי" כדי:

- לעמוד בדרישות החוק.
- להבהיר את אופן הפעולה (שמירת מידע, העברת מידע, מחיקה, עדכון וכו') במערכות בהן נמצא מידע אישי.

3. מסגרת

מסמך זה מיועד עבור אוניברסיטת תל אביב ועובדיה.
מסמך זה מתייחס לכל המסמכים והמערכות של אוניברסיטת תל אביב אשר מכילים מידע אישי.

4. אחריות

מנהל אבטחת המידע והסייבר (CISO) של הארגון אחראי על מסמך זה, עדכנו ואכיפתו.

5. מסמכים מקושרים

- נוהלי אבטחת מידע
- נוהלי הגנת פרטיות

הגנת הפרטיות הגדרת מידע אישי

3 מתוך 10

הוראת עבודה: הגנת פרטיות <> הגדרת מידע אישי

מהדורה: 1

6. מונחים והגדרות (על פי החוק הישראלי להגנת פרטיות)

- **מידע** - נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.
- **מאגר מידע** - אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב.
- **שלמות מידע** - זהות הנתונים במאגר מידע אל המקור שממנו נשאבו, בלא ששוננו, נמסרו או הושמדו ללא רשות כדין.
- **מנהל מאגר** - מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה.
- **דיוור ישיר** - פנייה אישית לאדם בהתבסס על השתייכותו לקבוצת אוכלוסין שנקבעה על פי אפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע.
- **נושא מידע** - אדם הניתן לזיהוי במערכות מידע, במישרין או בעקיפין, בייחוד על ידי שיוך לזיהוי כגון שם, מספר זיהוי, נתוני מיקום, זיהוי מקוון או מאפיינים מיוחדים אחרים, שהם ביטוי לזהות הפיזית, הפיזיולוגית, הגנטית, הנפשית, הכלכלית, התרבותית או החברתית של אדם זה (הווה אומר: כל המידע המתייחס לאדם מזוהה או ניתן לזיהוי).

הגנת הפרטיות הגדרת מידע אישי

4 מתוך 10

הוראת עבודה: הגנת פרטיות <> הגדרת מידע אישי

מהדורה: 1

7. הגדרת מידע אישי

מה הבסיס להגדרה של מידע אישי?

הזכות לפרטיות מעוגנת בחוק יסוד: כבוד האדם וחירותו כזכות חוקתית. כפועל יוצא מכך הזכות לפרטיות חלה על מידע אישי. הגדרה של מידע אישי אם כן מסתמכת על הגדרות החוק במדינת ישראל.

החוקים במדינת ישראל אשר מתייחסים למידע אישי ועליהם נסמך נוהל זה:

- חוק הגנת הפרטיות התשמ"א – 1981
- תקנות הגנת הפרטיות (אבטחת מידע) – 2017
- תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה) – 2001

התייחסות נוספת להגדרה של מידע אישי נכללת בהנחיות ובתקנות הבאות ונוהל זה מביא בחשבון גם מסמכים הבאים:

- הנחיות רשם מאגרי מידע מס 2012\4 שימוש במצלמות אבטחה ומעקב ובמאגרי תמונות הנקלטות בהן.
- הנחיית רשם מאגרי מידע מספר 2/2017 - פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר.
- תקנות הגנת הפרטיות האירופאיות – 2017 GDPR - General Data Protection Regulation

חוקי הפרטיות מתייחסים להגנה על הפרטיות וגם להגנה על מידע אישי בעולם הדיגיטלי. מסמך זה עוסק בהגדרת מידע אישי בעולם הדיגיטלי. הגדרת המידע האישי היא הבסיס לניהול המידע במערכות המידע של הארגון. על פי ההגדרה זו יש להתייחס לפרטי מידע הנשמרים במאגרי הנתונים של הארגון. פועל יוצא של הגדרה זו יהיו אמצעי האבטחה שינקטו במאגרי המידע אשר מכילים מידע אישי או מידע אישי רגיש.

חוקי הגנת הפרטיות (ולכן גם מסמך זה) מתייחסים למידע לגבי אנשים חיים בלבד. חוקי הגנת הפרטיות של מדינת ישראל באים להגן על המידע שמשויך לאזרחי מדינת ישראל החיים. מידע אירגוני או נכסים אינטלקטואלים של הארגון אינם נכללים בהגדרות החוק. יחד עם זאת מומלץ לנהוג בהם על פי אותם כללים של אבטחת מידע כדי להגן עליהם מדליפה או מחיקה.

הגנת הפרטיות הגדרת מידע אישי

5 מתוך 10

הוראת עבודה: הגנת פרטיות <> הגדרת מידע אישי

מהדורה: 1

מהי ההגדרה המדויקת של מידע אישי?

החוק הישראלי להגנת הפרטיות מגדיר באופן הבא את המידע אליו הוא מתייחס:

"מידע" - נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו;

"מידע רגיש" –

1. נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו;
2. מידע שישר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש;

"מידע" "מידע אישי" "מידע אישי רגיש" ?

במסמך זה נתייחס למונחים "מידע אישי" ו"מידע אישי רגיש" ונסביר את אופן ההתייחסות הנדרש לפריטי מידע אישיים במערכות המידע הארגון.

הגדרת החוק למונח "מידע" מתייחסת ל"מידע אישי" והגדרת החוק למונח "מידע רגיש" מתייחסת ל"מידע אישי רגיש", מאחר והחוק להגנת פרטיות עוסק במידע על בני אדם ההתייחסות בו היא למונח "מידע" כאשר הכוונה היא למידע אישי – נתונים פרטיים על האדם (נושא המידע).

על מה בא החוק להגן?

החוק בא להגן על מידע אישי ומידע אישי רגיש אשר נשמר במאגרי מידע. החוק מגדיר **מאגר מידע** כאוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב.

פועל יוצא מכך היא שיש אחריות לגוף אשר מנהל את מאגר המידע ולכן הוגדר על ידי החוק מנהל מאגר: "**מנהל מאגר**" - מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה.

מנהל מאגר אחראי בעיני החוק בין היתר לוודא שהמידע האישי הנמצא במאגר עומד בכללי אבטחת מידע:

- נשמר בשלמות ובדייקנות
- נגיש רק למי שמורשה לכך

תכולת האחריות של מנהל המאגר נמצאת בהוראת עבודה מינוי מנהל מאגר (חלק מנוהלי הגנת הפרטיות של היחידה לאבטחת מידע של אוניברסיטת תל אביב).

יש לשים לב שהחוק מגדיר גם את המונח "**שלמות המידע**" עליו מופקד מנהל המאגר וזאת כדי לוודא שהמאגר יהיה מדויק וישמור בהקפדה על אופן הלקוחות ויגן על המידע משינויים ואי דיוקים.

8. הגדרת החוק האירופי למידע אישי (GDPR)

מעצם היות הארגון ממוקמת בישראל ההגדרה של מידע אישי מסתמכת על החוק הישראלי, יחד עם זאת כאשר בוחנים את ההגדרה של מידע אישי ואת חוקי הפרטיות מומלץ להתייחס גם ל-GDPR – תקנות הגנת הפרטיות האירופאיות.

יש להתייחס גם להגדרת החוק האירופי ה-GDPR מהסיבות הבאות:

- הארגון נדרשת לעיתים קרובות לחתום על הסכמים עם גורמים באירופה. הסתמכות על הגדרות של האיחוד האירופי בנושאי פרטיות תקל על אישור הסכמים אלו ותאפשר לארגון להתחייב על פרטיות המידע.
- בהגדרה של ה-GDPR יש מענה רחב יותר להגדרה ולאבטחה של המידע האישי.

ב-2017 קבע האיחוד האירופי תקנות להגנת פרטיות ה-GDPR אשר הפכו לסטנדרט דה-פאקטו ברחבי העולם בנושא הגנת הפרטיות.

על פי ה-GDPR מידע אישי "כל מידע שאפשר לייחס לאדם מזוהה או בר-זיהוי"

(Any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person)

ה-GDPR גם יצר את המונח "Data subject" כלומר "נושא מידע", דהיינו הישות שאליה המידע האישי משויך. יש לשים לב שזו הגדרה כוללת ורחבה יותר מהגדרת החוק הישראלי. היא אינה תוחמת את הפרטים המגדירים מהו מידע אישי ומכילה כל נושא הנוגע בבני אדם.

אי לכך במקרים בהם יש התלבטות לגבי ההגדרה של נתונים כנתונים אישיים במאגרי נתונים, מומלץ לבחון את הנושא גם על פי ה-GDPR ולהשתמש בהגדרה של ה-GDPR לצורך הגדרת מידע המחייב התייחסות כמידע אישי.

הגנת הפרטיות הגדרת מידע אישי

7 מתוך 10

הוראת עבודה: הגנת פרטיות <> הגדרת מידע אישי

מהדורה: 1

9. דוגמאות למידע אישי רגיש

על מנת להמחיש את המשמעות של מידע אישי רגיש מובאות להלן מספר דוגמאות. נדגיש בזאת שאלו דוגמאות בלבד וניתן למצוא דוגמאות רבות אחרות. בכל ספק לגבי פריט מידע (האם הוא מוגדר מידע אישי רגיש) יש להתייחס להגדרות דלעיל.

הרשימה מטה כוללת דוגמאות להמחשת המושג מידע אישי רגיש:

שם ושם משפחה לבדם אינם מוגדרים כמידע רגיש. אך שילוב של השם המלא עם אחד מהבאים - יוגדר כמידע רגיש:

- מספר תעודת זהות
- כתובת דואר אלקטרונית

ובנוסף:

- מידע על צנעת חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד
- מידע רפואי או מידע על מצבו הנפשי של אדם
- מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א-2000
- חברות באיגודים מקצועיים
- מידע אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם
- מידע על אודות עברו הפלילי של אדם
- נתוני מיקום
- מידע ביומטרי
- מידע על נכסיו של אדם
- חובותיו והתחייבויותיו הכלכליות
- מצבו הכלכלי או שינוי בו
- יכולתו לעמוד בהתחייבויותיו הכלכלית ומידת עמידתו בהם
- הרגלי צריכה של אדם שיש בהם כדי ללמד על מידע לפי פרטים או על אישיותו של אדם, אמונתו או דעותיו
- נטייה מינית
- תמונות וידאו
- כתובת IP

הערה:

לפי [הגדרת חוק הגנת הפרטיות](#) 1996 למידע ומידע רגיש ניתן להניח כי שם וכתובת אינם נחשבים מידע אישי "אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף". חשוב לציין ש:

- א. האוניברסיטה כתאגיד שברשותו מאגרי מידע נוספים חייבת להתייחס גם לשמות כתובות ומייל כמידע אישי.
- ב. פרטים אישיים הללו נכללים במסגרת דרישות רגולטוריות בינלאומיות דוגמת ה-GDPR שגם אליהם האוניברסיטה מחויבת מכוח הסכמים בין-אוניברסיטאיים.

הגנת הפרטיות הגדרת מידע אישי

8 מתוך 10

הוראת עבודה: הגנת פרטיות <> הגדרת מידע אישי

מהדורה: 1

10. הגדרת מידע אישי – מורכבות ושיקול דעת

מידע אישי אשר נאגר במאגרי מידע מחייב התייחסות זהירה ושיקול דעת באיסוף המידע:

פריט מידע בודד בפני עצמו אינו בהכרח מידע אישי אך כאשר נאספים מספר פריטי מידע המידע הופך לאישי ולעיתים אף למידע אישי רגיש. לכן יש לקחת בחשבון את ההקשרים בין פרטי המידע אשר נאספים ולבחון בהליך התכנון של המאגר את הנתונים הנאספים.

להלן דוגמאות לצורך המחשה:

- כאשר יש נתונים אנונימיים על סטודנטים בקורס מסוים כוללים נתוני גיל אזי גם אם יש שני אנשים בני חמישים יהיה קל לזהות אותם גם אם לא יודעים את שמם אלא רק את הגיל שלהם. בדוגמה זו ניתן לראות שגם אם המידע הוא אנונימי לכאורה – עדיין שילוב של שני פרטי מידע מאפשר זיהוי.
- נתוני צריכת דלק של מנוע סילון נשלחים באופן מידי ממערכות המחשב של המנוע למאגרי המידע של יצרן המנוע, ומשם לאחר עיבוד מועברים לחברת התעופה, בחברת התעופה יודעים את שעות הטיסה ואת המטוס הקיים ועל פי נתונים אלו ידוע מי הטייס של המטוס ומה צריכת הדלק של המטוס שהוא מטיס. הדבר משליך על נתוני ההעסקה של הטייס – חברת התעופה תעדיף טייס עם צריכת דלק נמוכה. בדוגמה זו פריט מידע שאינו קשור לגורם אנושי כלל, נתוני צריכת דלק הופכים להיות מידע אישי רגיש ברגע שניתן לקשר אותם באמצעות מערכות מידע לגורם אנושי.

לכן בתהליך תכנון או עדכון של מאגר מידע יש לבחון את כל הפרטים הנשמרים, ובמידה ופרטים מסוימים עשויים להשליך על בעל מידע אנושי, יש לנוהג במידע כמידע אישי, לפעול בהתאם לנוהלי הגנת הפרטיות של היחידה לאבטחת מידע של הארגון, ובכלל זה להצפין את המידע במאגר, ולהעביר את המידע רק דרך תווך מוצפן.

הגנת הפרטיות הגדרת מידע אישי

9 מתוך 10

הוראת עבודה: הגנת פרטיות <> הגדרת מידע אישי

מהדורה: 1

11. הנחיות וכללים באיסוף מידע אישי

חובה על כל גוף בארגון אשר בונה או מחזיק או מנהל מאגר מידע המכיל מידע אישי, לאמץ את הכללים הבאים:

- ידיעה והסכמה: יש לוודא שאדם עליו נאסף המידע האישי יודע שהמידע עליו נאסף והוא מאשר את איסוף המידע. ההסכמה חייבת להיות "הסכמה מדעת":
 - האדם קבל הסבר מדויק לגבי פרטי המידע שנאסף
 - אופן איסוף המידע
 - מטרת איסוף המידע
 - מי נחשף למידע
 - כמה זמן המידע נשמר
 - היכן המידע נשמר (במסגרת גבולות המדינה או מחוצה לה)
 - מה זכויותיו
- תיעוד:
 - יש לתעד (אלקטרונית) את ההסכמה של נושא המידע לשתף במידע.
 - יש לתעד כל עדכון או מחיקה של פרטי מידע אישי.
- הסיבה לאיסוף מידע:
 - יש להגדיר בכתב מה הצורך עבורו נאסף מידע אישי (למעט מערכות ארגוניות, בכפוף לצרכים הארגוניים).
 - אין לאסוף פריטי מידע שלא לצורך.
- יש להגדיר מועד מחיקה של פרטי מידע אישי (לא מומלץ לשמור מידע ללא הגדרת מועד הסרה).
- הצפנה: מידע אישי ישמר באופן מוצפן במאגר המידע ויעובר על גבי תשתית רשת מוצפנת בלבד.

מידע מפורט ניתן למצוא בנוהלי היחידה לאבטחת מידע של הארגון או אצל הממונה על אבטחת המידע
בכתובת המייל: infosec@tauex.tau.ac.il

הגנת הפרטיות הגדרת מידע אישי

10 מתוך 10

הוראת עבודה: הגנת פרטיות <> הגדרת מידע אישי

מהדורה: 1

12. זכויות נושאי המידע

- נושאי המידע האישי הינם האנשים עליהם נאסף המידע: סטודנטים, אנשים המשתתפים במחקר, עובדי ארגון וכו'.
- לנושאי המידע יש זכויות לגבי המידע שלהם גם אם הוא לא ברשותם (יש להתייחס למידע שלהם כנתונים שהושאלו לארגון לצורך ביצוע פעילות מוגדרת מראש).
- מנהלי מאגרי מידע חייבים להיות מודעים לזכויות נושאי המידע ולתת להם מענה כחלק מהשירותים של מאגרי המידע:
- **זכות העיון:** אדם רשאי לצפות במידע אשר נאסף עליו.
 - **זכות לתיקון ומחיקה:** אדם זכאי לבקש לתקן או למחוק את המידע שנאסף עליו אם הוא שגוי או לא מעודכן.

13. סיכום

מסמך זה הינו חלק מנוהלי היחידה לאבטחת מידע בארגון ובאחריות מנהלת אבטחת המידע (CISO) של הארגון.

המסמך מגדיר את כללי היסוד לשמירה ושימוש במידע אישי במערכות הארגון.

כל שינוי בהגדרות המסמך מחייב אישור מנהלת אבטחת המידע של הארגון.

בכל שאלה או התלבטות בנוגע להגדרות של מידע אישי או התייחסות לשמירה על מידע אישי במאגרי מידע, נא לפנות למנהלת האבטחה של אוניברסיטת תל אביב בכתובת המייל:

infosec@tauex.tau.ac.il