# נוהל: ניהול מאגרי מידע על פי חוק הגנת הפרטיות

**----------------------------------------------------------------------------------------**

**נספחים:** **נספח א'- דוגמא- מסמך הגדרות מאגר- של משרד המשפטים**

**נספח ב'-** **קול קורא רישום ועדכון מאגרים**

**הפניות:** **חוק הגנת הפרטיות התשמ"א 1981.**

**תקנות הגנת הפרטיות התשע"ז 2017.**

**תקן ISO 27001:2013**

**GDPR**

**----------------------------------------------------------------------------------------**

1. **כללי**
   1. חוק הגנת הפרטיות, התשמ"א-1981( להלן: " החוק" או "חוק הגנת הפרטיות "( קובע הוראות שונות וחובות המוטלים על בעל מאגר מידע, מחזיק במאגר מידע ומנהל מאגר מידע. אחת החובות המרכזיות היא חובת אבטחת המידע, הקבועה בסעיף 17 לחוק, אשר מטרתה צמצום החשש מפני שימוש לרעה או פגיעה בשלמות המידע.
   2. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז- 2017( להלן: " תקנות אבטחת מידע ") קובעות עקרונות אבטחת מידע הקשורים בניהול ובשימוש מידע במאגרי המידע, בהתבסס על תקני אבטחת מידע מקובלים בעולם.
   3. אבטחת מידע ברשת ובמערכות האוניברסיטה הינה חיונית להגנת המידע של האוניברסיטה ועובדיה.
   4. לאור זאת, על האוניברסיטה להתקין ולהטמיע מערכות הגנה מפני איומים וחיצוניים ופנימיים וליישם בקרות נוהליות וטכנולוגיות לאכיפת רמת אבטחת מידע ואבטחה פיזית על תשתיות המידע.
2. **המטרה:**

נוהל זה קובע את מדיניות האוניברסיטה בכל הנוגע לניהול ואבטחת מאגרי המידע שלה, לרבות בהתאם

להוראות חוק הגנת הפרטיות, התשמ"א-1981 והתקנות שהותקנו מכוחו ("**חוק הגנת הפרטיות**") והנחיות

הממונה על הגנת הפרטיות ("**הממונה**"), העומד בראש הרשות להגנת הפרטיות.

נוהל זה חל על מאגרי מידע הכוללים מידע אישי.

1. **הגדרות**

* 1. **אבטחת מידע**- הגנה על שלמות המידע, סודיותו ואמינותו או הגנה מפני חשיפה, שימוש והעתקה בלתי מורשים של מידע השמור במאגרי המידע של האוניברסיטה.
  2. **האוניברסיטה-** אוניברסיטת בן-גוריון בנגב.
  3. **מאגר מידע-** אוסף פרטי מידע אישי המוחזק באמצעי מגנטי או אופטי או כל הגדרה אחרת כפי שתתעדכן מעת לעת בחוק הגנת הפרטיות.
  4. **מחזיק מאגר-** מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש (ספק/מנהל מערכת)
  5. **מידע אישי** -נתון הנוגע לאדם מזוהה, או לאדם הניתן לזיהוי, במישרין או בעקיפין, באמצעים סבירים, לרבות מזהה ביומטרי, מספר זהות או כל נתון מזהה ייחודי אחר.
  6. **מידע רגיש-** מידע בעל רגישות מיוחדת כהגדרת מונח זה בחוק הגנת הפרטיות או כל הגדרה אחרת כפי שתתעדכן מעת לעת בחוק הגנת הפרטיות, לרבות מידע רפואי ומידע שחלה עליו חובת סודיות שנקבעה בדין, מידע על מצבו הכלכלי של אדם, מידע אודות מוצאו או עברו הפלילי של אדם.
  7. **מנהל אבטחת מידע**-אדם שמונה לניהול אבטחת המידע באוניברסיטה.
  8. **מנהל מאגר מידע**-מי שהאוניברסיטה הסמיכה אותו כמנהל מאגר מידע של מאגר מידע אחד או יותר.
  9. **מערכות מידע**" או "**מערכות**- כל מערכות המחשוב של האוניברסיטה, לרבות שרתים, תוכנות, כונני רשת, שירותי ענן ודואר אלקטרוני.
  10. **משתמש/ים חיצוני/ים**- כל ספק, יועץ חיצוני, נותן שירותים לאוניברסיטה או כל גורם אחר שאינו

סטודנט באוניברסיטה ואינו עובד של האוניברסיטה אשר נדרש להשתמש במערכות המידע של

אוניברסיטה לצורך ביצוע תפקידו.

* 1. **משתמש/ים**– כל מי שמשתמש במערכות האוניברסיטה, לרבות סטודנטים, עובדים ובעלי תפקידים

באוניברסיטה, עובדים זמניים, משתמשים חיצונים.

* 1. **שלמות המידע**-נתונים הנמצאים במאגר המידע ללא שינוי, מסירה או השמדה בלתי מורשית.

1. **תוכן הנוהל**
   1. **רישום ועדכון מאגר מידע :**
      1. באחריות מנהל אבטחת מידע, לדאוג לרישום ועדכון מאגרי המידע המחויבים ברישום לפי חוק

הגנת הפרטיות, אצל הממונה על הגנת מידע, ברשות להגנת הפרטיות ("הממונה").

* + 1. באחריות הדרג הניהולי ומעלה ומנהלי מאגרי מידע לעדכן את מנהל אבטחת מידע אודות מידע

שלדעתם יש לאגד במאגר מידע ו/או מאגר מידע שיש לרשום אותו ולענות על מסמך הגדרות

מאגר- נספח א'..

* + 1. באחריות מנהל אבטחת מידע לוודא הפצת קול קורא – (נספח ב') ע"י רל"שית מנכ"ל

האוניברסיטה, אחת לשנה לפני תחילת שנת הלימודים, לדרג הניהול מדרגת מנהל מחלקה

ומעלה, מסמך בו הם מתבקשים, בין היתר, לבחון וליידע אם יש ברשותם מאגר מידע חדש ואת

זהות מנהל מאגר המידע.

* + 1. את מסמכי הרישום ניתן למצוא באתר הרשות להגנת הפרטות בכתובת: <https://www.gov.il/he/service/registration_in_the_database>
    2. כחלק מהליך רישום מאגר מידע חדש, מנהל אבטחת מידע יבצע את הפעולות הבאות:
    3. יצירת תיקיה חדשה עם כלל המסמכים הנדרשים- תחת מאגרי מידע רשומים ב-Teams.
    4. הוספת פרטי מאגר המידע בקובץ "עדכון המאגרים" ומילוי "שאלון המאגרים". – תחת תיקיית

מעקב מאגרים.

* + 1. יוודא יחד עם מנהל מאגר המידע הרלוונטי את תקינות הבקשה לרישום מאגר המידע והמסמכים

הנלווים ויגיש אותם לממונה.

* + 1. יבצע מעקב על רישום מאגר המידע ויפעל בהתאם להוראות הממונה- הצלבת מידע תתבצע מול

קובץ רשימת מאגרים לחופש המידע [https://data.gov.il/dataset/pinkas/resource/fd56bf5b-7918-4906-99e4- b0e5102ae268.](https://data.gov.il/dataset/pinkas/resource/fd56bf5b-7918-4906-99e4-%20%20b0e5102ae268.)

* 1. **עדכון מאגרי מידע:**

**באחריות כל מנהל מאגר מידע ליידע את מנהל אבטחת המידע אודות שינוי החל ביחס למאגר מידע שבתחום אחריותו וזאת על מנת שמנהל אבטחת המידע יעדכן את הממונה אודות השינוי החל ביחס למאגר(י) מידע:**

* + 1. מאגר המידע לא רלוונטי או לא בשימוש יותר.
    2. שינוי זהות או פרטים אחרים של מנהל מאגר המידע או הוספת מנהל מאגר נוסף
    3. שינוי בסוג המידע הכלול במאגר המידע
    4. נדרש לפעול בהתאם להנחיות הממונה או הרשות להגנת הפרטיות בדבר אופן ביצוע העדכון

והמסמכים הנדרשים לשם כך.

* 1. **אחריות מנהל אבטחת מידע :**
     1. מנהל אבטחת מידע או מי מטעמו יהיה אחראי להכנת תכנית בקרה שוטפת בדבר העמידה בנוהל

זה ובנהלים משלימים, וידווח אחת לשנה לסמנכ"ל אגף טכנולוגיות חדשנות ודיגיטל על

הממצאים והמלצותיו.

* + 1. מנהל אבטחת מידע או מי מטעמו יהיה אחראי לרישום מאגרי המידע.
    2. **רשימת מצאי- ביחס לכל מאגר מידע, מנהל אבטחת מידע ינהל רשימת מצאי של מערכות מאגר**

**המידע שתפרט את הבאים :**

* + - 1. תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע;
      2. מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהולו ולתחזוקתו, לתמיכה בפעילותו,

לניטור שלו ולאבטחתו;

* + - 1. תוכנות וממשקים המשמשים לתקשורת אל מערכות מאגר המידע ומהן;
      2. תרשים המתאר את מבנה מאגר המידע והקשרים בין המערכות השונות לבין מאגר המידע

ומיקומם של רכיבי המערכות השונות;

* + - 1. תאריך עדכון אחרון.
      2. רפרנטי מחשוב של הפקולטות שהמאגרים שלהם אינם מנוהלים תחת רשת ה-IT של האוניברסיטה אחראים להעברת המידע הנ"ל למנהל אבטחת מידע אחת לשנה או בכל שינוי מהותי.
    1. ככלל, מנהל אבטחת מידע ידאג לבצע הפרדה בין מאגר מידע אחד לשני וכן בין מאגר מידע לבין

מערכות אחרות של האוניברסיטה.

* + 1. תפעול ניהול אירוע אבטחת מידע יעשה בהתאם לנוהל טיפול באירוע אבטחת מידע.
    2. שמירת נתונים וניהול גיבויים יעשה בהתאם לנוהל גיבויים.
    3. ביצוע סקרים ומבדקי חדירה יבוצעו בהתאם לנוהל ניהול סיכונים במאגרים ברמה גבוה – אחת

ל-18 חודשים.

* + 1. ביצוע ביקורת עמידה בדרישות התקנות והפקת דוחות ייעודיים. דיון בדוחות הביקורת אשר

יועברו לו, ויבחן את הצורך בעדכון נוהל זה או את תוכנית הביקורת.

* + 1. בנוסף מנהל אבטחת מידע, בהתייעצות עם מנהלי מאגרי המידע, יבחן את הצורך לעדכן נוהל זה

אחת לשנה.

* + 1. מנהל אבטחת מידע יזום הדרכות תקופתיות להגברת המודעות של העובדים ומשתמשים נוספים

כפי שיקבע על ידי מנהל אבטחת המידע, בדבר סיכונים אפשריים לאירועי אבטחת מידע והטמעת

כלים להתנהגות מונעת ולהגברת המודעות באופן כללי בתחום אבטחת מידע. הדרכות אלו יועברו

על ידי מנהל אבטחת מידע או על מי מטעמו בהתאם לנוהל הדרכות. לעובדים ו/או משתמשים

בעלי גישה למאגר מידע עליו חלה רמת אבטחה בינונית או גבוהה כמפורט בנספח א' יערכו

ההדרכות לכל הפחות אחת לשנתיים.

* + 1. בנוסף להדרכות לעיל, באחריות מנהל אבטחת מידע להביא לידיעת כל משתמש ובמיוחד לעובדים

של האוניברסיטה את ההוראות המפורטות בנוהל "אבטחת מידע ומשאבי מחשוב".

* + 1. מנהל אבטחת מידע יוודא כי בכל מקרה של שינוי הרשאה של משתמש או קבלת הרשאות חדשות,

קיבל אותו משתמש את כל ההנחיות הנדרשות על פי נוהל זה ונהלים נוספים וכי הוסברו לו

חובותיו בקשר אליהן.

* + 1. ניהול סיכוני שרשרת אספקה מצד ספקים המחזיקים במאגר מידע של האוניברסיטה.
  1. **אחריות מנהל אגף טכנולוגיות חדשנות ודיגיטל:**
     1. אחראי לניהול ותפעול תקין של מערכות מאגרי המידע, לרבות על ידי ביצוע עדכונים שוטפים לכל

מערכות מאגרי המידע.

* + 1. שימוש במערכות שהיצרן תומך בהם בהיבטי האבטחה אלא אם ניתן מענה אבטחה מתאים.
    2. יישום הנחיות ומדיניות אבטחת מידע בנושא תשתיות.
  1. **אחריות מנהל מאגר מידע :** 
     1. **מסמך הגדרות מאגר-** כל מנהל מאגר מידע יהיה אחראי לכתיבת מסמך הגדרות ביחס למאגר

המידע עליו הוא אמון ("מסמך הגדרות מאגר"). הכנת מסמך הגדרות מאגר יתבסס על נוסח

הפורמט המצ"ב כנספח א' לנוהל זה. מנהל מאגר מידע יעדכן, וככל שנדרש, בסיוע מנהל אבטחת

מידע, את מסמך הגדרות מאגר בכל עת שנעשה שינוי משמעותי בנושאים המפורטים במסמך

הגדרות מאגר. בנוסף, אחת לשנה יבחן מנהל מאגר האם נדרש לעדכן את מסמך הגדרות המאגר

בשל שינויים טכנולוגיים, ארגוניים או בעקבות אירוע אבטחת מידע.

* + 1. מנהל מאגר יבחן, אחת לשנה, אם המידע השמור במאגר המידע נדרש וכי לא נשמר מידע מעבר

לנדרש לצורך קיום מטרות מאגר המידע.

* + 1. ניהול הרשאות- מנהל מאגר מידע יהיה אחראי לקבוע הרשאות גישה למאגר המידע ולמערכות

המאגר, בהתאם להגדרות התפקיד ובמידה הנדרשת לביצועו בלבד, והכל בהתאם לנוהל הרשאות

גישה למערכות מידע , נוהל גישה מרחוק וכל נוהל אחר, בשינויים המחויבים.

* + 1. באחרית מנהל מאגר מידע לעדכן את מנהל אבטחת מידע ביחס לכל שינוי במאגר המידע

בנושאים המפורטים המצורף.

* + 1. יהיה אחראי לוודא כי בהתקשרות עם משתמש חיצוני אשר ניתנת לו גישה למאגר מידע או למידע אישי הכלול במאגר מידע, מוסדרים תחומי האחריות כפי שנדרש בחוק הגנת הפרטיות ובהתאם לנהלי האוניברסיטה:
    2. **כל מנהל מאגר מידע יהיה אחראי לרכז ביחס לכל מתן גישה למידע אישי למשתמש חיצוני את הנושאים הבאים:** 
       1. סוגי המידע שהגורם החיצוני רשאי לעבד ולרבות לגשת אליו ו/או לעשות בו כל שימוש אחר;
       2. מטרות השימוש במידע האישי במסגרת ההתקשרות ופעולות העיבוד המותרות (לדוגמא, אחסון, איסוף, קריאה, עריכה, העברת המידע לגורם אחר ועוד);
       3. אופן מתן הגישה למידע האישי, לרבות המערכות הרלוונטיות (גישה למאגר המידע, שליחת נתונים ממאגר המידע לגורם החיצוני, קבלת המידע מגורם שלישי);
       4. משך ההתקשרות ואופן החזרת/מחיקת המידע האישי בתום ההתקשרות;
       5. אמצעי אבטחת המידע המיושמים בקשר להתקשרות זו.

1. **אחריות לביצוע:**
   1. האחריות למילוי נוהל זה חלה על מנהל אבטחת המידע וכל מנהל מאגר מידע באוניברסיטה ביחס למאגרי המידע שבאחריותו.
   2. תוכן נוהל זו יימסר לסמנכ"ל אגף טכנולוגיות חדשנות ודיגיטל, מנהל אבטחת מידע, דרג הניהול מדרגת מנהל מחלקה ומעלה, מנהלי מאגרי מידע ומנהל אבטחת מידע בהיקף הנדרש לצורך מילוי תפקידם.
   3. בסמכות ואחריות מנהל אבטחת מידע לבקר ולאכוף נוהל זה אחת לשנה או בכל שינוי משמעותי.

**6. תחולה: נוהל זה תקף מיום פרסומו.**

**נספח א'- דוגמא- מסמך הגדרות מאגר- משרד המשפטים**

**מסמך הגדרות מאגר**

**(יש למלא שאלון זה עבור כל מאגר ומאגר)**

| **ניהול שינויים** | | | |
| --- | --- | --- | --- |
| **תאריך** | **מחבר** | **גרסה** | **שינוי** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

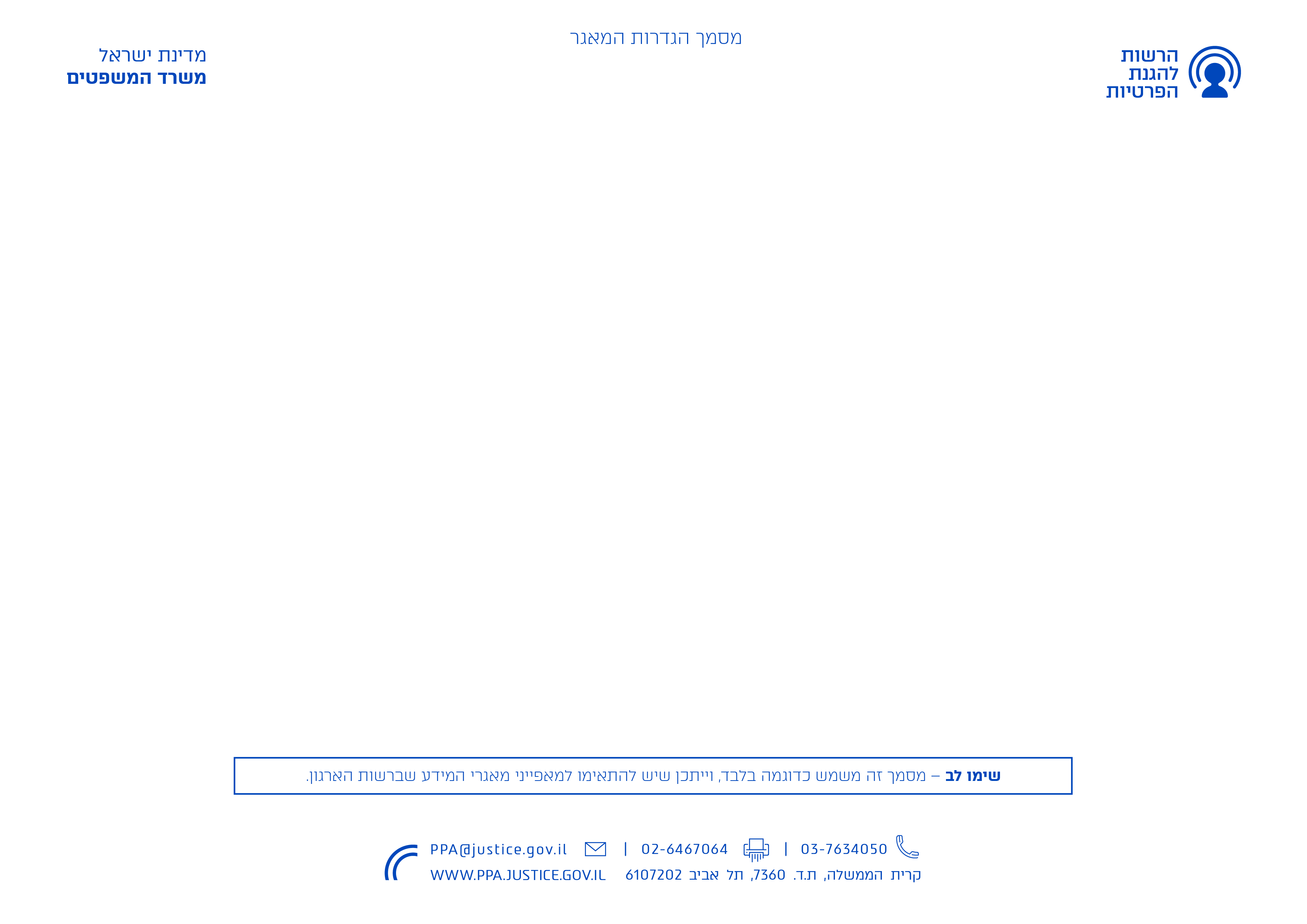
| **מס"ד** | **שאלה** | **רלוונטי\ לא רלוונטי** | **פירוט התשובה (במידה ולא רלוונטי יש לפרט מדוע)** | **הערות** |
| --- | --- | --- | --- | --- |
| **תיאור המאגר** | | | | |
|  | תאר באופן כללי את פעולות האיסוף והשימוש במידע   1. מהם המקורות מהם נאסף המידע? 2. למה משמש המאגר באופן שוטף? |  |  |  |
|  | תאר את מטרות השימוש במידע:   1. הסיבות שלשמן נאסף המידע במאגר 2. השימוש הנוכחי בנתוני המאגר 3. ההלימה בין הסיבות שלשמן נאסף המידע ולאופי השימוש הנוכחי |  |  |  |
|  | פרט את סוגי המידע השונים הכלולים במאגר המידע, בשים לב לרשימת סוגי המידע שבפרט 1(3) בתוספת הראשונה;  יש לפרט את סוג המידע- וכן תיאור של השדות הנאספים עבור אותו סוג.  לדוגמא- סעיף 1 (3) ב' מתייחס ל: " מידע רפואי או מידע על מצבו הנפשי של אדם" במידה ואתה שומר מידע מסוג זה, עליך לפרט את השדות השונים הנשמרים במאגר, כגון:   1. שם ושם משפחה 2. מספר זהות 3. כתובת 4. טלפון 5. מייל 6. מידע רפואי מסוג: XXX, YYY 7. מספר תיק 8. מספר חבר בקופת חולים 9. וכו'   פרט את סיווג הגורמים עליהם נאסף המידע (למשל: לקוחות, עובדים, ספקים, ילדים וכו') |  |  |  |

| **העברת המידע** | | | | |
| --- | --- | --- | --- | --- |
|  | אנא ספק פרטים על העברת מאגר המידע, או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה.  יש לפרט את:   1. מטרת ההעברה, 2. ארץ היעד, 3. אופן ההעברה 4. זהות הנעבר. 5. הבסיס החוקי עליו נשענת העברת המידע לחו"ל, בהתאם לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001. | כן לא |  |  |
|  | במידה ומתבצעת פעילות עיבוד מידע באמצעות גורם חיצוני, אנא פרט:   1. פרטי הגורם החיצוני (שם חברה, נציג אחראי, כתובת, פרטי קשר) 2. המיקום הפיזי בו נאגר המידע 3. פירוט טכנולוגי של הדרך בה מתבצע עיבוד המידע 4. הסיבה בעטיה מתבצע העיבוד באמצעות גורם חיצוני 5. ההלימה בין פעולות הגורם החיצוני לבין המטרה לשמה הוקם המאגר ונאסף המידע. 6. ציין האם נקבע הסכם לפי תקנה 15 | כן לא |  |  |

| **ניהול סיכונים** | | | | |
| --- | --- | --- | --- | --- |
|  | פרט את הסיכונים העיקריים של פגיעה באבטחת המידע, ואופן ההתמודדות עמם. יש לפרט עבור כל סיכון:   1. תיאור הסיכון 2. אופן ההתמודדות עם הסיכון |  |  |  |

| **פרטים של מנהל\מחזיק מאגר** | | | | |
| --- | --- | --- | --- | --- |
|  | אנא הוסף פרטי קשר של הגורמים הבאים:   1. שמו של מנהל מאגר המידע, 2. שמו של מחזיק המאגר - הגורם החיצוני (אם קיים) המעבד או מאחסן את המידע עבור בעל המאגר בהתאם להוראותיו 3. שמו של הממונה על אבטחת מידע במאגר   עבור כל אחד מהגורמים יש לציין:   1. שם ושם משפחה 2. ת.ז 3. תפקיד בארגון 4. פרטי קשר (כתובת דוא"ל וטלפון ישיר) |  |  |  |

| **פעילות תחזוקה שנתית למסמך הגדרות מאגר** | | | | |
| --- | --- | --- | --- | --- |
|  | התקנה קובעת כי: "בעל מאגר מידע יעדכן את מסמך הגדרות המאגר בכל עת שנעשה שינוי משמעותי בנושאים המפורטים בתקנת משנה (א), ויבחן את הצורך בעדכון כאמור, בשל שינויים טכנולוגים ארגונים או אירועי אבטחה כאמור בתקנה 11, בכל שנה עד ה- 31 בדצמבר"  אנא ציין:   1. את תאריך העדכון אחרון של מסמך הגדרות המאגר 2. אנא ציין בטבלת ניהול השינויים בראש המסמך, את תאריך שינוי המסמך, הגורם המתעד, מהי הגרסא הנוכחית של המסמך ומהו השינוי שהוביל לעדכון המסמך | כן |  |  |
|  | התקנה קובעת כי: "בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר" יש לציין בעמודה זו לפחות פעם בשנה את הנתונים הבאים ביחס לדרישה זו:   1. תאריך הבחינה 2. זהות מבצע הבחינה וזהות ותאריך הגורם שאישר את תוצאותיה 3. תמצית נימוקי מסקנת הבחינה, כולל התייחסות לסוג והיקף המידע הנשמר ולמשך שמירתו 4. תיאור תמציתי של הפעולות שננקטו למימוש המסקנה 5. התקופה (בהערכה) שעבורה יידרש לשמור את המידע | כן |  |  |





**נספח ב' – קול קורא רישום ועדכון מאגרים**

# הנחיות אבטחת מידע- ניהול מאגרי מידע

# כללי

* 1. אוניברסיטת בן-גוריון בנגב מחויבת לעמוד בדרישות חוק הגנת הפרטיות התשמ"א 1981 ובתקנות הגנת הפרטיות התשע"ז 2017.
  2. החוק נועד להגן על פרטיותם של בני אדם אשר נתוניהם האישיים מצויים במאגרי המידע השונים.
  3. באוניברסיטה 24 מאגרים רשומים.
  4. אחת לשנה אנחנו מבצעים ריענון ותיקוף הנחיות בהתאם לתקנות ויוצאים בקול קורא לרישום מאגרי מידע ע"פ חוק.

1. **מטרה**
   1. עמידה בדרישות הרלוונטיות בתקנות הגנת הפרטיות למנהלי מאגרים באוניברסיטה.
   2. קול קורא לרישום מאגרים ע"פ החוק והתקנות.
2. **מאגרים חדשים**
   1. כל כוונה לבצע איסוף מידע רגיש כהגדרתו בחוק נדרש לביצוע רישום מוסדר מול משרד המשפטים.
   2. באם קיים תהליך חדש שכזה נדרש לפנות למנהל אבטחת מידע- מיכאל אלבז לטובת ביצוע הליך הרישום של המאגר
3. **מאגרים קיימים- חובות מנהל מאגר**
   1. תיקוף ועדכון מסמך הגדרות המאגר – נדרש לבחון האם נעשו שינוי משמעותיים/שינויים טכנולוגיים/שינויים ארגוניים או התרחשו אירועי אבטחת מידע. **אם אכן קרה נדרש לתקף ולעדכן את מסמך הגדרות המאגר.**
   2. נדרש לבחון האם המידע הנשמר במאגר אינו רב מן הנדרש למטרות המאגר- **אם כן נדרש לבצע ביעור מבוקר של מידע.**
   3. נדרש לבחון אם בוצעה הדרכה לבעלי ההרשאה במאגר בדבר חובותיהם בשנתיים האחרונות- **אם כן נדרש להציג דו"ח ביצוע, אם לא נדרש לתאם הדרכה בתאם.**
   4. נדרש לבחון האם קיים נוהל אבטחת מאגר- אם כן- **נדרש לראות שאכן עומדים בדרישות הנוהל, אם לא נדרש לעדכן את מנהל אבטחת מידע.**
   5. נדרש לבחון האם בוצעה ביקורת לעמידה בדרישות התקנות**- אם כן נדרש לציין מי ביצע את הביקורת ומהם הממצאים.**
   6. נדרש לבצע סקירת הרשאות למאגר**- נדרש להראות תיעוד של סקירת ההרשאות.**
   7. ביצוע ביקורת אבטחת מידע על ספקים המחזיקים מידע או מעבדים מידע**- נדרש לבחון האם בוצע**
   8. ביצוע שחזור מגיבוישל מאגר**- נדרש לבחון האם בוצע ע"י מנהל אבטחת מידע**

# נדרש שת"פ מלא מצידכם לעמידה בדרישות החוק והתקנות.

# לכל שאלה/הבהרה ניתן לפנות במייל grc@bgu.ac.il