



1. **מבוא:**

- 1.1. מסמך זה נועד לפרט את חובות אוניברסיטת בר אילן (להלן: "האוניברסיטה") כלפיך, כעובד סגל מנהלי או סגל אקדמי, בדבר איסוף ועיבוד המידע האישי שלך, בהתאם לחובת היידוע הקבועה בסעיף 11 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "החוק" או "חוק הגנת הפרטיות"), התקנות שתוקנו מכוח החוק ובהתאם להנחיות רשם מאגרי המידע והרשות להגנת הפרטיות.
- 1.2. מדיניות זו מפרטת אילו סוגי מידע אישי האוניברסיטה מעבדת, לאילו מטרות, מקורות המידע, שיתוף מידע עם צדדים חיצוניים, אופן אחסון המידע, פרטי יצירת הקשר עם האוניברסיטה והממונה על הגנת הפרטיות, וכן זכויות העובדים ביחס למידע האישי שלהם.

2. **הגדרות:**

- 2.1. **"מידע אישי"** – כהגדרתו בחוק הגנת הפרטיות, תשמ"א-1981: נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי; לעניין הגדרה זו, "אדם הניתן לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי.
- 2.2. **"מידע בעל רגישות מיוחדת"** – כהגדרתו בחוק הגנת הפרטיות התשמ"א-1981: מידע אישי על צנעת חיי המשפחה של אדם, על צנעת אישיותו ועל נטייתו המינית, מידע בריאותי או רפואי, מידע גנטי, מזהה ביומטרי, מוצאו של אדם, עבר פלילי, דעות פוליטיות, אמונות דתיות, השקפת עולם, נתוני מיקום, נתוני תעבורה, שכר, פעילות פיננסית, מידע אישי שחלה עליו חובת סודיות שנקבעה בדיון.
- 2.3. **"מאגר מידע"** – כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981: אוסף פרטי מידע אישי המעובד באמצעי דיגיטלי. לדוגמא: אוסף נתונים אישי או רגיש, בכל פורמט דיגיטלי או ממוכן, הנגיש לעיבוד באמצעים ממוחשבים, לרבות מערכות מחשוב פנימיות, מערכות ענן, מערכות שכר ונוכחות, מערכות אבטחת מידע, או כל אוסף דומה המוחזק על ידי האוניברסיטה לצורך תפעול שוטף.
- 2.4. **עיבוד:** כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו או מתן גישה אליו.
- 2.5. **"ניטור"** בקרה אחר פעולות המתבצעות במערכות מידע באמצעות מערכות ייעודיות, לרבות בדוא"ל, הן באופן אוטומטי והן באופן ידני. לדוגמא: כל פעולה של איסוף, תיעוד או עיבוד נתונים הנוגעים לפעילותך במערכות האוניברסיטה או בתחומי הקמפוס.
- השימוש בתוצרי הניטור רלוונטי לצרכים הבאים: אבטחת מידע, שמירה על ביטחון, תפעול מערכות, עמידה בדרישות החוק ותחקור אירועי אבטחת מידע, בהתאם לעקרון המידתיות ובכפוף לחובת היידוע וההסכמה בדיון ובהתאמה והשלמה של תקנוני האוניברסיטה ונהליה וכן כמפורט בהוראת הנהלה: מדיניות וכללי שימוש בדואר אלקטרוני (18-005).
- 2.6. **"מנהל אבטחת מידע"** – מי שמונה ע"י סמנכ"ל תקשוב ואשר תפקידו לטפל בכל הקשור לנושאי אבטחת מידע וכן לגיבוש הנהלים הפנימיים הקשורים לאבטחת המידע באוניברסיטה, ביצועם ואכיפתם.

2.7. "ממונה על הגנת הפרטיות" - מי שמונה על ידי מנכ"ל האוניברסיטה להיות אחראי על הטמעה ויישום ההוראות החלות על האוניברסיטה מכוח חוק הגנת הפרטיות ותקנותיו ותקנות האיחוד האירופי-GDPR.

3. חובת מסירת המידע ותוצאות אי-מסירתו

- 3.1. מסירת מידע אישי על ידך כעובד יכולה להיות חובה חוקית או וולונטרית, בהתאם לסוג המידע.
- 3.2. מסירת מידע לפי דין: חלק מן המידע אודותך שנאסף על ידי האוניברסיטה הוא מידע שחובה לספק על-פי דין, ואי-מסירתו עלולה למנוע את העסקתך כעובד. כך למשל, הדרישה למסור פרטי זהות, כתובת, טופס 101, ופרטי בנק לצורך רישום ותשלום שכר היא דרישה חוקית והכרחית, ללא מידע זה האוניברסיטה אינה יכולה לקיים יחסי עבודה תקינים או לעמוד בדרישות תשלום השכר ובדיני העבודה. דוגמה נוספת: מסירת נתונים לצורך רישום לביטוח פנסיוני היא חובה המעוגנת בחוק, ואי-מסירתם תמנע מהאוניברסיטה מלרשום אותך לפנסיה כפי שמתחייב.
- 3.3. מסירת מידע בהתאם להסכמתך: ישנם סוגי מידע הניתנים לשם ניהול תקין של מערכות האוניברסיטה עמידה בהוראות הדין ומתן שירות מיטבי עבורך. מסירת המידע היא תנאי הכרחי לשם הכללתך במערכות הארגוניות, לרבות ניהול משכורות, זכויות סוציאליות, מתן שירותי רווחה, תפעול מערכות פנימיות והקצאת משאבים. אי מסירת מידע כאמור עלולה לפגוע ביכולת האוניברסיטה לספק את השירותים הדרושים לך, ואף להביא לעיכוב או מניעה בקבלת זכויות ותשלומים להם אתה זכאי על פי דין.

4. סוגי המידע האישי שמעובדים ע"י האוניברסיטה

- 4.1. פרטים מזיהוי ואישיים - כגון שם מלא, מספר זהות, כתובת, פרטי התקשרות (טלפון, דוא"ל), תאריך לידה, קשרים משפחתיים, מצב משפחתי, מגדר ופרטי חשבון בנק לצורך תשלום שכר וניהול זכויות, תשלומים שונים והחזר הוצאות, ניהול יחסי העבודה ומתן שירותים, מתן הטבות, והעמדת כלי עבודה במסגרת עבודתך.
- 4.2. מידע בריאותי הנוגע לך והרלוונטי להעסקתך, כגון מידע על מוגבלות לצורך ביצוע התאמות נדרשות, מידע מרופא תעסוקתי הנוגע לכשירות רפואית לביצוע תפקיד מסוים, אישורי מחלה וכיו"ב. מידע זה יאסף וישמר בכפוף לדין.
- 4.3. מידע תעסוקתי - כגון תפקיד, מתכונת ההעסקה, ותק ותאריכי העסקה, תנאי ההעסקה, נתוני שכר והטבות, הערכות ביצוע ומשוב מקצועי, מינויים/הסכמי העסקה, היקף ההעסקה, ניסיון מקצועי קודם, השכלה, מידע רלוונטי לתפקיד וכל מידע אחר הנדרש לניהול יחסי העבודה או לקביעת זכויותך ותנאי השכר.
- 4.4. נתוני נוכחות - לדוגמה, נתונים המשמשים לרישום כניסה ויציאה (שעון נוכחות) לצורך תשלום שכר ותנאים נלווים ולצרכי מעקב אחר שעות העבודה.
- 4.5. תיעוד ממצלמות אבטחה כפוף להוראות נוהל מצלמות שמספרו 10-007 והנחיות הרשות להגנת הפרטיות: הנחיה 5/17 והנחיה 4/12.



4.6. צילומים - צילומי קהל ואווירה בהם הנך מופיע/ה במהלך טקסים/כנסים/אירועים לצורך תיעוד ופרסום פנימי וחיצוני (לרבות באתר האינטרנט של האוניברסיטה, בניוזלטר וברשתות החברתיות). באפשרותך לבקש את הסרת התמונה מהפלטפורמות שבהן פורסמה (ככל שהדבר בשליטת האוניברסיטה וניתן לביצוע סביר). האוניברסיטה מתחייבת שלא לפרסם צילום פרטי וייעודי שלך למטרות שיווק, רשתות חברתיות ויחסי ציבור, ללא קבלת הסכמתך המפורשת לכך מראש.

4.7. נתוני שימוש דיגיטליים – לרבות נתוני לוגים (Logs) ממערכות מחשוב ותקשורת, שימוש בדוא"ל הארגוני, שימוש ברשת האינטרנט של האוניברסיטה, פעולות שבוצעו במערכות מידע פנימיות או חיצוניות (כגון מערכות ענן ושירותי אוניברסיטה מקוונים), כתובות IP, זמני חיבור וניתוק, פעילות במערכות קבצים או מערכות אבטחת מידע. נתונים אלה נאספים באופן אוטומטי ונשמרים לצורך אבטחת מידע, תפעול מערכות, עמידה בחובות החוקיות ותחקור אירועי אבטחת מידע וסייבר.

5. מטרות עיבוד המידע האישי

5.1. המידע האישי אודותך משמש את האוניברסיטה למטרות הבאות, בהתאם לעקרון צמידות המטרה:

- תשלום שכר וזכויות פנסיוניות - ניהול ענייני כוח אדם ומשאבי אנוש, חישוב משכורות ותשלומים חודשיים לרבות עיבוד שעות נוכחות והעברה לחשבונות הבנק ולגופים המוסדיים לתשלומי פנסיה לפי חוק.
- ניהול יחסי העבודה וניהול האוניברסיטה – לרבות לצורך הקצאת משאבים כלי עבודה, ניהול הרשאות וגישה למערכות מידע, והתקשרות עם ספקים לצורך אספקת שירותים / הטבות הדורשים הזדהות ככל שנדרש.
- שמירה על ביטחון וסדר - הבטחת ביטחון העובדים, המתקנים והמידע באוניברסיטה, שימוש במצלמות אבטחה למניעת אירועי ביטחון, חקירת תקריות או עבירות משמעת ככל שיתרחשו, והגנה על ציוד ורכוש האוניברסיטה.
- עמידה בדרישות חוקיות ורגולטוריות - קיום חובות המוטלות על האוניברסיטה על פי דין בקשר להעסקת עובדים. לדוגמה, דיווח נתוני שכר וניכויים לרשויות המס ולביטוח לאומי.
- התאמות לעובדים עם מוגבלות - שימוש במידע הרפואי הרלוונטי לצורך התאמת תנאי וסביבת העבודה עבור עובדים עם מוגבלויות או צרכים רפואיים מיוחדים. מטרת עיבוד מידע זה היא לאפשר הזדמנות שווה בעבודה ועמידה בדרישות החוק למתן התאמות.
- מתן שירותי רווחה והטבות לעובדים - לצורך מתן הטבות, כגון סבסוד ארוחות, מתנות לימי הולדת, ימי גיבוש, פעילויות שמקיימת האוניברסיטה וכיו"ב.
- יחסי ציבור, שיווק ותיעוד
- אבטחת מידע – ניטור פעילויות משתמשים, תחקור אירועי אבטחת מידע וסייבר.
- טעמים משפטיים - לרבות ניהול הליכים משפטיים, הוראות דין, צו שיפוטי, הוראות רגולטור וכיו"ב.
- מחקר ואקדמיה – פרסומים אקדמאיים, קולות קורא, פרסום מחקרים וכיו"ב.



- לצורך עיבוד מידע סטטיסטי באמצעות איסוף וניתוח מידע אנונימי, סטטיסטי, או מצרפי (אגרגטיבי)
- מטרות נוספות ככל שתינתן הסכמה מפורשת שלך.

6. שיתוף מידע עם גורמים חיצוניים

6.1. האוניברסיטה מקפידה על סודיות המידע ומעבירה מידע אישי עליך לגורמים חיצוניים, רק במקרים הנדרשים לצורך ניהול האוניברסיטה, ניהול יחסי העבודה / מתן שירותים / הטבות / כלי עבודה לעובדים / מטעמים משפטיים, לצורך עמידה בחובותיה או לפי הוראות הדין. בכל מקרה של העברה כאמור, ימסר רק המידע לפי הוראות הדין, או בכפוף להתחייבות הגורם המקבל לשמור על סודיות ואבטחת המידע ולהשתמש בו רק בצמידות למטרה שלשמו נמסר המידע. הגורמים החיצוניים העיקריים שעשויים לקבל גישה למידע עובדים הם:

- ספקים נותני שירות לאוניברסיטה – האוניברסיטה רשאית לשתף מידע אישי שלך עם גורמים חיצוניים, במידה הנדרשת לצרכים האמורים לעיל, ובכלל זה ספקי שירותים ויועצים של האוניברסיטה, שירותי רווחה, ביטוח, משכורות, הדרכות מקצועיות, ספקי שירותי נסיעות, חברות ליסינג, מפיקי אירועים וספקי אירועים, ותשתיות טכנולוגיות (כגון שירותי ענן, מערכות ניהול עובדים, מערכות דיווח, טיפול באירועי אבטחת מידע וסייבר, מחקר סטטיסטי) ועוד.
- שיתוף המידע יתבצע בכפוף לחוק, להסכמים מחייבים מול אותם גורמים, ולדרישות האבטחה והפרטיות הנהוגות באוניברסיטה, תוך שמירה על עיקרון המידתיות ושימוש במידע רק לצורך המוגדר.
- רשויות וגופים ציבוריים מוסמכים - במקרים שהדבר נדרש על פי חוק ו/או מכוח סמכות בחוק ו/או בדין, האוניברסיטה תעביר מידע אישי לרשויות הרלוונטיות. למשל, דיווחים שוטפים לרשות המיסים, למוסד לביטוח לאומי, למל"ג וות"ל לבתי משפט או לרשויות אכיפת חוק אם יתקבל צו חוקי המחייב זאת. העברה כזו תתבצע רק במתכונת ובהיקף הנדרש בדין.

7. אופן השימוש, אחסון ואבטחת המידע

- 7.1. המידע האישי שלך המעובד באמצעים דיגיטליים, נשמר במאגרי מידע ממוחשבים ומאובטחים של האוניברסיטה, ובכלל זה במערכות מקומיות או חיצוניות מוגנות. חלק מהמידע מאוחסן בשרתים של ספקי שירות חיצוניים (למשל שירותי ענן), אשר עשויים להימצא גם מחוץ לגבולות ישראל, בכפוף להוראות הדין לגבי העברת מידע לחו"ל. האוניברסיטה נוקטת באמצעי אבטחה טכניים וארגוניים סבירים בהתאם לתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, על מנת להגן על המידע האישי מפני גישה בלתי מורשית, דליפה, איבוד או שימוש לרעה.
- 7.2. עיבוד המידע האישי כמתואר במדיניות פרטיות זו עשוי להתבצע באמצעות שימוש בכלים טכנולוגיים מתקדמים, כדוגמת מערכות המבוססות על אלגוריתמים, בינה מלאכותית, למידת מכונה, ניתוחי שפה ועוד, והכול בכפוף לכל דין, באופן אחראי, תוך שמירה על פרטיות המשתמשים והימנעות מהטיות או אפליה ובהתאם לנוהלי האוניברסיטה.
- 7.3. המידע האישי יישמר על ידי האוניברסיטה למשך הזמן הדרוש לקיום המטרות שלשמן נאסף, או למשך פרק הזמן הקבוע בדיני העבודה, המס והגנת הפרטיות, לפי המאוחר מבניהם.



8. בעל שליטה במאגר המידע ופרטי יצירת קשר

8.1. בעל השליטה במאגרי המידע לגבי נתוניך הוא האוניברסיטה. ניתן ליצור קשר בעל השליטה:

כתובת: אנה ומקס ווב, רמת-גן.

טלפון: 03-5317000.

מנהל מאגר – סמנכ"ל משאבי אנוש, דוא"ל לפניות admin-manpower.office@biu.ac.il

9. ממונה על הגנת הפרטיות

9.1. באוניברסיטה מונה ממונה על הגנת הפרטיות במיקור חוץ בהתאם להוראות הדין.

כתובת דוא"ל הממונה: Privacy@biu.ac.il.

10. זכויות העובד ביחס למידע האישי

10.1. החוק מקנה לך מספר זכויות חשובות בנוגע למידע האישי עליך שנאסף במאגרי המידע של האוניברסיטה. האוניברסיטה מכבדת זכויות אלו ותאפשר את מימושן על פי החוק:

- זכות עיון (גישה למידע) – אתה זכאי לעיין ולקבל עותק מן המידע האישי המתייחס אליך שמוחזק במאגרי המידע של האוניברסיטה. בקשה לעיון יש להעביר לסמנכ"ל משאבי אנוש.
- זכות לתיקון/מחיקת מידע – אם גילית כי מידע מסוים שאנו מחזיקים אודותיך אינו נכון, אינו מלא או אינו מעודכן, עומדת לך הזכות לבקש תיקון ו/או מחיקה של המידע. בקשה כאמור תוגש לסמנכ"ל משאבי אנוש או למנהל המאגר הרלוונטי, לפי העניין.

1.1. אופן הגשת הבקשה ואופן טיפול בבקשות יהיה בהתאם לנוהל ניהול מאגרי מידע והגנת הפרטיות.

11. עדכון מדיניות:

11.1. מדיניות פרטיות זו עשויה להתעדכן מעת לעת, למשל עקב שינויים בדין או בנוהלי האוניברסיטה. בכל עדכון מהותי נודיע לך באמצעות דוא"ל או דרך מערכת פנימית. הגרסה העדכנית של המסמך תהיה זמינה לך בכל עת לעיון. מדיניות זו נוסחה בלשון זכר לצרכי נוחות בלבד, אך מיועדת לכל המגדרים. כל הפרה של מדיניות זו או של חוק הגנת הפרטיות על ידי האוניברסיטה נעשית בשוגג ונשמח שתפנה את תשומת לבנו לכך באופן מיידי לתיקון המצב.

11.2. אנו מחויבים להגן על פרטיותך ולקיים את כל הדרישות החוקיות החלות עלינו בתחום זה.

12. אישור וקבלת המדיניות:

12.1. פרסום מדיניות זו על ידי האוניברסיטה מהווה עמידה של האוניברסיטה בחובת היידוע לפי סעיף 11 לחוק הגנת הפרטיות, התשמ"א-1981.

12.2. עובדים המעוניינים בכך מוזמנים להפנות שאלות לסמנכ"ל משאבי אנוש ולקבל הבהרות במידת הצורך.