חשיפת מידע אישי על אודות סטודנטים באתרי מוסדות להשכלה גבוהה

מוסדות אקדמיים שונים נוהגים לעשות שימוש בממשקים אינטרנטיים ובמערכות לניהול אקדמי שנועדו לשרת את הסטודנטים והמרצים למטרות פדגוגיות שונות (להלן: "**המערכות**"). במערכות אלה מנוהל מהלך הלימודים בקורסים השונים, כגון התקשורת בין הסטודנטים למרצים, פרסום עבודות, מבחנים, ציונים והעברת מסמכים שונים. מטבע הדברים, מידע אישי ורגיש רב מעובד במערכות אלה.

ברשות להגנת הפרטיות (להלן: "**הרשות**") מתקבלות מעת לעת תלונות בעניין מסמכים שונים המכילים מידע אישי של תלמידים וסטודנטים שמאוחסנים באופן נגיש לכל דורש ברשת. למשל, גיליונות ציונים הנושאים את שמות הסטודנטים ומספרי תעודות הזהות שלהם, מסמכים הקשורים בלקויות למידה או מצב רפואי, ראיונות אישיים וכיו"ב.

נזכיר, מערכות אלה פועלות ככל אתר על גבי רשת האינטרנט, על כל הסיכונים למידע הנובעים מכך, ויש לנהל אותם בהתאם. ברי כי השימוש במערכות נועד לאפשר גם יעילות, גמישות וזמינות מרבית של המשתמשים השונים לפי צרכיהם.

אחת החולשות הנפוצות ביותר היא ה- Directory Listing (להלן: "**ליסטינג**"), לפיה השרת מאפשר את הצגת התיקיות המאוחסנות בו ואף גישה לתוך התיקיות השונות לרבות צפייה והורדת מסמכים. הליסטינג היא למעשה פעולת "אינדוקס" של תיקיות בשרת שנסרקו על-ידי גוגל והופכות לפומביות על תוכנן. הליסטינג כשלעצמו אמנם אינו מהווה חולשת אבטחה, אולם כאשר התיקיות "הפתוחות" מכילות מידע אישי, הדבר יוצר סיכון לאבטחת המידע, שהמוסד האקדמי נושא באחריות לה על פי חוק הגנת הפרטיות, התשמ"א-1981.

בחולשת הליסטינג ניתן לטפל בשני מישורים עיקריים – **האחד, הסרת מידע אישי מתוך התיקיות "הפתוחות". השני, הגדרת השרת באופן שיבטל את האפשרות לאינדוקס התיקיות** וליצירת הגישה אליהן בגלישה חופשית באתר (לכל סוג שרת יש הגדרות פרטניות שקבע היצרן).

אפשרות נוספת לחשיפת מידע אישי ורגיש היא באמצעות גוגל, אשר כידוע סורק אתרים על דפיהם השונים באופן רציף. כך, כאשר אתר מאחסן מסמכים בבסיס הנתונים, אלו עשויים להיסרק על-ידי "זחלני" גוגל. קצרה היריעה מכדי להרחיב עתה על אופן פעולת "זחלני" גוגל ומנגנוני הסריקה, אך חשוב להבין שכמעט כל מה שנסרק (כגון אתרים, תיקיות או מסמכים), עלול להיחשף במסגרת חיפוש חופשי או חיפוש מתקדם באמצעות מנוע החיפוש של גוגל.

כאשר אתר כלשהו מיישם בקרת גישה, ודורש הזדהות טרם קבלת גישה לאזור בו מאוחסן מידע אישי, בקרה זו **מגבילה את הסריקה** ואינה מאפשרת לגוגל לסרוק את המסמכים המוגנים. בתוך כך, למעשה לא ניתן יהיה לבצע אינדקס למסמכים המכילים מידע אישי, ויהיה צורך לעבור את מנגנון הגישה בכדי להתקדם לאזור המוגן.

על מנת להגביל סריקת מידע, **יש ליישם מנגנוני זיהוי ואימות,** טרם הגישה לאזור הרלוונטי באתר. זאת, בדומה לכל אתר אחר שבו קיים "אזור אישי" מוגן. כמובן שההמלצה הגורפת היא אף **ליישם בקרת אימות דו-שלבי,** כך שהליך ההזדהות יהיה מאובטח עוד יותר.

פעילות הגנתית נוספת שחשוב מאוד לבצע בקרב הסטודנטים, הסגל האקדמי, ועובדי המוסד האקדמי היא **הגברת המודעות**. יש לבצע הדרכות והסברה לכל אחת מקבוצות אלו בהתאם למאפייניה ולאופן עבודתה עם הסביבה הלימודית המקוונת. יש לדון בין היתר **בצמצום היקף המידע הרגיש שמאוחסן במערכות, במניעת חשיפת מידע עודף, בהעברת מידע בצורה מאובטחת ובהסרת מידע שאינו נחוץ עוד**.

לבסוף, נוסיף ונדגיש כי כל מוסד להשכלה גבוהה נושא באחריות למידע אודות הסטודנטים, הסגל האקדמי ועובדי המוסד, המאוחסן במאגרי המידע שברשותו. אי-לכך, פעילות הגנתית טובה תהיה יישום מדיניות של "אפס-אמון" בנוגע למשתמשים במערכות, והתקנת בקרות מפצות למניעת הכשל הבא. מדובר בניטור וזיהוי של טעות-אנוש; הונאה באמצעות הנדסת אנוש; מוצרי תוכנה שחסרים בהם עדכוני אבטחה; תצורת-רשת לקויה, כגון הפרדה לקויה בין סביבת ייצור לבין סביבת פיתוח או סביבת בדיקות, הפרדה לקויה בין שרת גיבויים לבין שרת וירטואליזציה, ועוד.

יובהר, כי מסמך זה נועד לשמש כלי עזר בלבד ואינו ממצה את החובות המוטלות על המוסד האקדמי לפי חוק הגנת הפרטיות, התשמ"א-1981, ולפי תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017. במקרה של ספק, הוראות החוק והתקנות גוברות על האמור במסמך.