

דו"ח פיקוח רוחב בקרב מגזר הקמעונאות פורסם לציבור

עדכוני לקוחות

ביום 19 ביוני 2023 הרשות להגנת הפרטיות ("הרשות") פרסמה [דו"ח פיקוח רוחב במגזר הקמעונאות](#) ("הדו"ח"). הדו"ח מסכם הליך פיקוח רוחב שנערך בין השנים 2020-2021 בקרב 29 גופים וחברות הפועלים במגזר הקמעונאות, בדגש על תחום המזון, הדלק, הפארם והאופטיקה. במסגרת ההליך, הרשות בחנה שלושה קריטריונים עיקריים בתחום הגנת הפרטיות:

1. **בקרה ארגונית:** קיום תכנית עבודה בתחומי אבטחת מידע והגנת הפרטיות ומינוי גורמים בעלי אחריות בתחום.
2. **ניהול מאגרי מידע (לרבות עיבוד מידע אישי במיקור חוץ):** אופן קבלת הסכמה לשימוש במידע, מתן הזכות לעיון במידע, וכן בחינת התקשרויות של בעלי מאגרי המידע עם צדדים שלישיים המחזיקים מידע.
3. **אבטחת מידע:** עמידת הגופים בהוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 בכל הנוגע לניהול המידע האישי שבבעלותם והחזקתם.

מבין כלל המאגרים המצויים בידי הגופים הקמעונאיים, הליך הפיקוח התמקד במאגרי מידע הכוללים נתוני לקוחות (ובכלל זה מכירות ומועדוני לקוחות) וכן מאגרי מידע ביומטריים. ממצאי הדו"ח, בשקלול כלל התחומים שנבדקו, מלמדים על רמה גבוהה של עמידה בהוראות חוק הגנת הפרטיות, התשמ"א-1981 והתקנות מכוחו בקרב מרבית הגופים במגזר הקמעונאות, כאשר כרבע מהגופים נמצאו ברמת עמידה בינונית. יחד עם זאת, הדו"ח מציין כי על אף רגישות המידע שבידי הגופים המפוקחים, המענה בתחום אבטחת המידע אינו משביע רצון, כאשר רק כמחצית הגופים צוינו ככאלה בהם רמת העמידה בקריטריון זה היא גבוהה.

בין היתר, הדו"ח הצביע על ליקויים בתחומים הבאים:

- היעדר תכנית עבודה ותכנית ביקורת בתחום הגנת הפרטיות ואבטחת המידע, או היותה בלתי איכותית;
- אי ביצוע סקרי סיכונים וביקורות בנושא אבטחת המידע;
- היעדר קיומו של נוהל אבטחת מידע או קיומו של נוהל חסר;
- אי עריכת הסכמי מיקור חוץ עם ספקים והיעדר פיקוח ובקרה על הספקים;
- היעדר מעקב אחר אירועי אבטחת מידע והיעדר תיעוד בנושא;
- אי שימוש באמצעי פיזי הנתון לשליטתו המלאה של בעל ההרשאה בגישה למאגר;
- היעדר בחינת השאלה אם מועמד לעבודה אינו מתאים לקבלת גישה למידע מהמאגר, בעת הליך מיון עובדים.

עיקרי ההמלצות לארגונים:

- רישום מאגרי מידע שבבעלות הארגון;
- מינוי מנהל מאגר וממונה על אבטחת מידע (היכן שמינויו נדרש);
- קיום נהלי אבטחת מידע בארגון המתייחסים, בין השאר, לאבטחה פיזית, הרשאות גישה, התמודדות עם אירועי אבטחה, התקנים ניידים, מדיניות הסיסמאות ועוד, ועדכונם באופן עיתי;
- ביצוע הדרכות תקופתיות לכללי בעלי ההרשאות בטרם מתן גישה למידע;
- עריכת הליכי מיון לעובדים על מנת לוודא כי בעל ההרשאה מתאים לקבלת גישה למידע המצוי במאגר, בשים לב לרגישות המידע והיקף ההרשאות; יידוע נושאי המידע בדבר מקור הסמכות לאיסוף המידע על אודותיהם. ככל שלא קיים מקור סמכות בחוק, יש לקבל את הסכמת נושא המידע לצורך איסוף המידע ושמירת פרטיו במאגרי המידע;
- ככל שהארגון מסתייע בגורם חיצוני לצורך עיבוד מידע, יש לבחון, **בטרם ההתקשרות**, את סיכוני אבטחת המידע הכרוכים בהתקשרות ולערוך הסכם מול הגורם החיצוני, אשר יפרט את חובותיו ואחריותו של הספק ביחס לאבטחת מידע. במהלך ההתקשרות, יש לקיים פיקוח ובקרה ביחס לעמידת הגורם החיצוני בחובותיו;
- סיווג רמת אבטחת המידע של מאגרי המידע בהתאם לסוג המידע, מספר הרשומות במאגר ומספר בעלי הגישה. בהקשר זה, הרשות מדגישה כי רמת אבטחת המידע הנדרשת של מאגר מידע לא משתנה, גם אם מאגר המידע מנוהל או מעובד בצורה מפוצלת על גבי מספר מערכות טכנולוגיות שונות בעלות מספר בעלי הרשאה שונה. לפיכך, מספר בעלי ההרשאה שיש להביא בחשבון לצורך קביעת רמת האבטחה של המאגר הוא **סך כל בעלי ההרשאה** לכלל המערכות הטכנולוגיות המשמשות את מאגר המידע הרלוונטי;
- תיעוד אירועי אבטחה וגיבוש נוהל סדור בנושא אשר יתייחס, בין השאר, לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת הלקחים. במאגרי מידע ברמת אבטחה גבוהה או בינונית יש לקיים דיונים עיתיים באירועי האבטחה ולבחון את הצורך בעדכון הנוהל;
- עריכת ביקורות במאגרים ברמת אבטחה בינונית ומעלה בנושא הגנת הפרטיות ואבטחת מידע בארגון מדי 24 חודשים. במאגר מידע שחלה עליו רמת אבטחה גבוהה יש לבצע מבדקי חדירה אחת לשנה וחצי, ולבחון את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהם, לצד תיקון הליקויים שהתגלו במסגרת המבדקים;
- בחינה כי מערכות המאגר נשמרות במקום מוגן, המונע חדירה וכניסה ללא הרשאה. במאגרי מידע בעלי רמת אבטחה בינונית וגבוהה יש לנקוט באמצעים לבקרה ותיעוד של הכניסות והיציאות מאתרים בהם מצויות מערכות תשתית, חומרה וסוגי רכיבי תקשורת ואבטחת מידע;
- ניהול מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר ושמירת נתוני מנגנון הבקרה במשך 24 חודשים;
- עריכת בחינת עיתית, לפחות אחת לשנה, של קיום מידע עודף במאגר המידע ומחיקתו במידת הצורך;
- בחינת הצורך בחיבור התקנים ניידים והגבלת או מניעת אפשרות חיבורם;
- התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית ושימוש באמצעי פיזי הנתון לשליטתו של מורשה הגישה בעת הגישה למערכות המאגר. בעת האחרונה גבר השימוש באפליקציות ובאמצעים דיגיטליים בהקשר הקמעונאי, בין השאר לאור התגברות המסחר המקוון. כמו כן, גבר השימוש באמצעים טכנולוגיים גם בסניפי הגופים הקמעונאיים, ובכלל כך שימוש במצלמות ובאמצעי זיהוי ביומטריים מטעמי אבטחה וביטחון. כל אלו מגדילים את הסיכון לפגיעה בפרטיות הצרכנים ומחייבים הקפדה על רמת אבטחה נאותה ועל עמידה בהוראות הדין הרלוונטיות. **צוות הסייבר והפרטיות בגורניצקי מלווה ארגונים רבים בהטמעת דרישות הדין**

בתחום הסייבר והגנת המידע, וישמח לעמוד לרשותכם בכל שאלה בנושא.

עדכון זה נועד לספק מידע כללי ותמציתי בלבד. הוא אינו מהווה ניתוח מלא או שלם של הסוגיות הנידונות, אינו מהווה חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו.

אנשי קשר



רבקה גניס שפטובסקי
עורכת דין בכירה



אסף הראל
שותף