

דו"ח פיקוח רוחב במגזר התקשורת פורסם לציבור

עדכוני לקוחות

לאחרונה פרסמה הרשות להגנת הפרטיות ("הרשות") [דו"ח פיקוח רוחב במגזר התקשורת](#) ("הדו"ח"). מגזר התקשורת הוגדר כיעד פיקוח רוחב משמעותי על-ידי הרשות בשים לב למאפיינים הייחודיים של נותני השירותים בו (למשל ספקי תקשורת סלולארית, ספקי שירות אינטרנט וספקי ניטור ואיכון רכב) וכן למאפיינים הייחודיים של המגזר עצמו, הכוללים החזקה של מאגרי מידע גדולים ורגישים על לקוחות, וכן שימוש במגוון של שירותים שמצריכים עיבוד מידע בהיקף נרחב (למשל, טלפונים חכמים, אפליקציות מבוססות מיקום ומכשירי חשמל ביתיים המחוברים לאינטרנט).

הדו"ח מסכם הליך פיקוח רוחב שנערך בקרב 25 גופים הפועלים במגזר התקשורת, ובהם חברות המספקות שירותים בתחומי תקשורת קווית וסלולרית, ספקי אינטרנט (ISP) וכן ספקי שירותי אלחוט. במסגרת הליך הביקורת הרשות בחנה ארבעה קריטריונים עיקריים בתחום הגנת הפרטיות:

1. **בקרה ארגונית** – קיום תכנית עבודה בתחומי אבטחת מידע והגנת הפרטיות ומינויים של גורמים בעלי אחריות בתחום.

2. **ניהול מאגרי מידע** – אופן קבלת הסכמה לשימוש במידע, רמת התאמת השימוש ומתן הזכות לעיון במידע.

3. **עיבוד מידע על-ידי גורם חיצוני** – בחינת התקשוריות של בעלי מאגרי המידע עם צדדים שלישיים המחזיקים מידע.

4. **אבטחת מידע** – עמידת הגופים בהוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("התקנות") בכל הנוגע לניהול המידע האישי שבבעלותם.

ממצאי הדו"ח, בשקלול כלל התחומים שנבדקו, מלמדים כי בקרב מרבית הגופים במגזר התקשורת (80% מהם) נמצאה רמה גבוהה של עמידה בהוראות חוק הגנת הפרטיות, התשמ"א-1981 ("החוק") והתקנות; ביחס ל-16% מהגופים נמצאה רמת עמידה בינונית; וכי רק ביחס ל-4% מהגופים רמת עמידה נמוכה. התחום העיקרי בו נמצאה רמת עמידה נמוכה הוא בתחום אבטחת המידע (20% מהגופים).

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

- אי קיומו של מנגנון תיעוד אוטומטי שמאפשר בקרה על הגישה למערכות המידע;
- הימצאות מערכות הפעלה שאינן מעודכנות או נתמכות;
- היעדר שימוש באמצעי פיזי לצורך זיהוי משתמשים בגישה מרחוק למאגר המידע;
- אי הקפדה על הליכי מיון נאותים בטרם מתן גישה לעובדים;
- אי הטמעה של נוהל אבטחת מידע כנדרש בהתאם לתקנות ואי קיומה של תכנית לבקרה שוטפת על עמידה

בדרישות התקנות;

- אי קיום סקרי סיכונים או ביקורות בנושא אבטחת מידע;
- אי קיום ההוראות הנדרשות בהתקשרויות עם צדדים שלישיים המקבלים גישה למידע והיעדר פיקוח הולם על נקיטה באמצעי הגנה הולמים על ידם.

עיקרי ההמלצות לארגונים:

- ניהול הגישה למאגר – ביטול הרשאות לעובדים שסיימו את תפקידם; הטמעת מנגנון גישה באמצעות אמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה; הגבלת חיבור התקנים ניידים למערכות המאגר; קביעת הוראות בעניין הגישה למאגר במסגרת נוהל האבטחה; והטמעה של מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר, שנתוניו יישמרו למשך 24 חודשים לפחות.
- הגנה על מערכות המאגר – ביצוע מבדקי חדירות וסקרי סיכונים כנדרש בהתאם לרמת האבטחה של מאגר המידע (להרחבה בנושא, ראו [כאן](#)); קיום הפרדה בין מערכות המאגר לבין מערכות מחשוב אחרות; שימוש בשיטות הצפנה מקובלות; והטמעה של מנגנוני אבטחה פיזית.
- טיפול באירועי אבטחת מידע – תיעוד כל מקרה בו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה (ככל הניתן, באופן אוטומטי); קביעת הוראות בעניין התמודדות עם אירועי אבטחה במסגרת נוהל האבטחה; וקיום דיונים עיתיים באירועי אבטחה.
- מינוי בעלי תפקידים בהתאם לדרישות החוק והתקנות – למשל, מינוי ממונה על אבטחת מידע. בהקשר זה נזכיר כי עם כניסת תיקון 13 לחוק לתוקף (בחודש אוגוסט 2025) גופים מסוימים יחויבו גם במינוי ממונה על הגנת הפרטיות (להרחבה בנושא תיקון 13 לחוק, ראו [כאן](#)).
- הטמעת נהלים – הטמעה של נהלי אבטחת מידע ארגוניים המתייחסים לאבטחה פיזית, הרשאות גישה, אמצעי הגנה, התמודדות עם אירועי אבטחה, ניהול התקנים ניידים וכיו"ב. בכלל כך, נדרש לוודא הטמעה של נוהל אבטחת מידע ולעדכן את הנוהל באופן עיתי. בנוסף, יש להטמיע תכנית לבקרה שוטפת על העמידה בדרישות החוק והתקנות.
- הליכי מיון לעובדים וקיום הדרכות – עריכה של הליכי מיון מתאימים לעובדים שמקבלים גישה למערכות המאגר, כאשר במסגרת הליכים אלו ייבדקו, בין השאר, אמינות העובד ויכולתו לשמור על סודיות. כמו כן, יש להקפיד על קיום הדרכות לעובדים בטרם הענקת הרשאת גישה למאגר או עם שינויה, וכן באופן תקופתי כנדרש בהתאם לרמת האבטחה של מאגר המידע.
- מיקור חוץ – עריכת הסכם כנדרש בהתאם להוראות תקנה 15 לתקנות ובהתאם להנחיית רשם מאגרי המידע מס' 2/2011 בנושא שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי; וכן פיקוח על פעילות הגורם החיצוני ועמידתו בהוראות ההסכם, החוק והתקנות.

פעילות הגופים במגזר התקשורת כרוכה בסיכונים רבים ומשמעותיים לפגיעה בפרטיות ובהתאם נדרשים הגופים הפועלים במגזר זה להקפיד הקפדה יתרה על קיום הוראות החוק והתקנות ולקיים בקרה על מאגרי המידע שברשותם. דברים אלו אף מקבלים משנה תוקף לאחר חקיקת תיקון 13 לחוק, במסגרתו סמכויותיה של הרשות להגנת הפרטיות הורחבו באופן משמעותי, כך שעתה תהיה מוסמכת הרשות להטיל עיצומים כספיים בגין הפרות של החוק והתקנות בהיקף שעשוי להסתכם במיליוני שקלים.

אנו בגורניצקי מלווים ארגונים רבים בהטמעת דרישות הדין בתחום הפרטיות ואבטחת המידע, ובכלל כך חברות

הפועלות בתחום התקשורת, ונשמח 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



אסף אבטובי
שותף



ליאור פורת
שותף מנהל