

עדכון לקוחות: דו"ח פעילות מערך פיקוח הרוחב ברשות הגנת הפרטיות

החודש פרסמה רשות הגנת הפרטיות דו"ח המסכם את פעילותו של מערך פיקוח הרוחב בשנים 2018-2020.

מערך פיקוח הרוחב ברשות הגנת הפרטיות הוקם בשנת 2018 ומטרתו לקיים פיקוחי רוחב לפי נושא מסוים או כלפי מגזר מסוים, כדי לבדוק את רמת קיום הוראות הדין בנושא או במגזר הרלוונטי, לאתר כשלים והפרות ולהגביר מודעות.

הליך פיקוח הרוחב כולל שלבים מקדמיים פנימיים ברשות, ולאחר מכן מופצים שאלוני פיקוח, מופקים דו"חות ביניים, נשלחות דרישות להשלמת ידיעות ומסמכים, הרשות נותנת הנחיות לתיקון ליקויים ולבסוף מפרסמת דו"ח מגזרי ודורשת התחייבות בכתב מנושא משרה בכיר בארגון המפוקח לגבי תיקון הליקויים תוך ציון לוחות זמנים לגביהם.

בכל אחת מן השנים שנסקרות בדו"ח בוצעו מעל 200 פיקוחי רוחב, על מגוון רחב של מגזרים, כולל, בין היתר, חברות המנהלות מידע על מועדוני לקוחות, חברות המספקות שירותי אחסון ועיבוד מידע, סוכנויות ביטוח, חברות כוח אדם והשמה, קופות גמל וקרנות השתלמות וגופים במגזר הקמעונאי.

על פי הדו"ח, בחודש הבא צפויים להסתיים הליכי הפיקוח המתנהלים היום בתחומים שונים, כולל תחבורה דיגיטלית ואפליקציות תשלום מבוססות מיקום, אפליקציות בתחום הבריאות הדיגיטלית וגופי תקשורת.

עוד עולה מן הדו"ח כי הרשות מבצעת פיקוחי מעקב מדגמיים במטרה לוודא את אופן הטיפול של הגופים הרלוונטיים בליקויים עליהם הצביעה הרשות, כאשר גוף שלא תיקן את הליקויים עשוי להיות כפוף לסנקציות מצד הרשות, העומדות לה על פי דין. גוף שלא משתף פעולה או שנמצאו בו ליקויים חמורים עשוי להיות חשוף להליכים מנהליים או פליליים שנמצאים בסמכותה של הרשות.

מעניין גם לראות שהרשות מבצעת מעין פיקוחים "חוזרים" או "משלימים", אשר בוחנים גופים חדשים במגזרים שכבר נבחנו בעבר.

הרשות מציינת כי המשותף למגזרים השונים שנבחנו עד כה הוא קיומם של סיכונים הנובעים מהסתמכות על מיקור חוץ, מהיכולת לבצע הצלבת מידע בין מאגרי מידע וכן סיכונים אבטחת מידע.

הדו"ח מפרט את הקריטריונים שעל פיהם הרשות קובעת את רמת הסיכון, כלי שמסייע לה להחליט באילו מגזרים עליה להתמקד ולבצע לגביהם פיקוחי רוחב. מדובר בקריטריונים הבאים: כמות נושאי המידע, כמות המידע שנשמר על כל אדם, רגישות המידע, משך שמירת המידע, כמות המידע שמועבר, כמות הממשקים החיצוניים למערכת המידע, סיכוי לנזק ממשי כתוצאה מגילוי המידע, קישור חזק של המידע לזהות, האפשרות להשתמש במידע לצורך אחר, מודעות נושאי המידע לשימוש במידע, איסוף מידע בהסכמת נושאי המידע ושימוש במידע בהסכמת נושאי המידע.

בין המגזרים שאותם דירגה הרשות ככאלה המצויים בסיכון גבוה ניתן למצוא מועדוני לקוחות וחברות שעוסקות במתן שירותי אחסון ועיבוד מידע (הכוונה היא ל"מחזיקים" הנותנים שירותי SAAS, PAAS, IAAS, כולל חברות שמעניקות שירותי אירוח אתרים, פיתוח אפליקציות ופיתוח של ממשקים שונים).

בנוסף, עולים מן הדו"ח שני היבטים מעניינים בהקשר של אבטחת מידע: (1) הרשות מציינת כי שימוש בספק שירותי ענן לא מהווה כשלעצמו עמידה אוטומטית בהוראות הדין בעניין אבטחת מידע, אלא נדרשת רכישה של שירותי אבטחה ספציפיים או נקיטת צעדי אבטחה עצמאיים נוספים; (2) הנחיית רשם מאגרי מידע בעניין תחולת תקנות אבטחת מידע על גופים שעומדים בתקן SO27001 ורלוונטיות רק עבור גופים שמחזיקים בתעודת הסמכה של התקן וגם מקיימים בפועל את הוראותיו, כאשר הרשות מבהירה שהנחיה זו לא תחול על גוף שהרשות מצאה שהוא אינו מקיים בפועל את הוראות התקן, וזאת גם אם גוף כאמור מחזיק בתעודת הסמכה.

בנוסף, הרשות מציינת כי במסגרת פיקוחי הרוחב בשנים 2019-2020 הופיעה בשאלוני הפיקוח שאלת רשות לגבי מינויו של ממונה הגנת פרטיות בארגון, למרות שלא מדובר בחובה שבדין. מן הנתונים עולה כי יש ממוני הגנת פרטיות ברשויות מקומיות, בתי אבות, סוכנויות ביטוח, מוקדים טלפוניים, מרכזי מימוש זכויות רפואיות, תאגידי מים וחברות סיעוד. במגזר האחרון אחוז המשיבים בחיוב לשאלה זו הוא הגבוה ביותר.

עוד עולה בהקשר זה כי בשל פיקוח הרוחב מונה ממונה הגנת פרטיות ב-40% ממועדוני הלקוחות שנבחנו.

אנחנו עומדים לרשותכם לכל שאלה,

בברכה,

עו"ד אייל שגיא, עו"ד שיר שושני-כץ
וצוות מחלקת משפט וטכנולוגיה



ShirS@ayr.co.il



EyalS@ayr.co.il