דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב
בקרב מגזר תקשורת

תוכן עניינים

1. תקציר מנהלים

מערך פיקוח הרוחב ברשות להגנת הפרטיות, מופקד על עריכת פיקוחי רוחב מגזריים או נושאיים לבחינת יישום הוראות חוק הגנת הפרטיות, התשמ"א- 1981 (להלן: "חוק הגנת הפרטיות" או "החוק") ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "תקנות הגנת הפרטיות (אבטחת מידע)" או "התקנות") במטרה לאתר הפרות של החוק והתקנות, לשם הגברת מודעות המשק להוראות החוק, הגברת האכיפה היזומה של הרשות, לאתר כשלים ענפיים וכלל-משקיים הדורשים התייחסות מוגברת של הרגולטור, וקבלת תמונת מצב כלל-מגזרית לגבי עמידה בהוראות החוק והתקנות.

1.1. מגזר תקשורת

במסגרת סקר רוחבי שערכה הרשות להגנת הפרטיות, אשר בוחן את סיכוני הפרטיות במגזרים השונים, נקבע מגזר התקשורת כאחד מיעדי פיקוח הרוחב המשמעותיים, וזאת בשל מאפייניו הייחודיים של מגזר זה המהווים סיכון בהיבטי הפרטיות, הבאים לידי ביטוי במספר היבטים:

1. איסוף והחזקה של מאגרי מידע עצומים ורגישים כגון מאגר נתוני תקשורת ומידע אודות הרגלי צריכה של לקוחות, אשר ניתן להפיק מהם ערך רב, לרבות ערך כלכלי.
2. מגזר התקשורת מבוסס על מגוון רחב של שירותים המצריכים עיבוד מידע בהיקף נרחב על ידי נותני שירותי תקשורת ובכלל זה: שימוש נרחב בטלפונים סלולריים חכמים, ישומונים מבוססי מיקום, מצלמות האבטחה במרחב הציבורי, מכשירים חשמליים בבית (IOT) ועוד.
3. במגזר תקשורת נכללים מספר סוגים של נותני שירותים אשר לכל אחד מהם מאפיינים ייחודיים בהיבטי הפרטיות: ספקי תקשורת סלולארית, ספקי שירותי תקשורת קווית פנים-ארצית, ספקי שירותי אינטרנט, ספקי שירותי זימון, ניטור ואיכון רכב.

ניהול מאגרי מידע, בהתייחס למאפייניו הייחודיים של המגזר, מחייב את הגופים במגזר זה לעמוד בדרישות חוק הגנת הפרטיות ותקנות אבטחת המידע ביתר שאת, לרבות קיום חובות אבטחת מידע, קיום בקרה ארגונית ועמידה בהוראות החוק בכל הנוגע לחובת היידוע.

נוכח כל אלה הרשות להגנת הפרטיות הגדירה מגזר זה כיעד פיקוח רוחב משמעותי.

1.2. תהליך העבודה

כחלק מפעילות הליך פיקוח הרוחב פנתה הרשות בדרישה למילוי שאלוני ביקורת ל- 34 גופים

במגזר תקשורת (15 חברות המספקות שירותים בתחומי תקשורת קווית וסלולרית, 13 ספקי אינטרנט (ISP) ו-6 ספקי שירות אלחוט).מתוך הגופים הללו, השיבו על השאלון 25 גופים. בחלק מן המקרים נדרשו הגופים בהמשך לספק מידע, מסמכים והבהרות נוספות לרשות. שאלוני הביקורת בחנו שלושה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית וממשל תאגידי, ניהול מאגרי מידע ואבטחת מידע.

הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם, המעידים על רמת עמידתם בהוראות חוק הגנת הפרטיות ובתקנות מכוחו.

לאחר קבלת השאלונים המלאים מהגופים המפוקחים, בחנה הרשות את המענה והמסמכים הנלווים. בסיום ההליך, נמצאו ליקויים הדורשים תיקון בכלל הגופים שנבדקו, ובהתאם דרשה הרשות מאותם גופים לתקן את הליקויים שנמצאו, ולספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים.

כחלק מההליך, בדקה הרשות באמצעות ביקורת חוזרת את אופן תיקון הליקויים בחלק מן הגופים. ממצאי הביקורת החוזרת העלו כי הגופים שיפרו את עמידתם בהוראות החוק והתקנות באופן משמעותי.

1.3. ליקויים, מסקנות והמלצות עיקריות

ממצאי פיקוח הרוחב עלה כי ככלל במגזר התקשורת נמצאה רמת עמידה גבוהה בהוראות חוק הגנת הפרטיות ובתקנות.מבחינת אבטחת מידע, נמצא כי 20% מהגופים שנבדקו נמצאים ברמת עמידה נמוכה בהוראות החוק והתקנות.

מבחינת בקרה ארגונית, נמצא כי 12% מהגופים שנבדקו נמצאים ברמה עמידה בינונית בהוראות החוק והתקנות.

מבחינת ניהול מאגרי מידע, נמצא כי 16% מהגופים שנבדקו נמצאים ברמת עמידה בינונית בהוראות החוק והתקנות.

לאור הממצאים שעלו מהליך פיקוח הרוחב, נשלחו הנחיות ספציפיות לתיקון ליקויים ל- 25 הגופים שהשיבו לשאלון. כמו כן, לאור בחינת כשלי המגזר, כולל דו"ח זה הנחיות לכלל הגופים הפועלים במגזר זה, באשר לצעדים שעליהם לנקוט בכדי לעמוד בדרישות החוק והתקנות.

ממצאי הליך פיקוח רוחב בקרב מגזר התקשורת

דו"ח פיקוח רוחב 2021-2022

אתגרים ומאפיינים ייחודיים של מגזר תקשורת

גופי התקשורת אוגרים מידע יחודי – "נתוני תקשורת", המהווים מידע רגיש במיוחד

מכשירים סלולריים המשמשים בתהליך התקשורת הינם אמצעי אישי המכיל מידע אישי רב

הגופים במגזר התקשורת אוגרים מידע רב אודות הרגלי הצריכה של לקוחותיהם

התהליך שבוצע במספרים

34 שאלונים שהופצו

9 גופים שלא שהשתתפו בפועל בהליך הפיקוח

25 מספר מפוקחים שענו על השאלון במלואו

25 הנחיות לתיקון ליקויים

- מיקור חוץ (עיבוד מידע על-ידי גורם חיצוני) - בהתאם לתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע, את סיכוני אבטחת המידע הכרוכים בהתקשרות. בנוסף, על הגופים, בעלי המאגר, לוודא עריכת הסכם מול כל גורם חיצוני עימו הם התקשרו לצורך קבלת שירות הכרוך במתן גישה למאגר, כאשר יש לקבוע במפורש בהסכם את כל הוראות תקנה 15(א)(2) לתקנות הגנת הפרטיות (אבטחת מידע).

- על הגופים להקפיד בכל פנייה המהווה פנייה בדיוור ישיר כהגדרתה בסעיף 17ג' לחוק, על ציון הפרטים המנויים בסעיף 17ו' לחוק - לרבות ציון כי הפניה היא בדיוור ישיר, זהותו ומענו של בעל מאגר המידע, מקור המידע, הגורמים להם נמסר המידע וכד'.

- בגוף המחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8, יש למנות ממונה על אבטחת מידע שיהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחרת הכפוף ישירות למנהל המאגר.

- יש לערוך ביקורות בנושא אבטחת מידע והגנת הפרטיות מדי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה.

- יש להבטיח כי מערכות המאגר יישמרו במקום מוגן, המונע חדירה וכניסה ללא הרשאה התואמת את אופי פעילות המאגר ורגישות המידע בו. במאגרי מידע עליהם חלה רמת אבטחת מידע בינונית או גבוהה על בעל המאגר לנקוט בנוסף באמצעים לבקרה ולתיעוד של הכניסות והיציאות מאתרים שבהם מצויות מערכות תשתיות, חומרה, סוגי רכיבי תקשורת ואבטחת מידע, ושל כל הכנסה והוצאה אל מערכות המאגר ומהן.

- תיעוד כל אירוע המעלה חשש לאירוע אבטחה, בנוסף נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחה מידע.

- יש לבחון את הצורך בחיבור התקנים ניידים ולפעול להגבלת או מניעת אפשרות לחיבור התקנים ניידים. במקרים בהם יוגדר כי קיים צורך בשימוש בהתקנים ניידים יש להצפין את הנתונים תורשימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.

- התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב במאגר המידע המחוברים לרשת האינטרנט או לרשת ציבורית אחרת בהתאם לדרישות התקנות.

- במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע מבדקי חדירה אחת לשנה וחצי, תוך בחינת הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת המבדקים.

2.1. כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין השנים 2021-2022 במגזר התקשורת.

2.2. רקע על המגזר

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר התקשורת כיעד פיקוח רוחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר, כדלהלן:

מידע שעשוי להיות בעל רגישות מיוחדת, בין היתר, בשל רגישות והיקפי המידע, האתגרים הטכנולוגיים, מגוון רחב של שירותים המצריכים עיבוד מידע בהיקף נרחב, מספר סוגים של נותני שירותים אשר לכל אחד מהם מאפיינים מיוחדים ועוד.

<u>תוכן מידע אישי, סודי ובעל יסודות צנעת הפרט</u>

מגוון השירותים התרחב ויחד עימו התרחב גם היקף המידע המעובד על ידי נותני שירותי תקשורת ובכלל זה: שימוש נרחב בטלפונים סלולריים חכמים, ישומונים מבוססי מקום, מצלמות האבטחה במרחב הציבורי, מכשירים חשמליים בבית (IOT) ועוד.

<u>התפתחות טכנולוגית</u>

ההתפתחות הטכנולוגית בעשורים האחרונים הביאה עימה שינויים רבים, במסגרתם הפך מידע למשאב מרכזי בחיי הפרט ובחיי הכלל, ולמשאב רב ערך, לרבות ערך כלכלי. לגורמים רבים יש אינטרס באיסוף המידע, בשמירתו ולעיתים אף במכירתו לשם רווח.

2.3. תהליך עבודה

במטרה לפעול באופן המיטבי למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, הרשות להגנת הפרטיות נוקטת בגישה מבוססת סיכון, הבוחנת באופן תדיר את אפקטיביות מהלכיה ואת פוטנציאל ההשפעה הרוחבית שיש לפעולותיה על המשק, על מנת לעמוד במכלול האתגרים העומדים לפתחה. הרשות פועלת על-פי תהליך הערכת מצב שנתי סדור המנתח את הסיכונים לפרטיות בכלל מגזרי המשק. סקר סיכוני פרטיות ממקד את תחומי הפעילות של הרשות ומאפשר לה לעסוק, בין היתר, בתחומים בהם ישנה השפעה רוחבית על מגזרים שונים, הכוללים מספר רב של משתמשים ומידע רגיש, וליישם את ממצאי הפעילות בצורה רוחבית.

תהליך העבודה של הליך פיקוח הרוחב כולל בתוכו מספר שלבים מובנים, החל משלב בניית תכנית העבודה השנתית ובחירת מגזרי הפיקוח בהתאם לתחומים בסיכון מוגבר לפרטיות שזיהתה הרשות, ולמדיניות השנתית של הרשות. התוכנית נבנית בהתחשב בקריטריונים הבאים: כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר

ברשות בנוגע למגזר או לנושא מסוים, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה מגזרית והבאת הגופים המשתייכים למגזר לרמת עמידה התואמת את דרישות החוק והתקנות.

הליך הפיקוח החל ב- 34 גופים המשתייכים למגזר תקשורת שנבחרו על ידי הרשות. במסגרת ההליך, 25 גופים השיבו לשאלוני הפיקוח. מתוכם, 4 גופים קיבלנו ציון בינוני ואחד קיבל ציון נמוך.
בסיום ההליך, בכלל הגופים שהשיבו לשאלון נמצאו ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות את הגופים לתקן את הליקויים שנמצאו, לספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה בדבר יישומה.

2.4. הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו

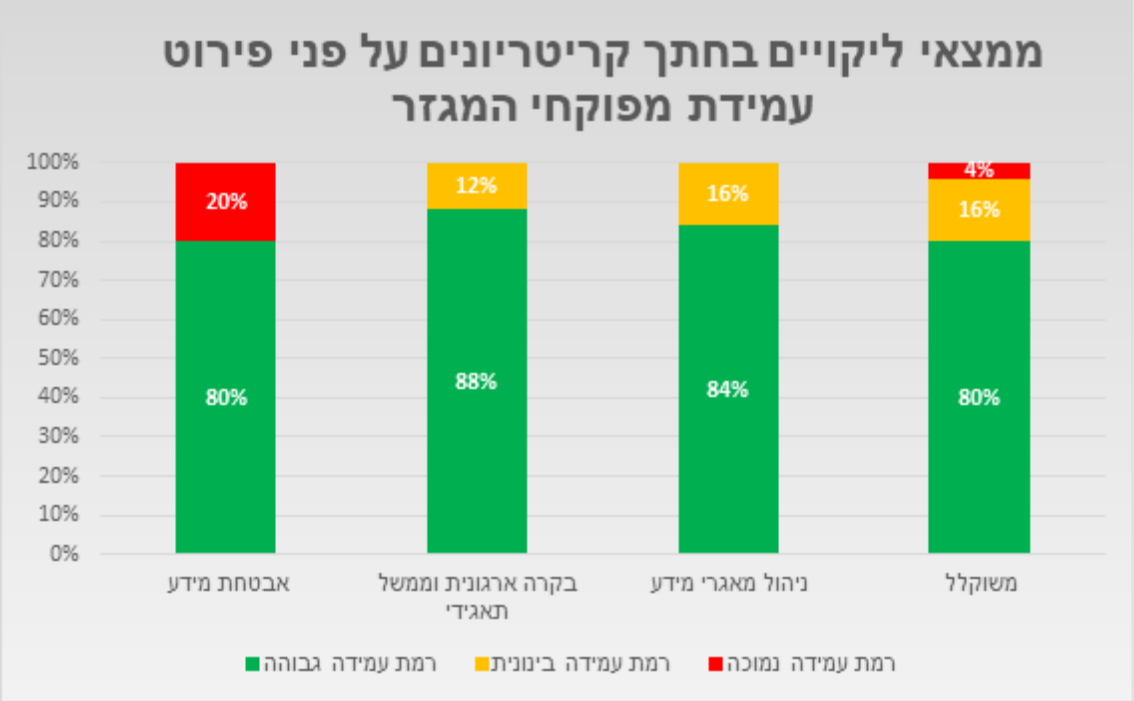
במטרה לבחון את רמת העמידה המגזרית בהוראות החוק והתקנות, פנתה הרשות כאמור בדרישה למילוי שאלוני ביקורת המתייחסים לקריטריונים שונים ובהם:[1]

רמות העמידה ביחס לקיום הוראות חוק הגנת הפרטיות והתקנות מכוחו נקבעו בהתאם לשקלול הציונים שקיבלו הגופים במגזר, וזאת בהתבסס על בחינת הרשות את תשובותיהם לשאלוני הביקורת והמידע שנאסף במסגרתו:

[1] קריטריון עיבוד מידע אישי על-ידי גורם חיצוני נבחן בהליך זה כקריטריון משנה תחת ניהול מאגרי מידע.

- עמידה של בין 100% - 80% מהקריטריונים, מוגדרת כרמת עמידה גבוהה;
- עמידה של בין 50% - 80% מוגדרת כרמת עמידה בינונית או חלקית;
- עמידה של מתחת ל-50% מוגדרת כרמת עמידה נמוכה.

2.5 ממצאים – ליקויים מרכזיים לפי קריטריונים במבט השוואתי והמלצות:



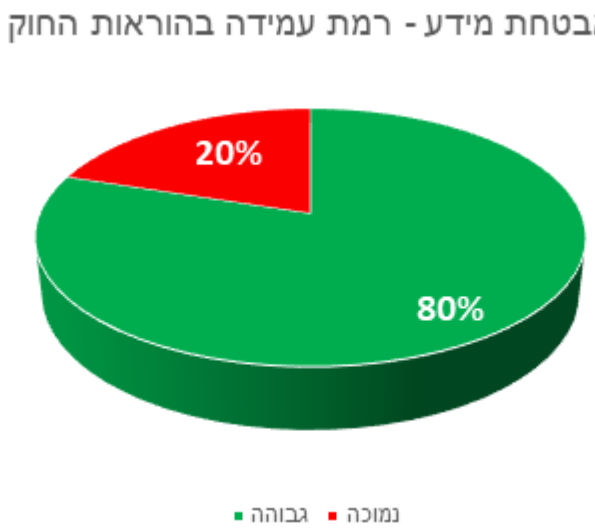
בתחום אבטחת מידע כ- 20% מן הגופים נמצאים ברמה נמוכה בעמידה בהוראות החוק והתקנות.

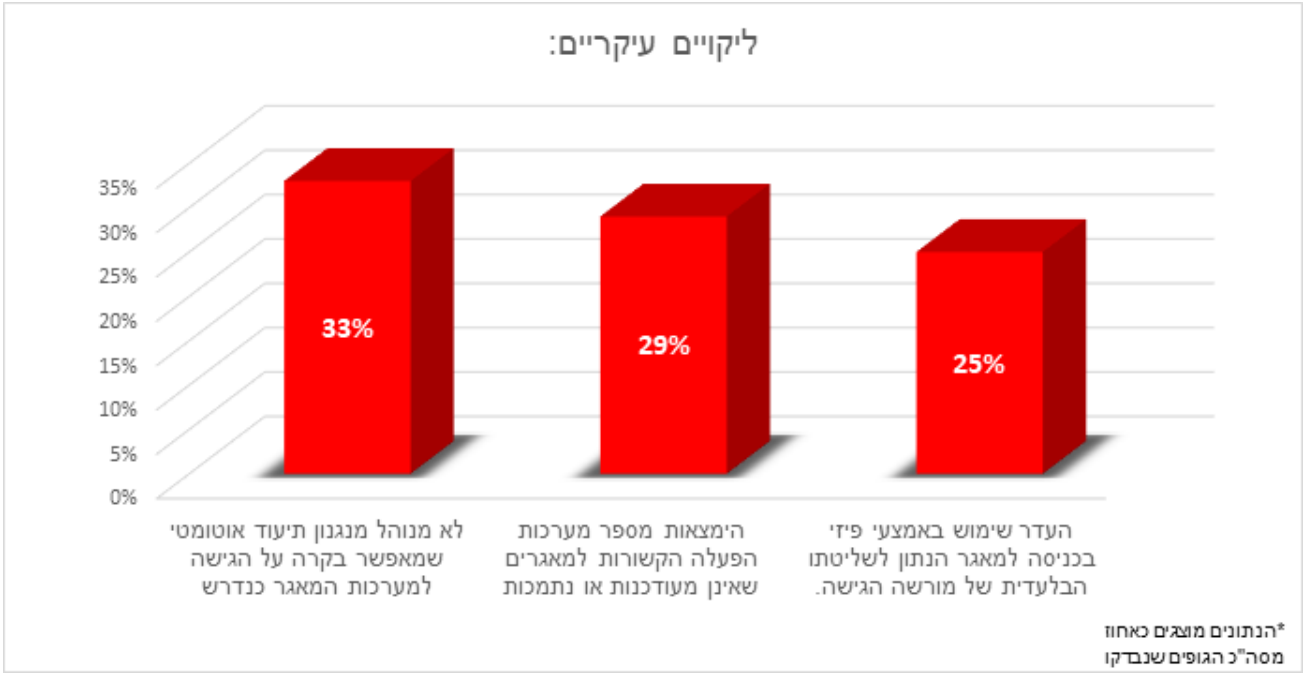
בתחום ניהול מאגרי מידע, כ- 16% מן הגופים נמצאים ברמת עמידה בינונית בלבד בהוראת החוק.

בתחום בקרה ארגונית וממשל תאגידי, נמצא כי 12% מהגופים עמדו ברמה בינונית בלבד בהוראות החוק.

אבטחת מידע

ממצאים:





*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

המלצות:

נוכח הפערים שנמצאו בקריטריון זה, נמצא כי על הגופים המפוקחים לחזק את נושא אבטחת המידע בנושאים הבאים:

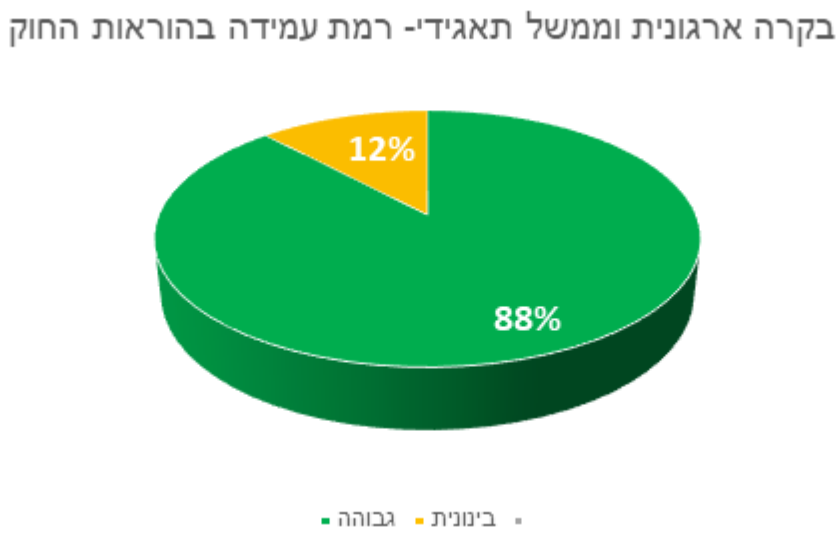
- **גישה למערכות המאגר**:
  - יש לבטל הרשאות בכל המאגרים לבעל הרשאה שסיים את תפקידו, מיד עם סיום תפקידו, לרבות לעניין מעבר תפקידים ככל שרלוונטי.
  - בהתאם לקבוע בתקנה 14(ג) לתקנות הגנת הפרטיות (אבטחת מידע), בחיבור מרחוק למאגר ברמת אבטחה בינונית או גבוהה יש לוודא שהגישה של בעל הרשאה למערכות המאגר תתבצע באמצעות אמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה, וכן גורם המתקשר עם המאגר, קרי לקוח קצה, יזוהה על-ידי בעל במאגר במנגנון הזדהות נוסף אחר.
  - בהתאם לקבוע בתקנה 12 לתקנות הגנת הפרטיות (אבטחת מידע), בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה.
  - בהתאם לתקנה 9(ב)(2) לתקנות הגנת הפרטיות (אבטחת מידע), ברמת אבטחה בינונית ומעלה, הגופים נדרשים לקבוע בנוהל אבטחת מידע הוראות, בהתאם לאופי המאגר וטיבו, כדי לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות. כמו כן, יש לקבוע בנוהל אבטחת מידע הוראות לעניין ניתוק אוטומטי לאחר פרק זמן של אי פעילות במערכות המאגר.
  - בנוסף ובהתאם לתקנה 9(ב)(2) לתקנות הגנת פרטיות (אבטחת מידע) במאגרים בעלי רמת אבטחה בינונית ומעלה, נדרשים הגופים לקבוע בנוהל אבטחת המידע את אופן הזיהוי בעת גישה למאגרי המידע, ובאשר אופן הזיהוי מבוסס על סיסמאות הנוהל יתייחס גם לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד מורשה הגישה, ובכל מקרה לתקופה שלא תעלה על שישה חודשים.
  - בהתאם לתקנה 8(א) לתקנות הגנת הפרטיות (אבטחת מידע), על הגופים לקבוע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.
  - במאגרי מידע ברמת אבטחה בינונית ומעלה על הגופים ליישם מנגנון תיעוד אוטומטי, שיאפשר ביקורת על הגישה למערכות המאגר ויכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם

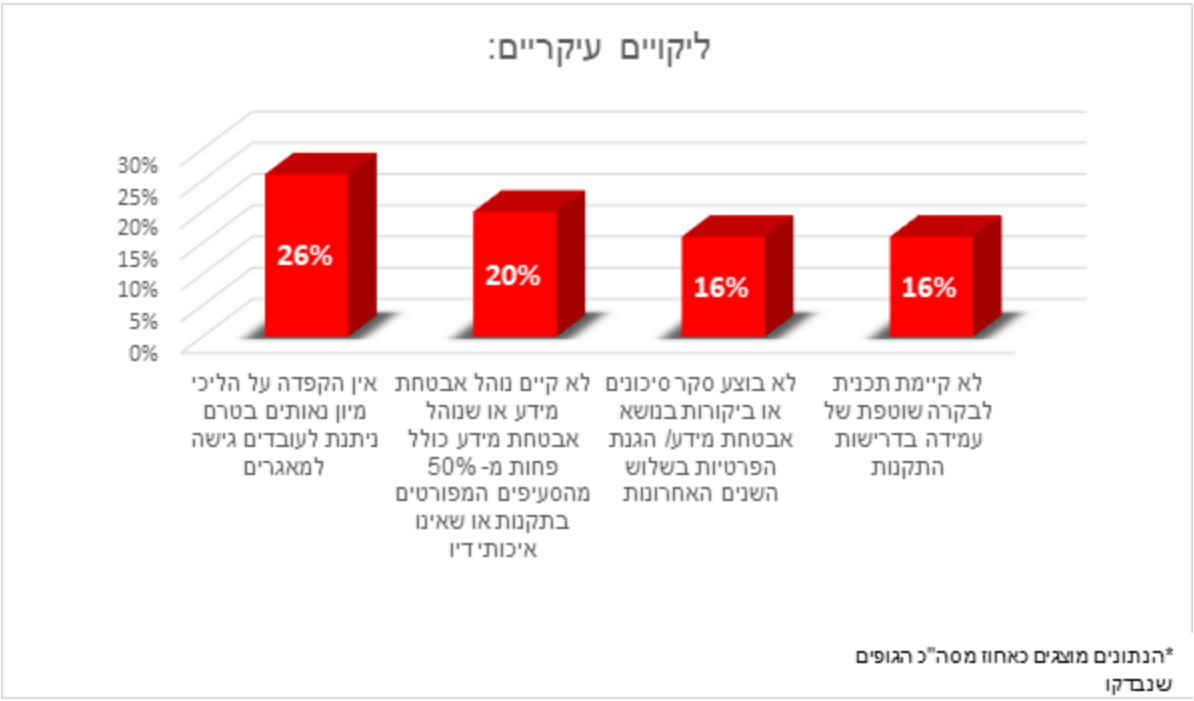
הגישה אושרה או נדחתה, כנדרש בתקנה 10. נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות. על בעל מאגר המידע לקבוע נוהל בדיקה שגרתי עבור נתוני התיעוד של מנגנון הבקרה.

- **הגנה על מערכות המאגר**:
  - במאגר מידע שחלה עליו רמת אבטחה גבוהה- יש לבצע מבדקי חדירות מידי שנה וחצי, בחינת הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת המבדקים.
  - במאגר מידע שחלה עליו רמת אבטחה גבוהה יש לבצע סקר סיכונים על ידי גורם חיצוני מקצועי ובלתי תלוי מידי אחת לשנה וחצי, בחינה את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת הסקר.
  - יש לקיים הפרדה, בהיקף ובמידה הסבירים האפשריים, בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר בהתאם לתקנות.
  - העברת מידע ממאגרי המידע ברשת ציבורית או האינטרנט תיעשה באמצעות שימוש בשיטות הצפנה מקובלות בלבד (TLS 1.2 ומעלה).
  - בנוסף, על הגופים המפוקחים לנקוט באמצעים מספקים בכדי למנוע חדירה למיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים או המאפשרים גישה אל מאגרי המידע. כמו כן, עליהם לוודא שבכניסה לאתר מאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה על פי תקנות אבטחת מידע (תקנה 9(ב)(2)).
- **טיפול באירועי אבטחת מידע**:
  - עפ"י תקנה 11 לתקנות הגנת פרטיות (אבטחת מידע), על הגופים לתעד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה (להלן- אירועי אבטחה) אשר יבוסס ככל האפשר על רישום אוטומטי. עוד נדרש כי, נוהל האבטחה יכלול התייחסות לאופן ההתמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן לעניין דיווח על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.
  - בעל מאגר ברמת אבטחה בינונית יקיים אחת לשנה דיון באירועי האבטחה ויבחן את הצורך בעדכון נוהל האבטחה, במאגר מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני באירועי האבטחה ולבחון את הצורך בעדכון נוהל האבטחה.

1.1. בקרה ארגונית וממשל תאגידי

ממצאים:





*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

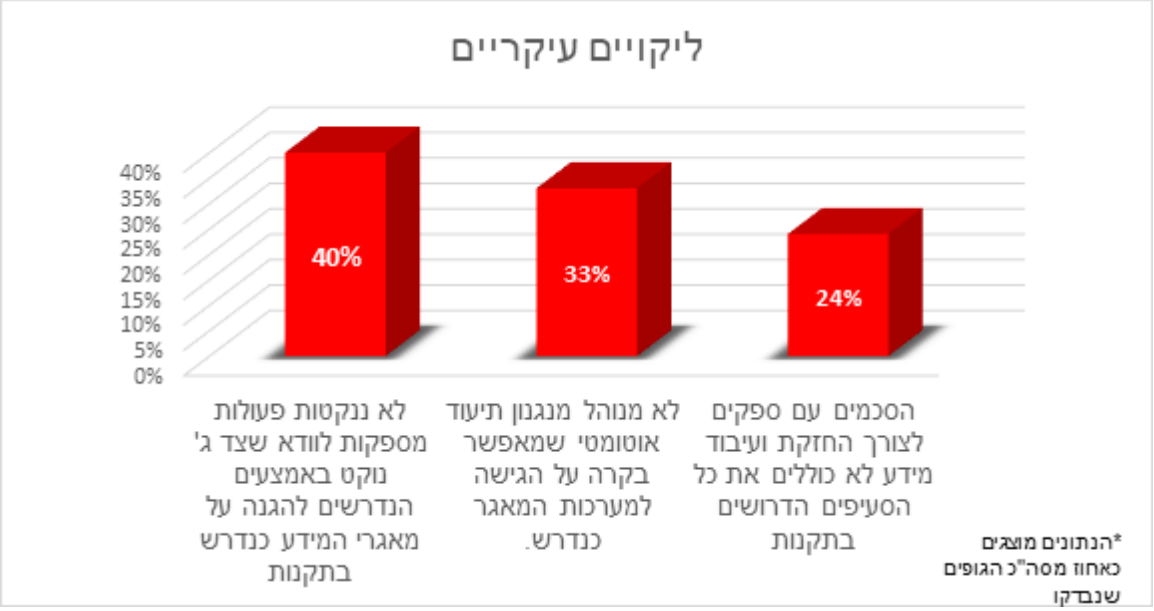
המלצות:

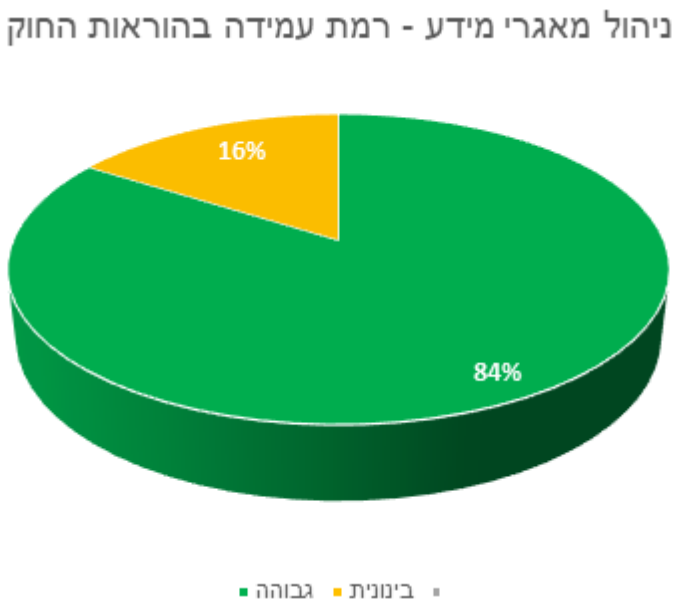
נוכח הפערים שנמצאו בקריטריון זה, נמצא כי על הגופים המפוקחים לחזק את נושא בקרה ארגונית וממשל תאגידי בנושאים הבאים:

- על הגופים לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות הוצאות כתב מינוי רשמי למנהל המאגר ולממונה אבטחת המידע ככל שהדבר נדרש לפי הוראות סעיף 17ב לחוק, וכן לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות אבטחת מידע.
- על הגופים למנות ממונה על אבטחת מידע שיהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה הכפוף ישירות למנהל המאגר, בהתאם לתקנה 3 לתקנות הגנת הפרטיות (אבטחת מידע). הגופים נדרשים, בין היתר, לוודא כי ממונה אבטחת המידע אינו משמש בתפקיד נוסף שיכול להעמיד אותו בניגוד עניינים.
- כמו כן, על הגופים המפוקחים לוודא כי קיימים נהלי אבטחת מידע בארגון הכוללים התייחסות לנושאים כגון: אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, הוראות למורשה גישה, ניהול סיכונים, התמודדות עם אירועי אבטחת מידע, התקנים ניידים וכו'. בנוסף, יש לעדכן את נוהל אבטחת המידע ולבחון את עדכניותו אחת לשנה, כנדרש בתקנה 4 לתקנות הגנת הפרטיות (אבטחת מידע).
- על פי תקנה 7(ג) לתקנות הגנת הפרטיות (אבטחת מידע) על הגופים לקבוע הדרכות תקופתיות לעובדים, לפחות פעם בשנתיים במאגרים שחלה עליהם רמת אבטחה בינונית או גבוהה, בנושא אבטחת מידע והגנת הפרטיות וניהול תיעוד ומעקב אחר הדרכות אלו.
- בנוסף, בהתאם לנדרש בתקנות אבטחת מידע (תקנה 7), על הגופים המפוקחים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או לכל גורם אחר שמקבל גישה למאגר או למערכת הכוללת מספר מאגרים. יש להקפיד כי במסגרת הליך קליטת עובדים, משולבים תהליכי מיון נאותים (בדגש על אמינות, שמירת סודיות וכיוצ"ב) בטרם ניתנת להם גישה למאגרים.
- על הגופים להקפיד על ביצוע הדרכות לעובדים לפני מתן או שינוי הרשאות גישה.
- על הגופים לגבש תוכניות לבקרה שוטפת על העמידה בדרישות החוק והתקנות כנדרש בתקנה 3(3) לתקנות הגנת הפרטיות (אבטחת מידע).

1.2. ניהול מאגרי מידע

ממצאים:





המלצות:

נוכח הפערים שנמצאו בקריטריון זה, נמצא כי על הגופים המפוקחים לחזק את נושא ניהול מאגר המידע בנושאים הבאים:

- על הגופים לאפשר לנושא המידע לממש את זכותו החוקית לעיון במידע אודותיו בהתאם לסעיף 13 לחוק, בכלל מאגרי המידע.
- על הגופים לאפשר לנושא המידע לבקש לתקן או למחוק את המידע אודותיו המוחזק במאגר המידע, במידה ומצא כי המידע עליו אינו נכון, שלם, ברור או מעודכן בהתאם לסעיף 14 לחוק.
- בעת שימוש בשירותי מיקור חוץ נדרש לפעול בהתאם להוראות תקנה 15 וכן ליישם את הוראות הנחיית רשם מאגרי מידע מס' 2/2011 בנושא שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי[2]. על המפוקחים לוודא כי כל גורם חיצוני הנותן שירותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע, תוך נקיטה באמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות.
- על הגופים לעגן במסמך ההתקשרות התייחסות לחובותיו ואחריותו של הספק, בהתאם להוראות התקנות, לרבות:
  - דיווח אודות אירועי אבטחת מידע.
  - מנגנוני אבטחת המידע הנדרשים.
  - שמירת המידע לאחר סיום תקופת ההתקשרות.
  - חובות צד ג' בהעברת מידע לאחר.

[2] הנחיית רשם מאגרי המידע מס' 2/2011 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי". ההנחיה זמינה כאן

4. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

במהלך שנת 2022, נערך מעקב תיקון ליקויים במגזר זה, שבמסגרתו נדרשו הגופים המפוקחים לנקוט בגישה מבוססת סיכון, ומתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים ביתר הקריטריונים. בנוסף, בוצעו ע"י הרשות להגנת הפרטיות, באופן מדגמי, פיקוחי מעקב על חלק מהגופים בהם נמצאו ליקויים. ההחלטה על קיום פיקוח המעקב בגופים מסוימים התקבלה לאחר שנלקחה בחשבון כמות הליקויים, מהות הליקויים והמסמכים אותם נדרשו הגופים להציג לרשות, בכדי לוודא את יישום דרישות הרשות לתיקון הליקויים. בעת פיקוח המעקב בחנה הרשות את אופן התקדמות תיקון הליקויים אצל הגופים, ואת העמידה בלוחות הזמנים שהגדירו ליישום התוכנית ותיקון יתרת הליקויים שטרם תוקנו.

במסגרת ביקורת המעקב שנעשתה בקרב 24% מהגופים במגזר התקשורת שקיבלו הנחיות לתיקון ליקויים, נמצא שיפור של 66% בתיקון הליקויים.

5. סיכום

כאמור, קיימים סיכונים לא מעטים לפרטיות בקרב מגזר תקשורת, אשר נובעים מניהול ואחזקת מידע רב, מזוהה ורגיש, וניהול קשר אינטראקטיבי עם נושאי המידע באמצעות הגופים. כל אלה דורשים הקפדה יתרה על קיום הוראות תקנות אבטחת מידע, שקיפות מול הלקוח, ומילוי החובות החלות מכוח פרק הדיווח הישיר ושירותי הדיוור הישיר בחוק. ממצאי הליך פיקוח הרוחב במגזר התקשרות מצביעים על פערים בחלק מהגופים בנוגע לעמידה בהוראות החוק בתחום אבטחת מידע, בקרה ארגונית וממשל תאגידי וניהול מאגרי מידע. ניכר, כי עצם קיום הליך פיקוח הרוחב עורר אצל המפוקחים תהליך בחינה עצמית והנעה לשיפור עצמי באופן הציות לחוק ולתקנות, כאשר בסיום ההליך כאמור, הגופים שבהתנהלותם נתגלו ליקויים, נדרשו להציג לרשות התחייבות נושא משרה ותוכנית מסודרת לתיקונם.

גופי התקשורת למיניהם מהווים חלק משמעותי מפעילות המשק הישראלי. במסגרת המגמות החלות בשוק, פעילות גופי התקשורת מתרחבת וכפועל יוצא מתרחב גם השימוש במידע בגופים אלו.

מגמות אלו מגדילות את החשיפה לסיכוני אבטחת מידע ולפגיעה בפרטיות הצרכנים הן בשל סיכוני סייבר והן בשל שימוש לא נאות במאגרים. לאור האמור, נדרש כי גופים אלו יקפידו על מידה נאותה של בקרה על מאגרי המידע שברשותם.

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלים ומחזיקים במאגרי מידע אישי באמצעות הליך פיקוחי הרוחב, לרבות באמצעות ביקורות חוזרות בגופים מפוקחים במגזר זה אשר הונחו לתקן ליקויים, וזאת לשם הגברת עמידתם בהוראות החוק והתקנות, ועל מנת לחזק את ההגנה על זכות הציבור לפרטיות.

במסגרת תכנית העבודה של הרשות ולשם בחינת ההשפעה שיצרה פעילות פיקוח הרוחב על המגזרים שנבדקו, תשקול הרשות לבחון את השינוי היחסי ברמת הציות להוראות החוק במגזר התקשורת, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.