דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב
בקרב מגזר תחבורה חכמה



אדר ב' תשפ"ג
מרץ 2023

תוכן עניינים

1.תקציר מנהלים..... 3

1.1.מגזר תחבורה חכמה 3

1.2.תהליך העבודה..... 4

1.3.ליקויים, מסקנות והמלצות עיקריות..... 5

2. מגזר תחבורה חכמה - תמונת מצב 8

2.1.כללי..... 8

2.2.רקע על המגזר..... 8

2.3.תהליך עבודה..... 10

2.4.הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו..... 11

3. ממצאים – ליקויים מרכזיים לפי קריטריונים ובמבט השוואתי והמלצות: 12

3.1.בקרה ארגונית..... 13

3.2.ניהול מאגרי מידע ועיבוד מידע אישי במיקור חוץ..... 15

3.3.אבטחת מידע..... 17

4.מסקנות/ תמונת מצב 20

5.מעקב תיקון ליקויים 21

6.סיכום..... 22

1. תקציר מנהלים

מערך פיקוח הרוחב ברשות להגנת הפרטיות, מופקד על עריכת פיקוחי רוחב מגזריים או נושאיים לבחינת יישום הוראות חוק הגנת הפרטיות (להלן: "החוק"), התשמ"א-1981 ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "תקנות אבטחת מידע"), 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 תחבורה חכמה בישראל

במסגרת סקר רוחבי שערכה הרשות להגנת הפרטיות אשר בוחן את סיכוני הפרטיות במשק , מגזר תחבורה חכמה בישראל המבטא יישום אינטגרטיבי של מערכות טכנולוגיות למידע, תקשורת וניהול במערכות ותשתיות תחבורה, וכן כלי תחבורה והמשתמשים בהם אותר כאחד מיעדי פיקוח הרוחב המשמעותיים, וזאת בשל מאפייניו הייחודיים של מגזר זה בהיבטי הפרטיות בהיבטים הבאים:

1. שירותי התחבורה החכמה הציבורית נוגעים למרבית האוכלוסייה, וכפועל יוצא מדובר באיסוף מידע על מספר גבוה במיוחד של נושאי מידע.
2. מאגרי מידע המכילים מידע אישי בהיקפים נרחבים במיוחד, בדגש על נתוני מיקום, וזאת לצד מספר רב של גופים וחברות הפועלים בתחום.
3. מנגנוני תפעול גדולים המאפשרים גישה בהיקף נרחב במיוחד למידע אישי.

השימוש ביישומים ומערכות של תחבורה חכמה מתבססים על איסוף, עיבוד וניתוח של מידע המאפשר לגופי תחבורה לקבל החלטות מבוססות נתוני עתק (Big Data) לשם שיפור וייעול מערכת התחבורה. האופן שבו נאסף ומעובד המידע מביא עמו סיכונים לפרטיות המשתמשים בשירותים אלה, המהווים במקרים מסוימים מעין "קהל שבוי" שאין בידיו האפשרות להימנע משימוש בשירות או בתשתית הכרוכים באיסוף מידע אישי. הסיכונים נובעים מאיסוף נתונים רגישים בהיקף נרחב, ריבוי נותני שירותים ועוד. כל אלו מחייבים את הגופים הפועלים במגזר זה לעמוד בהוראות חוק הגנת הפרטיות לעניין הגנה על מידע אישי, ובכלל זה לעמוד בדרישות אבטחת המידע, לרבות קיום מנגנון הרשאות גישה יעיל בהתאם לצורך לדעת, קיום מעקב ובקרה בקרב ספקים חיצוניים המקבלים גישה למידע.

1.2. תהליך העבודה

במטרה לפעול באופן המיטבי ביותר למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, וכחלק מהליך כולל שבמסגרתו גם פרסמה הרשות את "מדריך הגנת הפרטיות בגופי תחבורה בסביבה דיגיטלית"[1], בחודש ספטמבר 2021 פנתה הרשות לחברות תחבורה חכמה בישראל, בדגש על חברות המעניקות שירותי תחבורה לציבור בדרישה למילוי שאלוני ביקורת. יצוין כי בהליך בחירת הגופים נלקחו בחשבון היקפי המידע ורגישות המידע הנאסף. הרשות פנתה בדרישה למילוי שאלוני ביקורת ל- 13 גופים בתחום שירותי תחבורה חכמה.

פעילות פיקוח הרוחב של הרשות כללה בחינה של יישום חוק הגנת הפרטיות ותקנותיו, במטרה לבחון ולסייע לגופים הפועלים בסביבה זו במימוש אחריותן לשמירה על פרטיות המשתמשים, תוך בחינת היקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע לסיכוני פרטיות באותו מגזר או נושא מסוים, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה מגזרית והבאת הגופים המשתייכים למגזר לרמת עמידה התואמת את דרישות החוק והתקנות.

שאלוני הביקורת בחנו ארבעה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית, 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] https://www.gov.il/BlobFolder/news/guide-transportation-privacy/he/--transformation--privacy--2020--.pdf

1.3. ליקויים, מסקנות והמלצות עיקריות

במגזר תחבורה חכמה בישראל מרבית הגופים הציגו רמת עמידה גבוהה בשקלול כל התחומים שנבדקו, ורק כרבע מהגופים נמצאו כבעלי רמת עמידה חלקית. בשקלול הציונים שניתנו לגבי מידת ההיענות להוראות החוק והתקנות, נמצא כי הציון הממוצע של המגזר עומד על 85%.
ביתר פירוט, ממצאי הליך פיקוח הרוחב מלמדים על בקיאות מספקת בדרישות תקנות אבטחת מידע ברוב הגופים שנבדקו. חשוב לציין, כי לצד הממצאים החיוביים, ממצאי פיקוח הרוחב העלו שב- 8% מן הגופים, רמת העמידה בדרישות אבטחת המידע היא נמוכה וכי קרוב ל- 20% מן הגופים נמצאים ברמת עמידה בינונית. בתחום ניהול מאגרי מידע, שליש מן הגופים נמצאים ברמת עמידה בינונית בלבד. בתחום בקרה ארגונית, מרבית הגופים מצויים ברמת עמידה גבוהה בדרישות החוק.
נוכח הממצאים שעלו מהליך פיקוח הרוחב, 9 גופים מתוך 12 קיבלו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם.

ממצאי הליך פיקוח רוחב
בקרב מגזר תחבורה חכמה בישראל

דו"ח פיקוח רוחב 2021-2022

אתגרים ומאפיינים ייחודיים של מגזר תחבורה חכמה בישראל

הפעלת שירותי תחבורה חכמה מצריכה החזקה במאגרי מידע עם מידע אישי רב ורגיש, כגון: פרטי לקוחות, נתוני המיקום שלהם, פרטי תשלום, ועוד. פגיעה אפשרית במאגרי המידע, עלולה להיות משמעותית במיוחד לאור רגישות המידע השמור במאגרי החברות.

מאגרי מידע מכילים מידע אישי בהיקפים נרחבים במיוחד, וזאת לצד מספר רב של גופים וחברות הפועלים בתחום.

הנתונים במאגרי המידע חשופים לגורמים רבים (גוף מנהל, גוף מתפעל, מוקדי שירות לקוחות, סוכנים וכו').

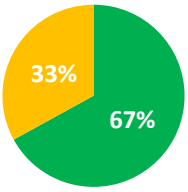
התהליך שבוצע במספרים

13 שאלונים שהופצו

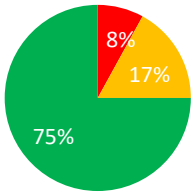
12 גופים שהשתתפו בפועל בהליך הפיקוח

9 הנחיות לתיקון ליקויים

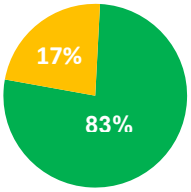
ממצאים – ליקויים מרכזיים:



ניהול מאגרי מידע



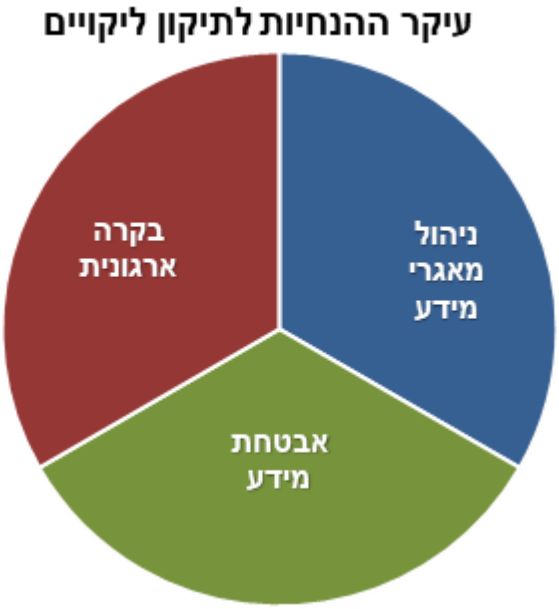
אבטחת מידע



בקרה ארגונית

- **רמת עמידה גבוהה**
- **רמת עמידה בינונית/חלקית**
- **רמת עמידה נמוכה**

- מיקור חוץ - בהתאם לתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), יש לפעול לעיגון במסמך ההתקשרות התייחסות לחובותיו ואחריותו של ספק במיקור חוץ, בהתאם להוראות התקנות.
- מיקור חוץ - ווידוא כי כל גורם חיצוני אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע מידי תקופה, בהתאם לתקנה 15, תוך נקיטה באמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות.
- ניסוח הודעה לכל פניה בדיוור ישיר אשר תכיל את הנושאים הנדרשים בחוק.
- בגופים המחזיקים 5 מאגרים ומעלה, 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 אחר הכפוף ישירות למנהל המאגר.
- עריכת ביקורות בנושא אבטחת מידע מדי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה.



- יש להבטיח כי המערכות 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 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.
- הגבלת או מניעת אפשרות לחיבור התקנים ניידים, ושימוש בשיטות הצפנה מקובלות כאמצעים 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. תחבורה חכמה בישראל - תמונת מצב

כללי

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

רקע על המגזר

תחום "תחבורה חכמה" מבטא יישום אינטגרטיבי של מערכות טכנולוגיות למידע, תקשורת וניהול במערכות ותשתיות תחבורה, וכן כלי תחבורה והמשתמשים בהם.
בשנים האחרונות חל גידול ניכר במספרם של אמצעים טכנולוגיים המאפשרים שינוי באופן ההתניידות של המשתמש.
בכדי להציע למשתמשים היצע של חלופות, תחבורה חכמה יוצרת מסד נתוני עתק (BIG DATA) כגון נתונים על מוצא ויעד (נתוני מיקום), הרגלי נסיעה ונתונים נוספים המועברים לגופי התחבורה השונים ולרשויות, במטרה לשפר את שירותיהם.

היבטי איסוף המידע הפרטי של המשתמשים מתקיימים במגזר זה בשני תחומי ליבה:

<u>פלטפורמת תחבורה (ניידות)</u>

תחום זה מאפשר שילוב בין אמצעי תחבורה שונים – ציבוריים, שיתופיים ואף פרטיים, והנגשתם למשתמשים דרך פלטפורמות שבאמצעותן ניתן לתכנן נסיעה על פי העדפות שמגדיר המשתמש.

<u>איסוף ושיתוף מידע כבסיס לתכנון, פיקוח ולפיתוח שוק התחבורה</u>

פעולות אלו מהוות כלי מפתח לייעול והגברת האפקטיביות של שירותי התחבורה.

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

רגישות המידע

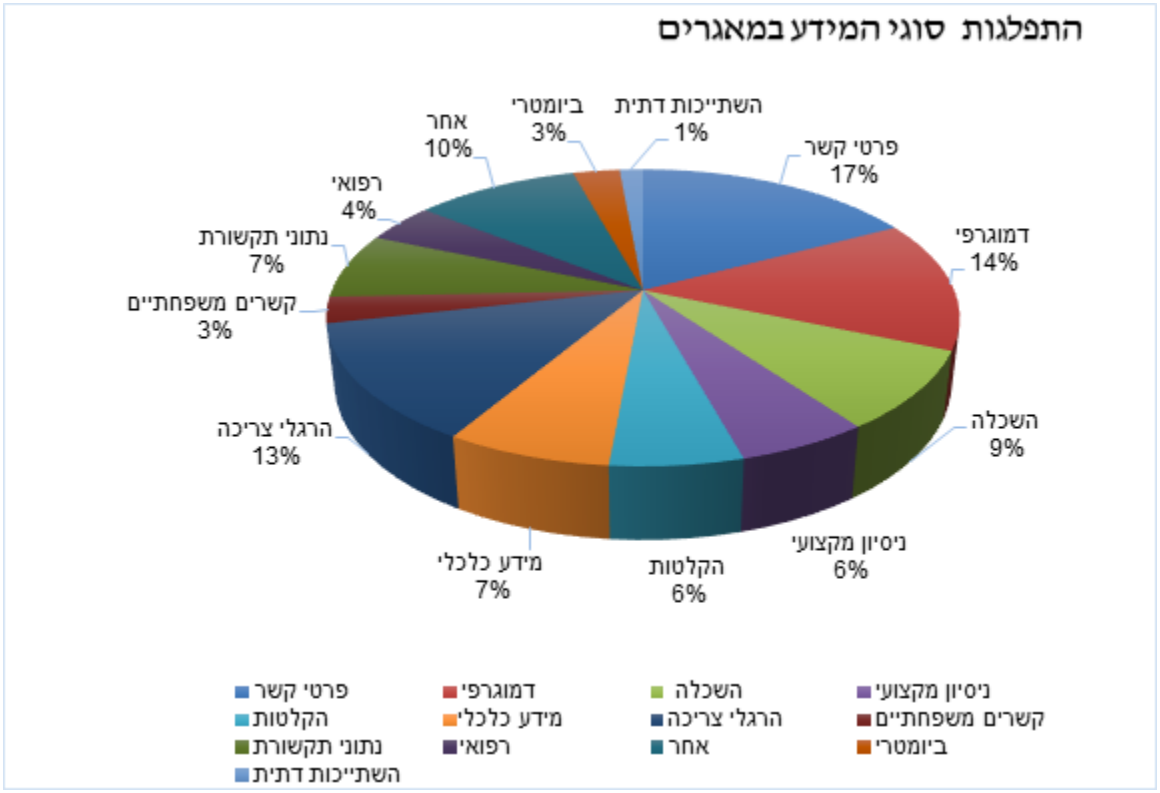
- הפעלת שירותי תחבורה מצריכה החזקה במאגרי מידע עם מידע אישי רב ורגיש
- פגיעה אפשרית במאגרי המידע, עלולה להיות משמעותית במיוחד לאור רגישות המידע השמור במאגרי החברות.

מידע עודף

- מספר החיישנים שנפרסים ע"י גופי התחבורה גדל בקצב מהיר.
- פריסה זו עשויה עלולה להביא לאיסוף נתונים רב מזה שנחוץ להשגת המטרה הראויה.
- היקף המידע מחייב בדיקה ופיקוח כי לא נעשה במידע שימוש מעבר למטרה שלשמה נמסר.

היקף המידע ותפוצתו

- רוב האוכלוסייה נדרשת לאמצעי תחבורה במידה רבה.
- כתוצאה מכך חלקים נרחבים בקרב הציבור מצטרפים למערכות השונות של התחבורה החכמה.
- משמעות הדבר הוא צבירה של היקף עצום של מידע על רוב האוכלוסייה.



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. הרשות פועלת על פי תהליך הערכת מצב שנתי סדור המנתח את הסיכונים לפרטיות בכלל המשק. על מנת לעמוד במכלול האתגרים העומדים לפתחה, פועלת הרשות על-פי תהליך שנתי סדור המנתח את הסיכונים לפרטיות בכלל מגזרי המשק. סקר סיכוני פרטיות ממקד את תחומי הפעילות ומאפשר לרשות לעסוק, בין היתר, במגזרים שונים הכוללים מידע אישי על מספר רב של נושאי מידע ומידע רגיש, וליישם את ממצאי הפעילות בצורה רוחבית.

תהליך העבודה של הליך פיקוח הרוחב כולל בתוכו מספר שלבים מובנים, ומתחיל בשלב של בניית תכנית עבודה שנתית ובחירת מגזרי הפיקוח בהתאם לתחומים בסיכון מוגבר לפרטיות שזיהתה הרשות, ולמדיניות השנתית של הרשות. התוכנית נבנית בהתחשב בגורמים הבוחנים את כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר/נושא, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה מגזרית והבאתו לרמת עמידה נאותה.

הליך הפיקוח החל ב- 13 גופים המשתייכים למגזר תחבורה חכמה, שנבחרו על ידי הרשות. 12 גופים השיבו לשאלוני הפיקוח, וגוף אחד הועבר להמשך טיפול אכיפתי.

בסיום ההליך, ב-9 מתוך 12 הגופים המפוקחים נמצאו ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות את הגופים לתקן את הליקויים שנמצאו, לספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה בדבר יישומה. 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.

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, הבוחנים זאת על בסיס קריטריונים שונים ובהם:[2]



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

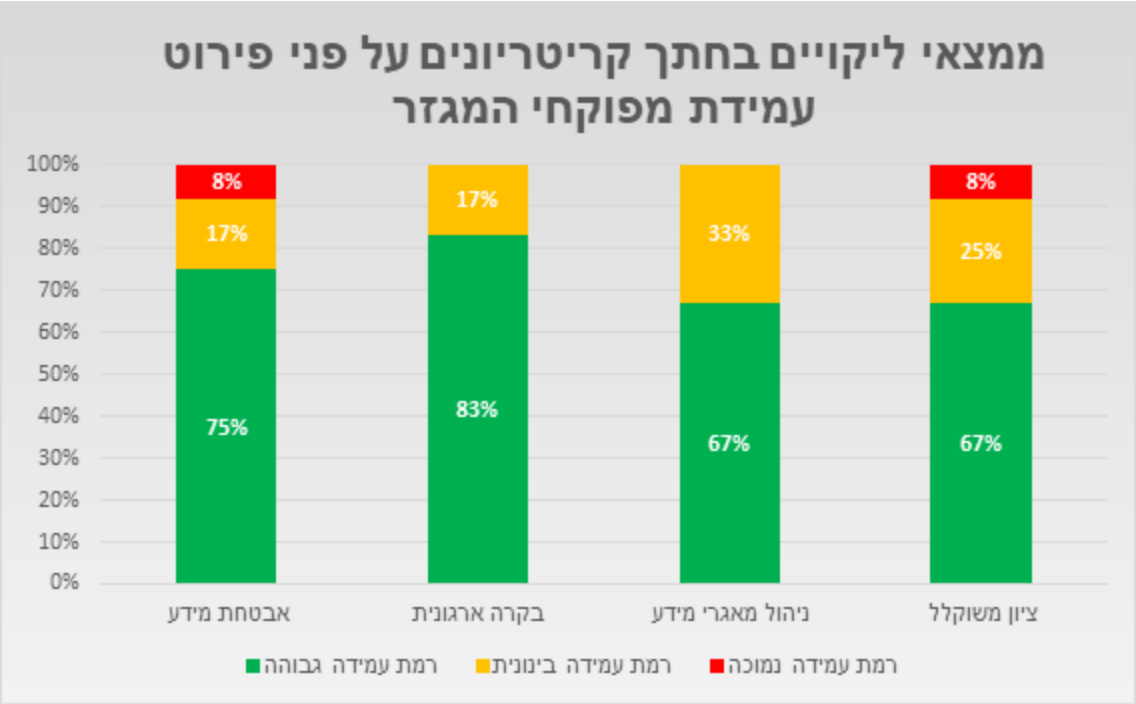
עמידה של בין 80%-100% מהקריטריונים, מוגדרת כרמת עמידה גבוהה;

[2] קריטריון עיבוד מידע אישי במיקור חוץ נבחן בהליך זה כקריטריון משנה תחת ניהול מאגרי מידע

עמידה של בין 50%-80% מוגדרת כרמת עמידה בינונית או חלקית;

עמידה של מתחת ל- 50% מוגדרת כרמת עמידה נמוכה.

3. ממצאים – ליקויים מרכזיים לפי קריטריונים במבט השוואתי והמלצות:



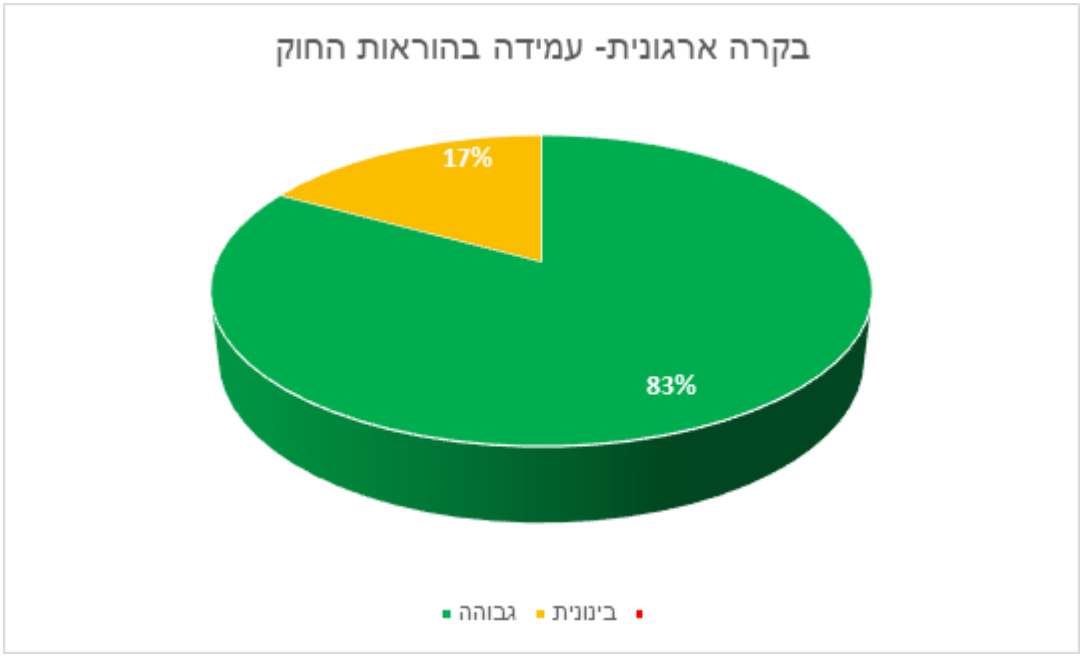
בתחום אבטחת מידע כ-25% מן הגופים אינם עומדים בדרישות החוק באופן מלא. כ-10% מן הגופים מצויים ברמת עמידה נמוכה.

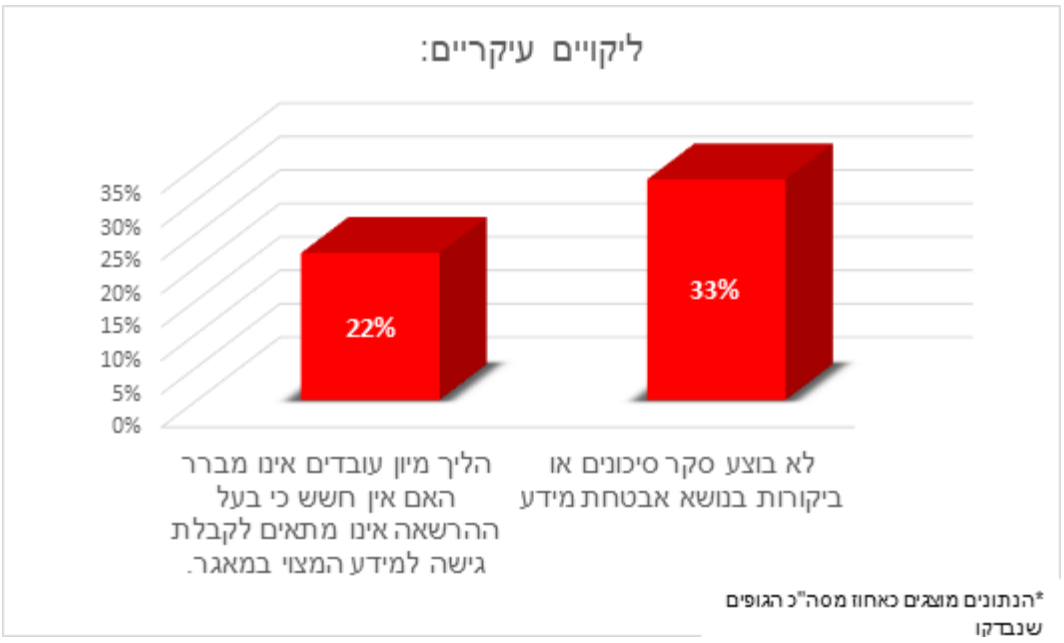
בתחום ניהול מאגרי מידע, כשליש מן הגופים נמצאים ברמת עמידה בינונית בלבד.

בציון המשוקלל, כ-35% מן הגופים הציגו רמת עמידה חלקית בלבד בשקלול כל התחומים שנבדקו, מתוכם כ-10% מצויים ברמת עמידה נמוכה.

בקרה ארגונית

ממצאים:





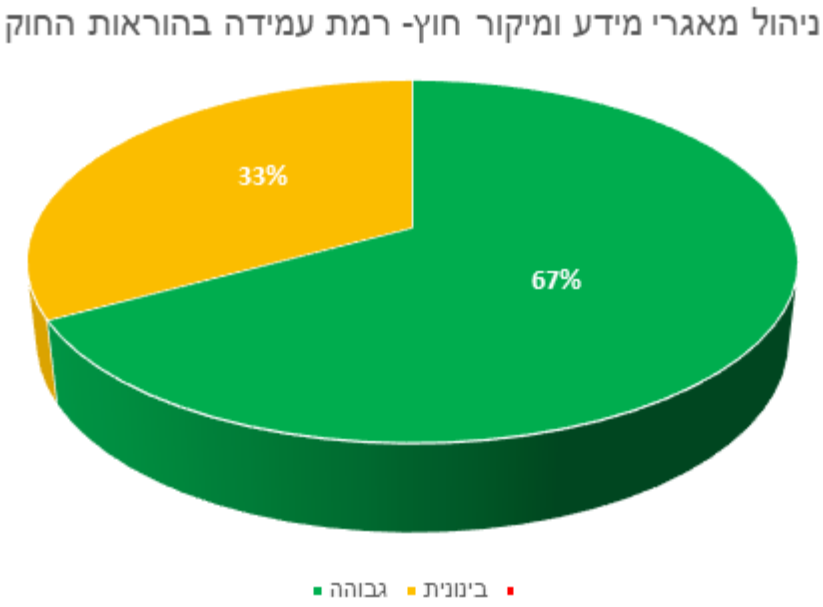
*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

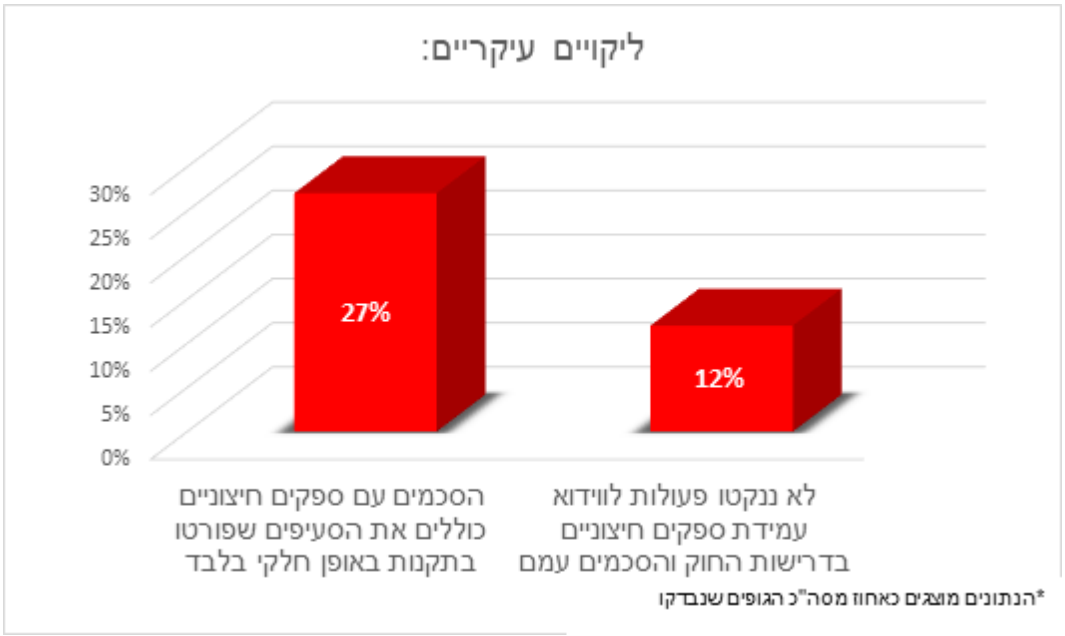
המלצות:

- כחלק ממכלול התיקונים הנדרשים בכדי לעמוד בהוראות החוק והתקנות, נדרשים הגופים, בין היתר, לוודא את רישום כלל מאגרי המידע שבבעלותם בהתאם להוראות החוק, תוך התאמה בין זהות מנהל המאגר במסמכי החברה לבין הרשום אצל רשם מאגרי המידע.
- על הגופים לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות הוצאת כתבי מינוי רשמיים למנהל המאגר ולממונה אבטחת המידע היכן שמינויו נדרש, וכן לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות.
- על הגופים לוודא כי קיימים נהלי אבטחת מידע בארגון הכוללים התייחסות לנושאים כגון :אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, הוראות למורשי גישה, ניהול סיכונים ,התמודדות עם אירועי אבטחת מידע, התקנים ניידים וכו'. בנוסף, על הארגונים לגבש נוהל אבטחת מידע ולבחון את הצורך לעדכנו אחת לשנה, כנדרש בתקנות (תקנה 4).
- בהתאם להוראות התקנות, יש לבצע הדרכות לכלל בעלי הרשאות הגישה בטרם יקבלו גישה למאגר המידע, ובמאגרי מידע בעלי רמת אבטחה בינונית או גבוהה יש לקיים הדרכה זו לפחות אחת לשנתיים. הדרכות אלו יבוצעו באמצעות חומרי הדרכה סדורים. יש לשמור את תיעוד החומרים שהועברו וכן את התיעוד בדבר ביצוע ההדרכות.
- בנוסף, בהתאם לנדרש בתקנות אבטחת מידע (תקנה 7), על הגופים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או בעלי הרשאת גישה אחרים למאגר המידע, על מנת לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגרים .זאת, בהתאם לרגישות המידע הנכלל במאגר, ולהיקף ההרשאה שצפוי להינתן.

ניהול מאגרי מידע ומיקור חוץ

ממצאים:





*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

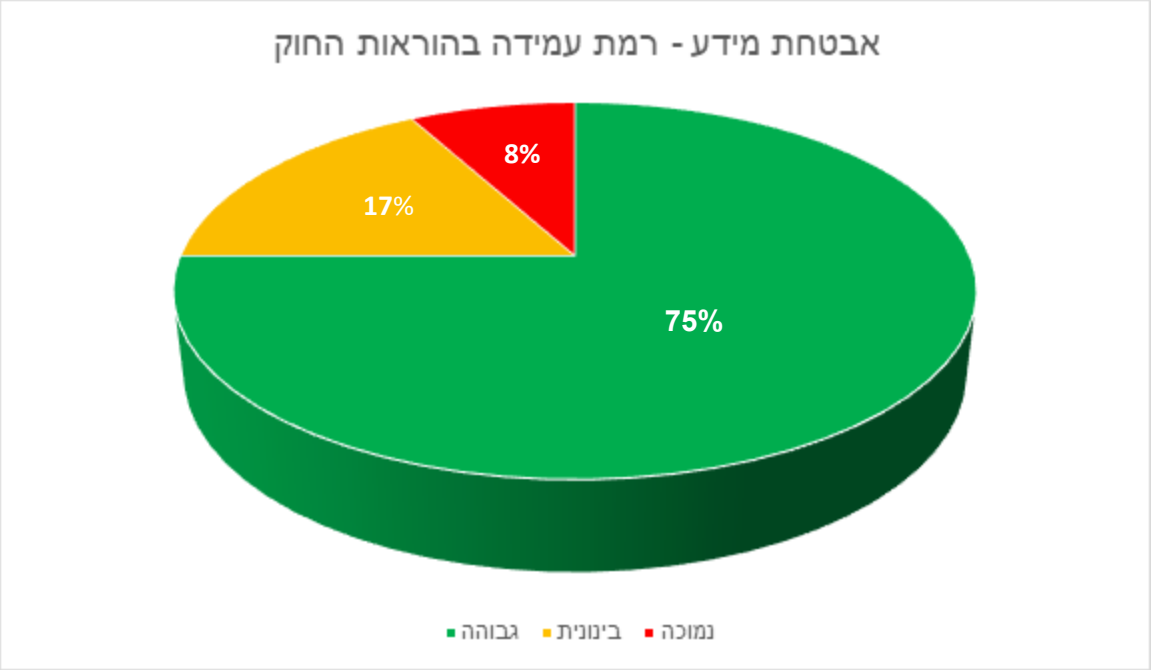
המלצות:

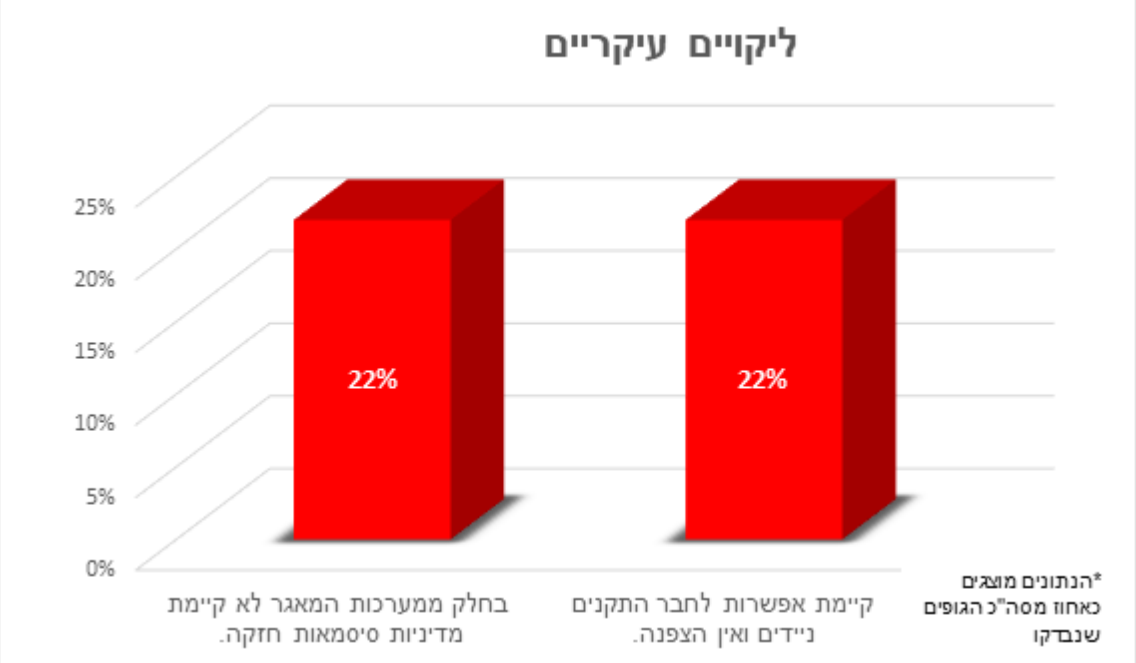
- יש ליידע את נושא המידע בדבר מקור הסמכות לאיסוף המידע על אודותיו. אם לא קיים מקור סמכות בחוק, יש לקבל את הסכמתו עבור איסוף המידע ושמירת פרטיו במאגרי המידע. זאת, תוך מתן הודעה בעת איסוף המידע, הכוללת התייחסות לשאלה האם חלה עליו חובה חוקית למסור את המידע כאמור, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה, בהתאם להוראת סעיף 11 לחוק.
- בהתאם לתקנה 15 לתקנות אבטחת מידע, על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות.
- בנוסף, על הגופים לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, בו ייקבעו במפורש כל הרכיבים המנויים בתקנה 15(א)(2) לתקנות, לרבות חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי התקנות וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה.
- בעניין זה יש לנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות, כנדרש בתקנה 15 ובהנחיית רשם מאגרי המידע מס' 2/2011, ובמדריך פעולה ליישום תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע) בעת התקשרות עם גורם חיצוני.[3]

[3] לקריאה נוספת ר' מדריך פעולה ליישום תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע) בעת התקשרות עם גורם חיצוני, ספטמבר 2023

3.1. אבטחת מידע

ממצאים:





המלצות:

- על הגופים לבצע בחינה עצמית לצורך סיווג רמת אבטחת המידע של מאגרי המידע בהתאם לקבוע בתוספת לתקנות. בעניין זה על הגופים לבדוק את סוג המידע שהם אוספים, את המטרות והשימושים שנעשה במידע הנ"ל. עמדת הרשות היא כי רמת אבטחת המידע הנדרשת של מאגרי המידע לא משתנה, גם אם מאגרי המידע מנוהלים או מעובדים בצורה מפוצלת על גבי מספר מערכות טכנולוגיות שונות בעלות מספר בעלי הרשאה שונה, שכן הבחינה לצורך סיווג רמת האבטחה הינה מהותית, ואינה תלויה בהיבטים הטכניים של אופן ניהול המידע. בהתאם לכך, מספר בעלי ההרשאה לצורך קביעת רמת האבטחה של המאגר הינו סך כל בעלי ההרשאה לכלל המערכות הטכנולוגיות המשמשות את מאגר המידע הרלוונטי.
- על הגופים לוודא כי תיעוד של אירועי אבטחת מידע יישמר, ויגובש נוהל עבודה סדור בנושא, בהתאם לתקנה 11 לתקנות. בנוסף, על נוהל העבודה לכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחת מידע .במאגרי מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמת אבטחה בינונית אחת לשנה) באירועי האבטחה, ולבחון את הצורך בעדכון הנוהל.
- על הגופים לבחון את הצורך בחיבור אמצעים נתיקים. ככל שיוחלט כי לא קיים צורך ממשי או שהצורך מינימאלי – מוצע להגביל השימוש למתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד למערכת, ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. במקרים בהם יוגדר כי קיים צורך בשימוש באמצעים נתיקים, יש להצפין הנתונים באמצעות שיטות הצפנה מקובלות.
- על הגופים לוודא שבכניסה לאתר האינטרנט המאפשר גישה למאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, בהתאם לתקנה 9(ב)(2) לתקנות, וכן לוודא קיום תיעוד עבור אירועי אבטחת מידע, בהתאם לתקנה 11 לתקנות.
- על הארגון לקבוע מדיניות סיסמאות חזקה הכוללת סיסמאות מורכבות המוחלפות בתדירות של עד 6 חודשים. כמו כן יש לעגן את מדיניות הסיסמאות בנוהל עבודה כנדרש בתקנה 9 (ב) לתקנות.
- על הארגון לנהל 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. יש לשמור את נתוני התיעוד של מנגנון הבקרה למשך 24 חודשים לפחות.
- בנוסף, על בעל מאגר המידע לקבוע נוהל בדיקה שגרתי עבור נתוני התיעוד של מנגנון הבקרה.

- במאגרים בעלי רמת אבטחה בינונית ומעלה, יש לפעול להטמעת תהליכי גיבוי ללוג אבטחת מידע, ולקביעת נהלים וביצוע גיבויים ללוג נתוני האבטחה במאגר, באופן שיבטיח כי ניתן יהיה לשחזר בכל עת את הנתונים האמורים למצבם המקורי, כנדרש בתקנה 17 ותקנה 18 לתקנות .

בהתאם לתקנה 2(ג) לתקנות אבטחת מידע, על הגופים לערוך, לפחות אחת לשנה, בחינה האם קיים במאגר מידע עודף, רב מן הנדרש למטרות המאגר, ולתעד בחינה זו. בין היתר, יש לבחון האם מצוי במאגר מידע עודף בנוגע לדיירים שעזבו או שנפטרו, ששוב אינו נדרש עוד למטרות המאגר.

4. מסקנות/ תמונת מצב

להלן התובנות המרכזיות בנוגע ליעד פיקוח הרוחב:

- מגזר תחבורה חכמה אוסף מידע רב אודות משתמשים. מידע זה נוגע לדפוסי התנהגותם היומיומיים, לרבות נתוני , מיקום וכו', בתחום אבטחת מידע נמצא, כי כ- 25% מן הגופים שנבדקו מצויים ברמת עמידה בינונית ונמוכה, ונדרשת הגברת המודעות להפעלת המנגנונים שנבנו במסגרת הבקרה הארגונית באופן מלא ויעיל על מנת שיבטיחו עמידה מלאה בדרישות אבטחת המידע.

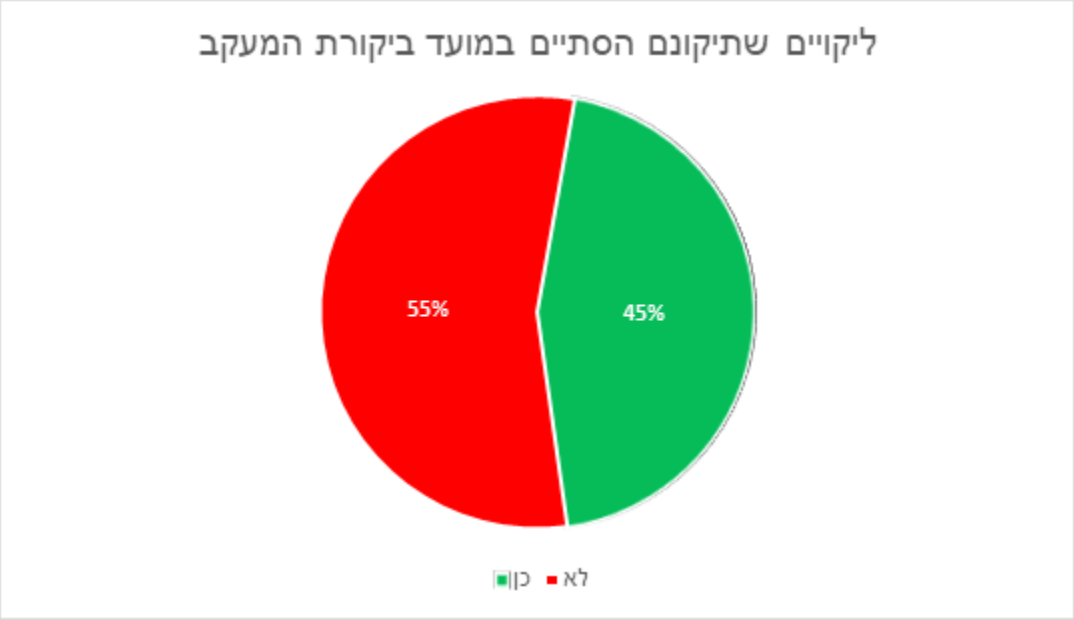
- ממצאי פיקוח הרחב העלו תמונה מדאיגה ביחס לעמידת חלק מן הגופים בהוראות החוק ותקנות אבטחת מידע. בין הליקויים ניתן למנות היעדר מדיניות סיסמאות חזקה, אי קיום מבדקי חדירות וסקרי סיכונים בתדירות הנדרשת, תיעוד גישה חלקי ועוד. בהתחשב באיסוף המידע הנרחב ובשים לב לכך שמדובר במגזר טכנולוגי במהותו, יש לצפות להקפדה יתירה על אבטחת המידע ושמירה על פרטיות המשתמשים.

- בתחום ניהול מאגרי מידע כשליש מן הגופים מצויים, כאמור, ברמת עמידה בינונית בלבד. ביתר פירוט, נמצאה עמידה חלקית בדרישות התקנות והנחיית רשם מאגרי המידע 2/2011 בהתקשרות עם גורם חיצוני לצורך עיבוד או ניהול מידע.

5. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

שנה לאחר עריכת פיקוח הרוחב, ערכה הרשות מעקב תיקון ליקויים במגזר תחבורה חכמה בישראל, 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, בין היתר תוך שקלול מספר הליקויים, סוג הליקוי והמסמכים אותם נדרשו הגופים להציג לרשות, בכדי לוודא את יישום דרישות הרשות לתיקון הליקויים. בעת פיקוח המעקב בוחנת 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 45% מהגופים במגזר תחבורה חכמה בישראל שקיבלו הנחיות לתיקון ליקויים, נמצא כי הגופים שיפרו את העמידה בתקנות אבטחת מידע באופן משמעותי וכי 55% מהליקויים יושמו וטופלו.



לגבי הגופים המפוקחים בכלל ולגבי גופים אלו בפרט, הרשות שומרת לעצמה את שיקול הדעת בכל הנוגע לביצוע הליכי אכיפה משלימים, לרבות בכל הנוגע למסירת תכניות העבודה לתיקון הליקויים וליישומן. פיקוחי המעקב שבוצעו במגזר תחבורה חכמה מעידים באופן חד משמעי על כך שעצם קיום הליכי פיקוח הרוחב מהווה תמריץ לגופים השונים לבצע הליך בחינה באשר לאופן הציות לחוק ולתקנות. אלה מעידים על שיפור משמעותי בעמידת הגופים המפוקחים ביישום הוראות הדין בתחום הגנת הפרטיות ואבטחת המידע כתוצאה מהליך פיקוח הרוחב.

6. סיכום

כאמור, במגזר תחבורה חכמה בישראל מנוהל מידע אישי בהיקפים נרחבים. ממצאי הליך פיקוח הרוחב במגזר תחבורה חכמה בישראל העלו ליקויים בעיקר בנוגע לעמידה בהוראות החוק בתחום אבטחת מידע. יצוין כי חלק משמעותי מן הגופים במגזר תחבורה חכמה בישראל, מחזיק במאגרי מידע שחלה עליהם רמת האבטחה הגבוהה, ובהתאם נדרשת היערכות מתאימה לצורך עמידה בדרישות תקנות אבטחת מידע ביחס למאגרים מסוג זה.

ניכר, כי עצם קיום הליך פיקוח הרוחב עורר אצל הגופים שנבדקו תהליך בחינה והנעה לשיפור אופן הציות לחוק ולתקנות, כאשר בסיום ההליך כאמור, הגופים שבהתנהלותם נתגלו ליקויים נדרשו להציג לרשות התחייבות נושא משרה ותכנית עבודה לתיקון הליקויים .

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלי מאגרי מידע והמחזיקים בהם באמצעות הליך פיקוחי הרוחב, לרבות באמצעות ביקורות חוזרות בגופים שהונחו לתקן ליקויים, וזאת לשם הגברת עמידתם בהוראות החוק והתקנות, ועל מנת לחזק את ההגנה על הזכות החוקתית 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 תחבורה חכמה בישראל, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.