פיקוח רוחב

ממצאי הליך פיקוח הרוחב בקרב מגזר הקמעונאות

סיון תשפ"ג - יוני 2023



תוכן עניינים

1.תקציר מנהלים..... 3

1.1.מגזר הקמעונאות..... 3

1.2.תהליך העבודה..... 4

1.3.ליקויים, מסקנות והמלצות עיקריות..... 4

2. קמעונאות - תמונת מצב 7

2.1.כללי..... 5

2.2.רקע על המגזר..... 7

2.3.תהליך עבודה..... 9

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..... 16

4.מעקב תיקון ליקויים 19

5.סיכום..... 20

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 ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, 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 הקמעונאות

במסגרת סקר רוחבי שערכה הרשות להגנת הפרטיות, אשר בוחן את סיכוני הפרטיות במשק, מגזר הקמעונאות אותר כאחד מיעדי פיקוח הרוחב המשמעותיים. זאת בשל מאפייניו הייחודיים של מגזר זה בתחום הפרטיות, הבאים לידי ביטוי במספר היבטים:

- השימוש הגובר באפליקציות ובאמצעים דיגיטליים, יחד עם מהפכת הקניות באינטרנט, הגדירו מחדש את הרגלי הצריכה של מיליוני צרכנים ישראלים והפכו את המסחר המקוון במוצרים קמעונאיים לתחום מרכזי בעולם המסחר המקוון.
- נכון לשנת הליך פיקוח הרוחב, היקף הפעילות של מגזר הקמעונאות, בדגש על קמעונאות המקוונת עלה בכ-14% לעומת השנה בשנה שלפניה, בעיקר מהשפעת התפרצות נגיף הקורונה.
- במגזר הקמעונאות הלא מקוון, גובר השימוש במערכות ביטחון הכוללות מערך מצלמות במרחבים הציבוריים לצרכי מניעת גניבות. מערכות אלו עשויות לכלול גם אמצעי בקרה וזיהוי ביומטריים, העלולים לפגוע פגיעה חמורה בפרטיות.
- הגופים במגזר זה מנהלים מאגרי מידע בהיקף נרחב המחייבים אותם לעמוד בדרישות אבטחת המידע, בהתאם לרמת אבטחה בינונית. בגופים המנהלים מאגרי מידע הכוללים מעל 100,000 נושאי מידע – ברמת אבטחה גבוהה.

1.2. תהליך העבודה

בהליך פיקוח הרוחב במגזר זה, פנתה הרשות לחברות הפועלות במגזר הקמעונאות, בדגש על קמעונאיות מזון, קמעונאיות דלק, קמעונאיות פארם וקמעונאיות אופטיקה, בדרישה למילוי שאלוני ביקורת. יצוין כי בהליך בחירת הגופים נלקחו בחשבון היקפי המידע ורגישות המידע הנאסף.

בסופו של יום, השיבו 29 גופים קמעונאיים לשאלונים לפי הפילוח הבא: 15 קמעונאיות מזון, 7 קמעונאיות דלק, 3 קמעונאיות פארם ו-4 קמעונאיות אופטיקה.

שאלוני הביקורת בחנו שלושה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית, ניהול מאגרי מידע הכולל בתוכו תת קריטריון הבוחן את השימוש בשירותי מיקור חוץ, ואבטחת מידע. הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם, המעידים על רמת עמידתם בהוראות חוק הגנת הפרטיות ובתקנות מכוח. 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

במרבית הגופים במגזר הקמעונאות נמצאה רמת עמידה גבוהה בהוראות חוק הגנת הפרטיות והתקנות מכוחו בשקלול כל התחומים שנבדקו, כאשר רק כרבע מהגופים נמצאו ברמת עמידה בינונית.

בשקלול הציונים שניתנו לגבי מידת ההיענות להוראות החוק והתקנות, נמצא כי הציון הממוצע של המגזר עומד על 68%. ביתר פירוט, ממצאי הליך פיקוח הרוחב מלמדים על בקיאות מספקת בדרישות תקנות אבטחת מידע. יצוין, כי ממצאי פיקוח הרוחב העלו כי בקריטריון אבטחת המידע כ-33% מן הגופים נמצאו ברמת עמידה נמוכה בדרישות החוק והתקנות, מחציתם נמצאו ברמת עמידה גבוהה, והיתר (17%) נמצאו ברמת עמידה בינונית-חלקית. בתחום ניהול מאגרי מידע, 79% מן הגופים נמצאו ברמת עמידה גבוהה בהוראות החוק והתקנות, וכ- 8% מן הגופים נמצאו ברמת עמידה נמוכה.

נוכח הממצאים שעלו מהליך פיקוח הרוחב, כל הגופים שנבדקו (29 גופים) קיבלו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם.

ממצאי הליך פיקוח רוחב
בקרב מגזר הקמעונאות

דו"ח פיקוח רוחב 2020-2021

אתגרים ומאפיינים ייחודיים של מגזר הקמעונאות

הגופים במגזר הקמעונאות מפעילים מערכות ביטחון הכוללות מערך מצלמות במרחבים ציבוריים.

חלק גדול מהגופים במגזר הקמעונאות משתמשים במערכות נוכחות ביומטריות.

הגופים במגזר הקמעונאות אוגרים מידע רב אודות הרגלי הצריכה של לקוחותיהם.
רוב המגזר הקמעונאי נעזר בדיוור ישיר במסגרת מאמצי השווק.

התהליך שבוצע במספרים

29 שאלונים שהופצו

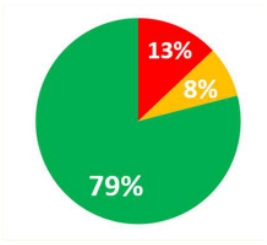
25 גופים שהשתתפו בפועל בהליך הפיקוח (למעט גופים שהוסרו מההליך)

4 מספר הגופים שהועברו להליך אכיפתי נוסף

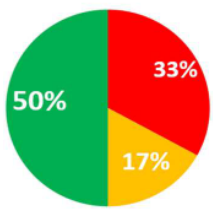
24 הנחיות לתיקון ליקויים

ממצאים – ליקויים מרכזיים:

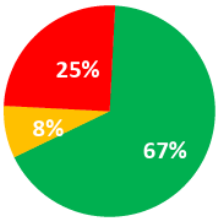
ממצאי ליקויים בחתך קריטריונים על פני פירוט עמידת מפוקחי המגזר



ניהול מאגרי מידע



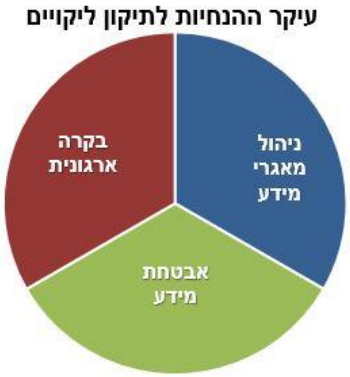
אבטחת מידע



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 התקנה.
- 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.
- 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 אחת הכפוף ישירות למנהל המאגר.
- עריכת ביקורות בנושא אבטחת מידע והגנת הפרטיות מידי 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 בהם מצויות מערכות תשתיות, חומרה, סוגי רכיבי תקשורת ואבטחת מידע, ושל כל הכנסה והוצאה של ציוד 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 הנתונים באמצעות שיטות 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 מידי אחת לשנה וחצי, בחינת הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת המבדקים.

2. מגזר הקמעונאות – תמונת מצב

2.1 כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2020 למאי 2021 במגזר יעד קמעונאות.

2.2 רקע על המגזר

בשנים האחרונות שוק המסחר המקוון גדל באופן משמעותי, וביתר שאת, במהלך תקופת מגפת הקורונה. מגמה זו הביאה לגידול חד בכמות הנתונים שבידי המגזר הקמעונאי ובמספר מאגרי המידע שבבעלותו.
היבטי איסוף מידע אישי של לקוחות המגזר, מתרכזים בשני תחומי ליבה:

פלטפורמת הקמעונאות הדיגיטלית

שימוש גובר באפליקציות ובאמצעים דיגיטליים יחד עם מהפכת הקניות באינטרנט הגדירו מחדש את הרגלי הצריכה של מיליוני צרכנים ישראלים. תחום המסחר המקוון במוצרים קמעונאיים הפך לתחום מרכזי בעולם המסחר המקוון.

איסוף ושיתוף מידע כבסיס לתכנון, פיקוח ולפיתוח שוק הקמעונאות

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

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר הקמעונאות כיעד פיקוח רוחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר ותתי המגזרים שקיימים בו, כדלהלן:

קמעונאות פארם

- בתת מגזר זה נבחרו 3 קמעונאיות.
- תת מגזר זה מאופיין באספקת תכשירים רפואיים בהתאם למרשמים רפואיים ועל כן מאגריו כוללים נתוני צריכה, לרבות מרשמים תרופות בעלי מידע רגיש.
- עיקר הליקויים בתת מגזר זה היו בחלק א' - בקרה ארגונית וממשל תאגידי.

קמעונאות אופטיקה

- בתת מגזר זה נבחרו 4 קמעונאיות.
- תת מגזר זה מאופיין במתן שירותים רפואיים ועל כן מאגריו כוללים מידע רפואי רגיש.
- ליקוי שבלט במיוחד בתת מגזר זה הוא העדר בחינת השאלה אם מועמד לעבודה אינו מתאים לקבלת גישה למידע מהמאגר, בעת הליך מיון עובדים.

קמעונאות מזון

- בתת מגזר זה נבחרו 15 קמעונאיות מזון.
- ליקוי מרכזי שנמצא אצל 71% מפוקחים מתת מגזר זה הוא העדר תכנית ביקורת או היותה בלתי איכותית. ליקוי נוסף הוא העדר מעקב אחר אירועי אבטחה.
- תת מגזר זה וכן תת מגזר קמעונאות הדלק מאופיינים בהקמה וניהול של מועדוני לקוחות המכילים פרטי מידע אישי (ת"ז, כתובות דואר אלקטרוני וכו').
- מבדיקה שערכנו בפרסומים ציבוריים של הגופים המפוקחים, חלק מהמאגרים מכילים מעל 100,000 נושאי מידע, כך שחלה עליהם רמת אבטחה גבוהה.

קמעונאות דלק

- בתת מגזר זה נבחרו 7 קמעונאיות דלק.
- ליקוי שבלט במיוחד בתת מגזר זה הוא העדר שימוש של העובדים באמצעי פיזי הנתון לשליטתו המלאה של בעל ההרשאה בעת כניסה למאגר.

להלן פירוט אופייני של מאגרי המידע:



הליך פיקוח הרוחב במגזר התמקד במאגרי המידע הבאים:

- **לקוחות, מכירות, ומועדוני לקוחות.**
- **מאגרי מידע ביומטרים.**

2.3. תהליך עבודה

במטרה לפעול באופן המיטבי למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, הרשות להגנת הפרטיות נוקטת בגישה מבוססת סיכון, הבוחנת 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 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 או לנושא, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה מגזרית והבאתו לרמת עמידה נאותה.

הליך הפיקוח החל ב- 29 גופים המשתייכים למגזר הקמעונאות, שנבחרו על ידי הרשות. בסופו של יום, השיבו 25 גופים לשאלוני הפיקוח, והארבעה הגופים הנוספים הועברו להליך אכיפתי נוסף.

בסיום ההליך, ב-24 מהגופים 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: [1]

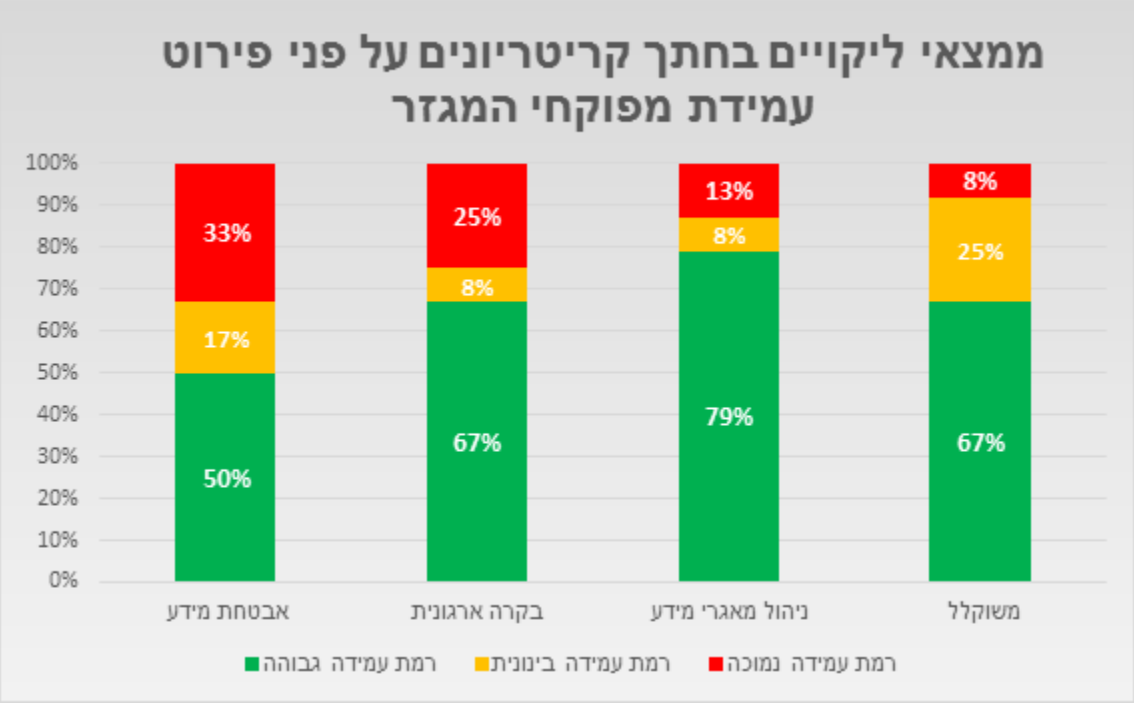


[1] קריטריון עיבוד מידע אישי במיקור חוץ נבחן בהליך זה כקריטריון משנה תחת ניהול מאגרי מידע

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:

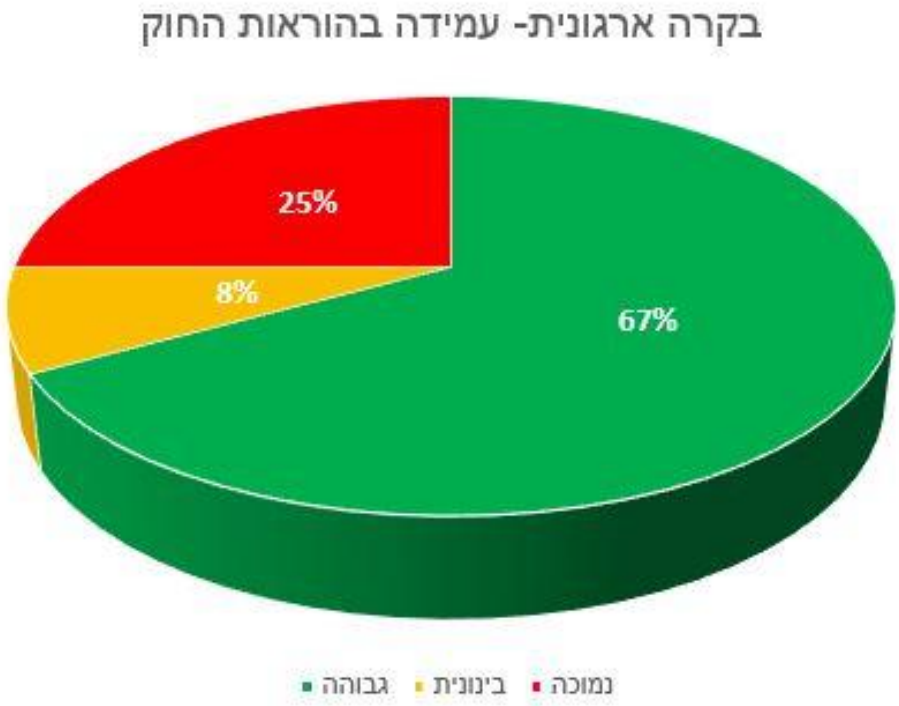
- עמידה של בין 100% - 80% מהקריטריונים, מוגדרת כרמת עמידה גבוהה;
- עמידה של בין 80% - 50% מוגדרת כרמת עמידה בינונית או חלקית;
- עמידה של מתחת ל-50% מוגדרת כרמת עמידה נמוכה.

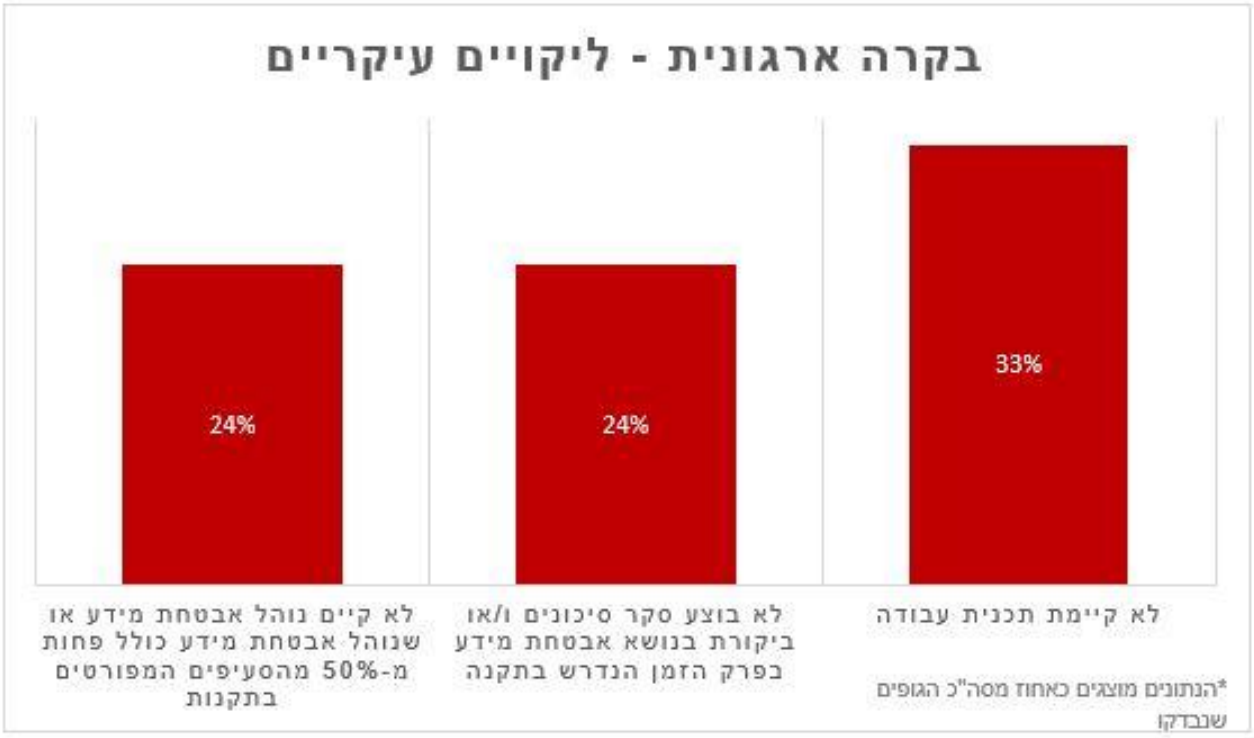
3. ממצאים – ליקויים מרכזיים לפי קריטריונים ובמבט השוואתי והמלצות



3.1. בקרה ארגונית

ממצאים:



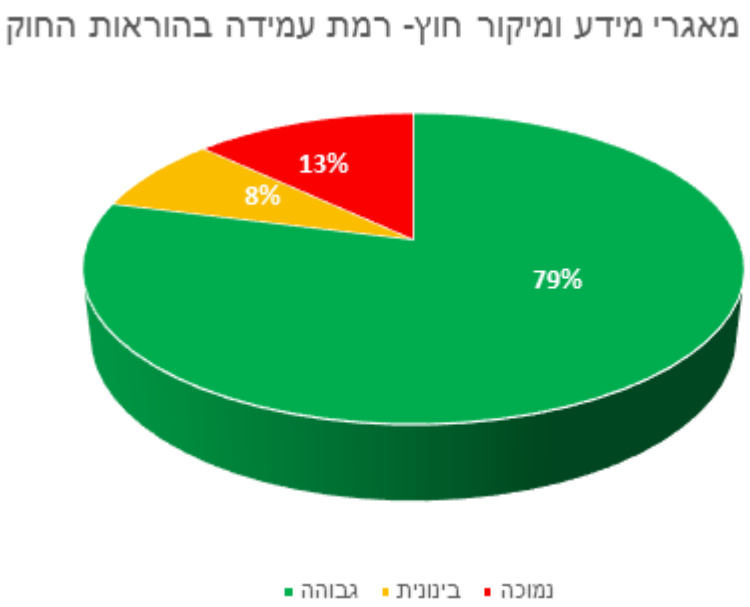


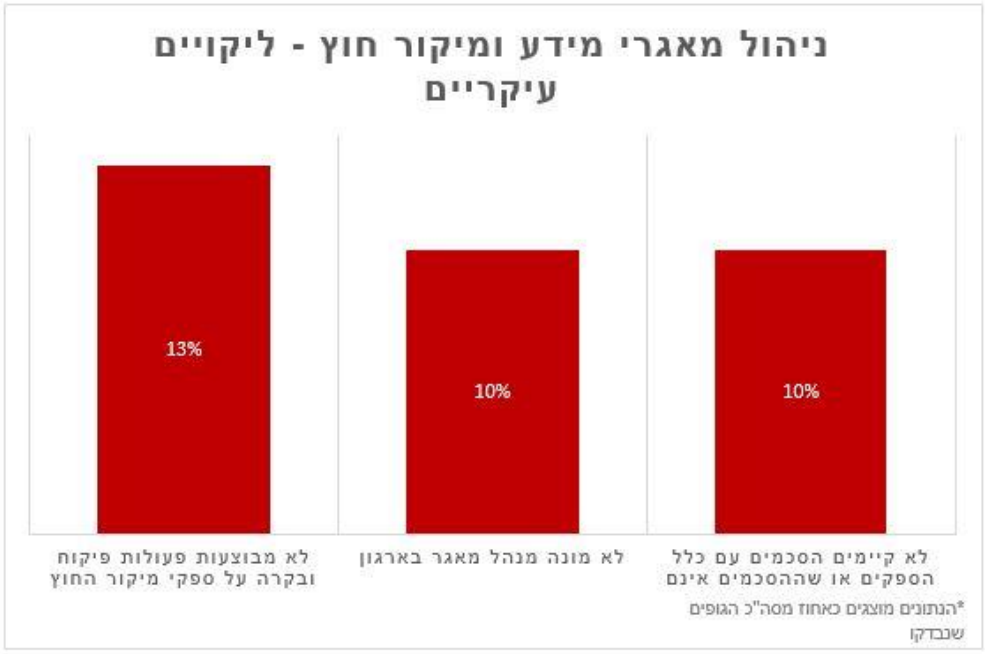
המלצות:

- 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 התיעוד לביצוע 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.

3.2. ניהול מאגרי מידע ומיקור חוץ

ממצאים:



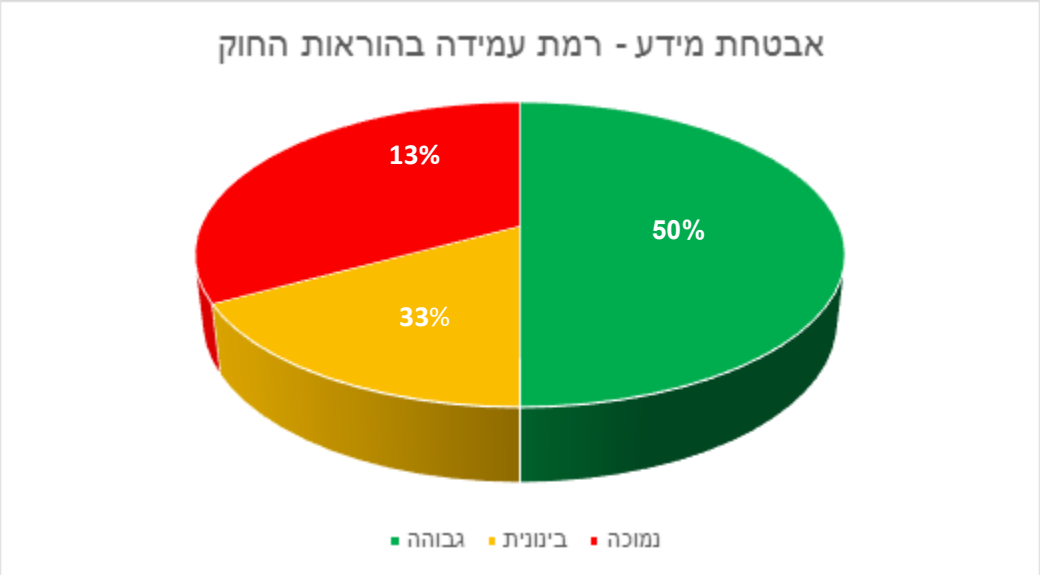


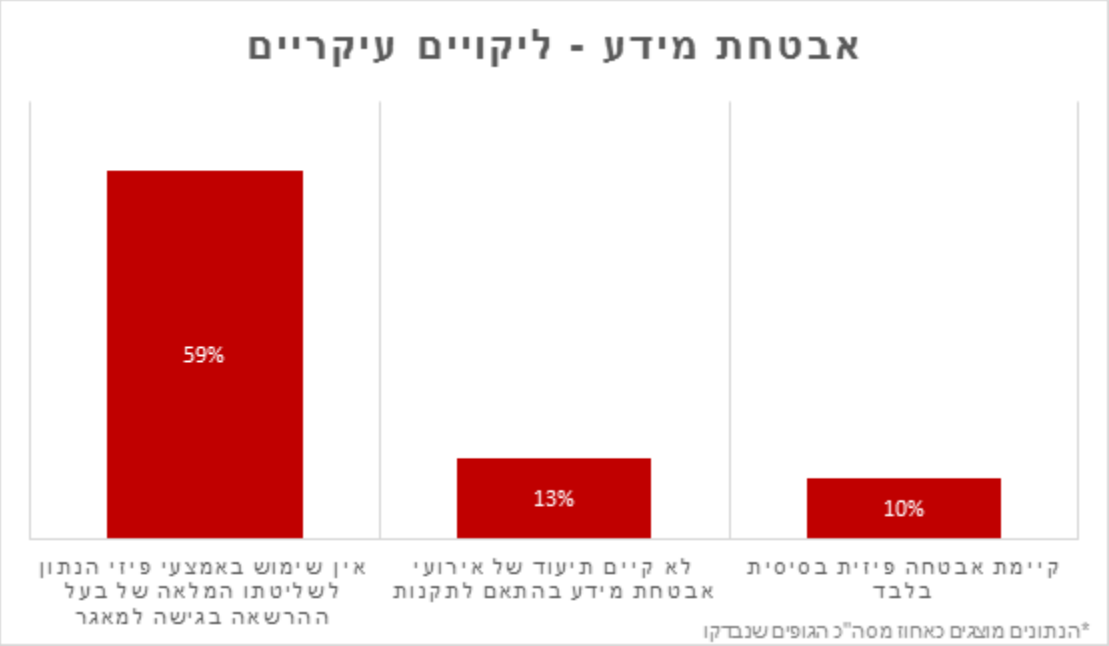
המלצות:

- 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 6 והתקנות, כנדרש בתקנה 15 ובהנחיית רשם מאגרי המידע מס' 2011/2.

3.3. אבטחת מידע

ממצאים:





המלצות:

- על הגופים לבצע בחינה עצמית לצורך סיווג רמת אבטחת המידע של מאגרי המידע בהתאם לקבוע בתוספת בתקנות. בעניין זה על הגופים לבדוק את סוג המידע שהם אוספים, את המטרות והשימושים שנעשה במידע הנ"ל. **בעניין זה, 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, נוהל העבודה יכלול 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 התקנים ניידים. 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 בהתקנים ניידים, יש להצפין הנתונים באמצעות שיטות הצפנה מקובלות.

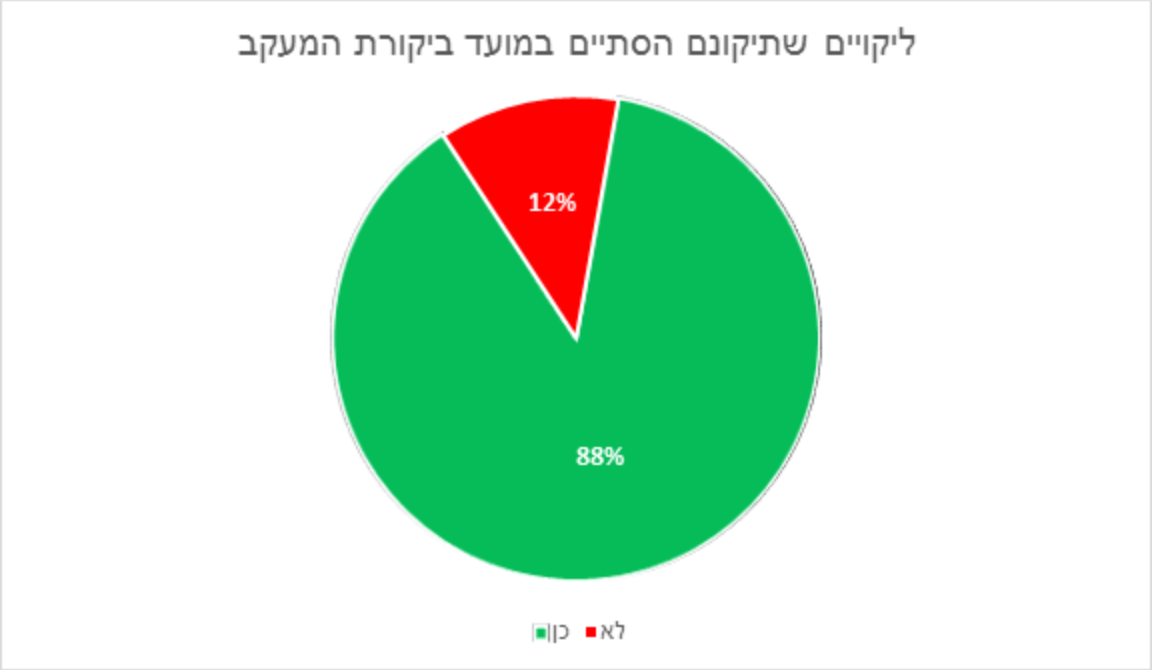
- על הגופים לוודא שבכניסה לאתר האינטרנט המאפשר גישה למאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, בהתאם לתקנה 9(ב)(2) לתקנות, וכן לוודא קיום תיעוד עבור אירועי אבטחת מידע, בהתאם לתקנה 11 לתקנות.
- על הארגון לקבוע מדיניות סיסמאות חזקה הכוללת סיסמאות מורכבות המוחלפות בתדירות של עד 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. נתוני התיעוד של מנגנון הבקרה יישמרו 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. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

במהלך שנת 2022, נערך מעקב תיקון ליקויים במגזר הקמעונאות, 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 תיקון 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 86% מהגופים במגזר הקמעונאות שקיבלו הנחיות לתיקון ליקויים, נמצא כי הגופים שיפרו את העמידה בתקנות הגנת הפרטיות באופן משמעותי וכי 88% 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 כוח אדם והשמה 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 כתוצאה מהליך פיקוח הרוחב.

5. סיכום

במסגרת פיקוח הרוחב שכלל 29 גופים קמעונאיים מתת מגזרי המזון, הפארם, הדלק והאופטיקה, עלה כי למרות הרגישות הגדולה של המידע הנאגר במאגרי הגופים הקמעונאיים, עולה כי המענה בתחום אבטחת המידע והגנת הפרטיות רחוק מלהשביע רצון. ממצאי הבדיקות שנערכו במסגרת הליך פיקוח הרוחב מצביעים על חשיפה לסיכוני אבטחת מידע הנובעים מאי יישום הכללים הנדרשים בתקנות הגנת הפרטיות. הגופים הקמעונאיים הם גופים משמעותיים במשק הישראלי, ובמסגרת המגמות החלות במשק, פעילותם של גופים אלו מתרחבת, כן מתרחב השימוש ברכישות מקוונות בקרב הציבור ובנוסף, הגופים במגזר זה עושים שימוש במערכות מתקדמות לאיסוף מידע צרכני וניתוחו.

מגמות אלו מגדילות את הסיכון לכאורה, לפגיעה 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 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 הקמעונאות, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.