הרשות להגנת הפרטיות

דוח פיקוח רוחב

ממצאי הליך פיקוח הרוחב בקרב סוכנויות ביטוח

תשרי תשפ"ג

אוקטובר 2022

תוכן

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 אבטחת מידע" או "תקנות הגנת הפרטיות" או "התקנות"**). זאת, במטרה לאתר הפרות של החוק, לשם הגברת מודעות המשק להוראות החוק, להגברת האכיפה היזומה של הרשות, לאיתור כשלים ענפיים הדורשים התייחסות והבהרות ולקבלת תמונת מצב כלל-מגזרית לגבי עמידה בהוראות החוק והתקנות.

1.1. מגזר סוכנויות הביטוח

בעקבות סקר רוחבי שערכה הרשות להגנת הפרטיות במגזרי המשק, אשר בחן את סיכוני הפרטיות במגזרים השונים במשק, נקבע מגזר סוכנויות הביטוח כאחד מיעדי פיקוח הרוחב המשמעותיים. זאת, בשל מאפייניו הייחודיים בהיבטי הפרטיות, אשר באים לידי ביטוי במספר היבטים:

- הזדקקות נרחבת של כלל הציבור לשירותי סוכנויות הביטוח;
- איסוף מידע בהיקפים נרחבים ואגירתו לתקופה ממושכת;
- החזקה במידע אישי רגיש כגון מצב נפשי, מצב בריאותי, מידע על נכסים וכו';
- מעבר טכנולוגי מואץ בשנים האחרונות לרכישת שירותי ביטוח במרחב הדיגיטלי.

בתוך כך, המעבר של מגזר סוכנויות הביטוח למרחב הדיגיטלי עלול לעורר סיכונים נוספים על אלו הקיימים, באופן המעלה את החשש לפריצה למאגרי מידע וגניבת נתונים. פרשת שירביט[1] שעלתה לכותרות לפני כשנתיים המחישה את החשיבות שבעמידה בחוק הגנת הפרטיות ובתקנות הנלוות לו, קל וחומר עבור סוכנויות המספקות שירותי ביטוח לחברות וגורמים ביטחוניים.

המאפיינים הייחודיים של מגזר זה, מחייבים את סוכנויות הביטוח לעמוד בדרישות החוק והתקנות ביתר שאת, לרבות קיום חובות אבטחת המידע, קיום בקרה ארגונית והתנהלות תקינה בכל הנוגע לשירותי דיוור ישיר.

[1] מידע נוסף אודות "דגשים לאבטחת מידע בחברות וארגונים והמלצות לציבור בעקבות אירוע אבטחת מידע חמור בחברת שירביט" ניתן למצוא כאן: https://www.gov.il/he/departments/news/shirbit_security_breach

1.2. תהליך העבודה

על מנת לממש את אחריותה באופן המיטבי, למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, הרשות להגנת הפרטיות מקיימת סקרי סיכונים המבוססים על הערכות מצב עיתיות, ונוקטת בגישה מבוססת סיכון הבוחנת כל העת את אפקטיביות מהלכיה ואת פוטנציאל ההשפעה הרוחבית שיש בפעולתה על המשק.

תוצר הערכת המצב כולל תופעות ומגזרים בעלי סיכונים מיוחדים לפרטיות, וממקד את תחומי העיסוק העתידיים של הרשות ואת התשתית לתכנית העבודה. מגזר סוכנויות הביטוח הינו שירות חיוני המאפשר איסוף מידע רגיש בהיקף גדול והוגדר כאחד מהיעדים בהם תמקד הרשות פעילותה.

כחלק מפעילות הליך פיקוח הרוחב פנתה הרשות ל- 35 סוכנויות ביטוח המנהלות מאגרי מידע, בדרישה למילוי שאלוני ביקורת. יש לציין כי 2 סוכנויות סיימו את או שינו את פעילותן העסקית, ו- 5 גופים הועברו לטיפול אכיפתי ממוקד. בסה"כ, במסגרת הליך פיקוח הרוחב נבדקו 28 גופים. שאלוני הביקורת בחנו ארבעה קריטריונים עיקריים בתחום הגנת הפרטיות: (1) בקרה ארגונית, (2) ניהול מאגרי מידע, (3) אבטחת מידע (4) ושימוש במיקור חוץ. הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם המעידים על רמת עמידתם בהוראות חוק הגנת הפרטיות ובתקנות מכוחו.

בסיום הליך בדיקת השאלונים נמצאו ליקויים הדורשים תיקון אצל 26 סוכנויות מתוך 28 הסוכנויות שנבדקו, ובהתאם דרשה הרשות מאותם גופים לתקן את הליקויים שנמצאו, לספק תכנית מפורטת לתיקונם בליווי התחייבות נושא משרה לביצוע ולהשלמת התיקונים. כחלק מההליך, ביצעה הרשות ביקורת חוזרת לבדיקת יישום הדרישה לתיקון הליקויים בקרב 20% מהגופים שקיבלו הנחיות לתיקון ליקויים. במסגרת ביקורת זו נמצא כי הגופים שיפרו את העמידה בתקנות הגנת הפרטיות באופן משמעותי וכי 97% מהליקויים יושמו וטופלו. בכוונת הרשות להגנת הפרטיות להמשיך ולפעול לאכיפת מדיניותה, ונשקלת האפשרות לשוב ולבחון עמידתן של סוכנויות הביטוח בהוראת החוק ותקנותיו, תוך שביחס לגופים שיימצא כי לא מילאו אחר ההנחיה לתיקון ליקויים, תשקול הרשות להטיל סנקציות בהתאם לסמכויותיה מכוח החוק.

1.3. ליקויים, מסקנות והמלצות עיקריות

בקרה ארגונית - כחלק ממכלול התיקונים הנדרשים כדי לעמוד בהוראות החוק והתקנות נדרשים הגופים, בין היתר, לבצע סקרי סיכונים וביקורות בנושא אבטחת מידע בהיקף הנדרש במאגרים ברמת אבטחה בינונית וגבוהה.

ניהול מאגרי מידע - מממצאי פיקוח הרוחב עלה כי ישנה אי-בהירות בקרב סוכנויות הביטוח בקשר לשימושים שמותר להן לעשות במידע שהן אוספות על הלקוחות, כאשר הן משמשות כמחזיקות עבור חברות הביטוח.

בעניין זה עמדת הרשות היא כי בעסקת ביטוח טיפוסית, חברת הביטוח היא **בעלת** מאגר המידע, וסוכנות הביטוח משמשת כזרועה הארוכה של חברת הביטוח כמחזיקה גרידא, ואסור לה להשתמש במידע על הלקוחות למטרותיה של הסוכנות עצמה, ככל שהן חורגות מהמטרות שביחס אליהן ניתנה הסכמת הלקוח לחברות הביטוח. כלומר, **ההסכמה** הניתנת על-ידי המבוטח לחברת הביטוח למטרה המוצהרת (או למטרות המוצהרות), **אינה מהווה הסכמה לשימושים** נוספים, גם אם מטרתם דומה, **על ידי סוכנות הביטוח**.

מובן, כי אין באמור כדי לשלול את אפשרותה של סוכנות הביטוח להקים מאגרי מידע בבעלותה, אך יובהר כי, כאשר מבקשת סוכנות הביטוח לעשות במידע שימושים החורגים ממטרות חברת הביטוח עבורה אספה את המידע, באופן שיהפוך את הסוכנות לבעלת מאגר מידע נפרד, עליה לקבל את הסכמתו הנפרדת של הלקוח להצטרף למאגר הלקוחות של סוכנות הביטוח. זאת, תוך מתן הודעה בעת איסוף המידע לפי סעיף 11 לחוק, הכוללת התייחסות לשאלה האם חלה על הלקוח חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה.

לצד הדרישות הקבועות בסעיף 11 לחוק המפרטות את חובות מבקש המידע, על סוכנות הביטוח להקפיד בכל פנייה בכתב, בדפוס, בטלפון, בפקס, בדוא"ל או בכל אמצעי אחר, 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'.

אבטחת מידע –על אף רמת עמידה יחסית גבוהה, נמצאו ליקויים בקריטריון זה. כדי לשפר את רמות העמידה בו, בין היתר, על הגופים לוודא כי תיעוד של כל אירועי אבטחת מידע יישמר וכי יגובש נוהל עבודה סדור בנושא בהתאם לתקנה 11 לתקנות אבטחת מידע, לרבות קיומו של דיון עתי באירועי אבטחה בהתאם לסעיף 11 (ג) לתקנות. בנוסף, על הגופים לבחון את הצורך בחיבור התקנים ניידים ולפעול בהתאם לתקנה 12 לתקנות.

עיבוד מידע אישי במיקור חוץ - 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 בעל המאגר לוודא עריכת הסכם מול כל גורם חיצוני המחזיק במאגר, בו ייקבעו במפורש כל הוראות תקנה 15(א)(2) לתקנות אבטחת מידע, לרבות חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל המאגר אודות אופן ביצוע חובותיו לפי התקנות וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה. יובהר, כי גם כאשר משמשת

הסוכנות כמחזיקת מאגר עבור חברת ביטוח, יש לוודא עריכת הסכם מול כל גורם חיצוני נוסף שמחזיק במאגר, וזאת בהתאם להוראות תקנה 15(א)(2)(ז) לתקנות.

עוד דורשות התקנות מן הגופים לנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות. הוראות דומות לעניין החובות המוטלות על בעל מאגר המסתייע במיקור חוץ של עיבוד מידע, מפורטות בהנחיית רשם מאגרי המידע מס' 2011/2 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי".

במגזר סוכנויות ביטוח נמצאה רמת עמידה בינונית בהוראות חוק הגנת הפרטיות בנוגע לעיבוד מידע אישי במיקור חוץ. כמו כן, עולה כי סוכנויות רבות כלל אינן מודעות לכך שהשימוש שהן עושות בתוכנות ניהול אינטרנטיות, מהוות למעשה העברת מידע למיקור חוץ.

לאור הממצאים שעלו מהליך פיקוח הרוחב, קיבלו 26 גופים מתוך 28 הגופים שנבדקו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם. **לנוכח הכשלים שהתגלו בהליך פיקוח הרוחב, המפורטים בממצאי דו"ח זה, נשלחו הנחיות לכלל הגופים הפועלים במגזר, באשר לצעדים שעליהם לנקוט כדי לעמוד בדרישות החוק והתקנות.**

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

ממצאי הליך פיקוח רוחב בקרב מגזר סוכנויות הביטוח

אתגרים ומאפיינים ייחודיים של מגזר סוכנויות הביטוח

הזדקקות כמעט מלאה של האוכלוסייה לשירותי הסוכנויות בהיותו של השירות שירות חיוני לציבור

סוכנויות ביטוח עשויות לאסוף מידע פרטי רב ורגיש על לקוחות חברות הביטוח ולקוחותיהן, ובכלל זה מידע אישיותי ורפואי, מידע על מצבו הכלכלי של אדם, רכושו ועוד

מעבר טכנולוגי מואץ בשנים האחרונות לרכישת שירותי ביטוח במרחב המקוון

התהליך שבוצע במספרים

35 שאלונים שהופצו

2 גופים שסיימו פעילות/שינו פעילות

5 גופים שהועברו לטיפול אכיפתי

8 דרישות להשלמת מידע חסר בכתב

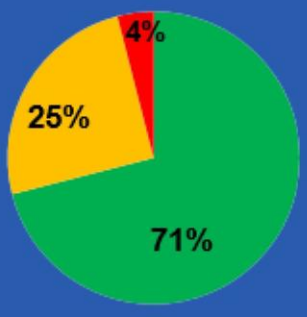
1 בגוף אחד בוצע פיקוח במקום

26 הנחיות לתיקון ליקויים

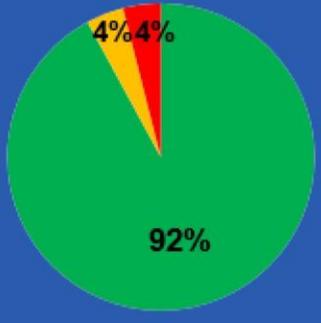
* מתוכם, על 6 גופים בוצע פיקוח מעקב

ממצאים - ליקויים מרכזיים

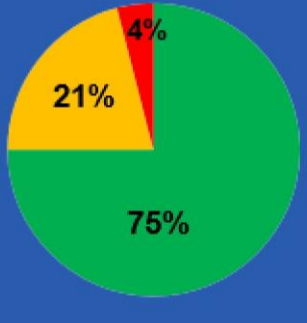
רמת עמידה גבוהה
רמת עמידה בינונית
רמת עמידה נמוכה



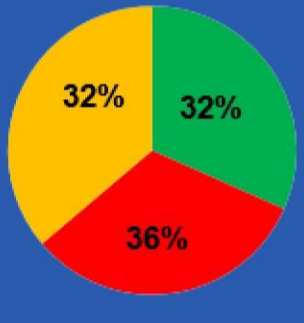
בקרה ארגונית



ניהול מאגרי המידע



אבטחת מידע



עיבוד מידע אישי במיקור חוץ

- יש לפעול ע"פ הקווים המנחים וכלי העזר המופעים בהנחיית רשם מאגרי מידע מס' 2/2011 בעניין שימוש בשירותי מיקור חוץ (outsourcing)לעיבוד מידע אישי.
- בעת עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, ייקבעו במפורש כל ההוראות המפורטות בתקנה 15(א)(2) לתקנות אבטחת מידע, 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.

- יש למסור הודעה ללקוח בעת איסוף המידע. על נוסח ההודעה לכלול את כל המוגדר בסעיף 11 לחוק, ובכלל זה התייחסות לשאלה האם חלה חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו של הלקוח; המטרה אשר לשמה מבוקש המידע; למי יימסר המידע ומטרות המסירה.
- על כל פניה בדיוור ישיר להכיל את הפרטים הנדרשים בהתאם להוראות החוק.

- יש לפעול ע"פ הקווים המנחים וכלי העזר המופעים בהנחיית רשם מאגרי מידע מס' 2/2011 בעניין שימוש בשירותי מיקור חוץ (outsourcing)לעיבוד מידע אישי.
- בעת עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, ייקבעו במפורש כל ההוראות המפורטות בתקנה 15(א)(2) לתקנות אבטחת מידע, 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.
- יש לבנות מנגנוני הרשאות גישה במאגרי המידע של סוכנות הביטוח ובמאגרים בהם מחזיקה הסוכנות, וזאת בהתאם לתקנות 8 ו- 9(א) לתקנות אבטחת מידע, אשר יבטיחו הפרדת סמכויות ויאפשרו גישה למאגרים ולמידע על פי עקרון "הצורך לדעת".
- אופן הזיהוי יעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה.
- במאגרים ברמת אבטחה גבוהה, יש לבצע מבדקי חדירה אחת ל – 18 חודשים ולדון בממצאים שהתגלו במסגרתם, בהתאם לתקנה 5(ד) לתקנות אבטחת מידע. יש לוודא כי תיעוד של אירועי אבטחת מידע יישמר ויגובש נוהל עבודה סדור בנושא, וכן לקיים דיונים באירועים, בהתאם לתקנה 11 לתקנות אבטחת מידע.
- במאגרים ברמת אבטחה גבוהה, יש לבצע סקר סיכונים ע"י גורם חיצוני מקצועי ובלתי תלוי אחת ל-18 חודשים. כמו-כן, יש לבצע בחינה של הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבות תוצאות הסקר, ותיקון הליקויים שהתגלו במסגרתו.

2. מגזר סוכנויות הביטוח - תמונת מצב

2.1. כללי

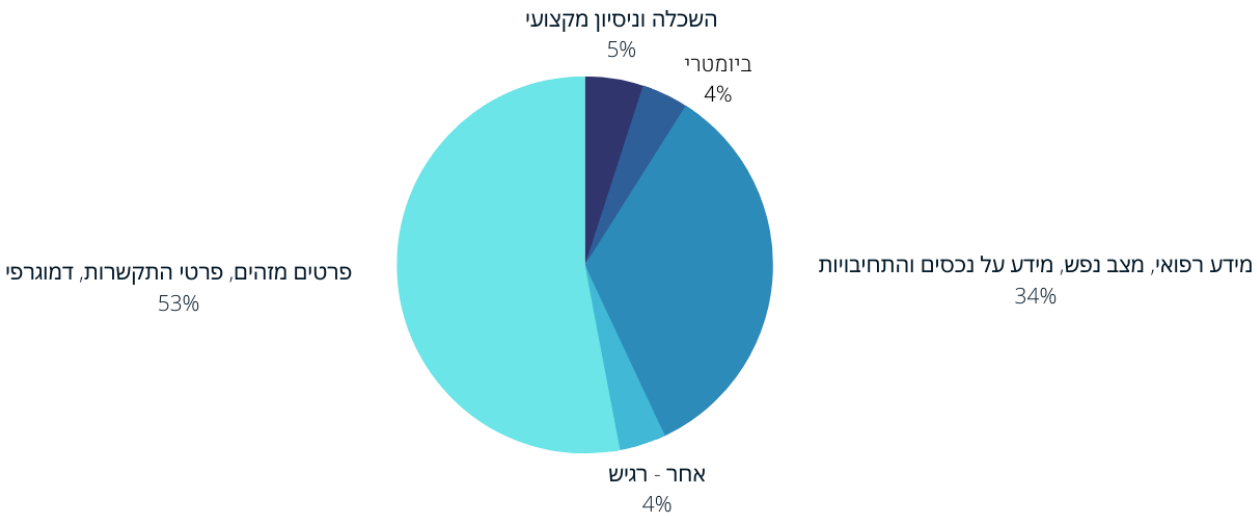
הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2019 למאי 2020 במגזר סוכנויות הביטוח ולביקורות מעקב על הגופים שהיו תחת פיקוח רוחב זה בתקופה שבין החודשים ינואר 2021 למרץ 2021.

2.2. רקע על מגזר סוכנויות הביטוח

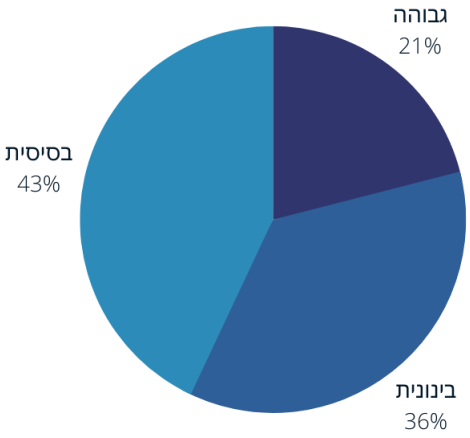
במסגרת סקר רוחבי במגזרי המשק שערכה הרשות להגנת הפרטיות, אשר בחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר סוכנויות הביטוח כיעד פיקוח רוחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר, כדלהלן:

- הזדקקות כמעט מלאה של האוכלוסייה לשירותי הסוכנויות שהינם בגדר "שירות חיוני לציבור".
- רבים מתקשרים עם חברות הביטוח באמצעות סוכנויות ביטוח. כפועל יוצא מכך, סוכנויות רבות מחזיקות במאגרי מידע גדולים ומשמעותיים.
- סוכנויות ביטוח עשויות לאסוף מידע פרטי רב ורגיש על לקוחות חברות הביטוח ולקוחותיהן, ובכלל זה מידע על אישיותו של האדם, מצבו הרפואי, מידע על מצבו הכלכלי, רכושו ועוד.
- סוכנויות רבות מציעות בשנים האחרונות שירותי ביטוח מקוונים במרחב הדיגיטלי, בין אם בעצמן ובין אם באמצעות חברות הביטוח. מידע רב מועבר ביניהן לבין לקוחותיהן, בין היתר באמצעות שימוש בתוכנות ייעודיות ושירותי ענן לצורך ניהול המידע הרב שברשותן, דבר העלול לעורר סיכונים נוספים על אלו הקיימים, באופן המעלה חשש לפריצה למאגרי המידע וגניבת נתונים בצורה נגישה יותר מהעבר.

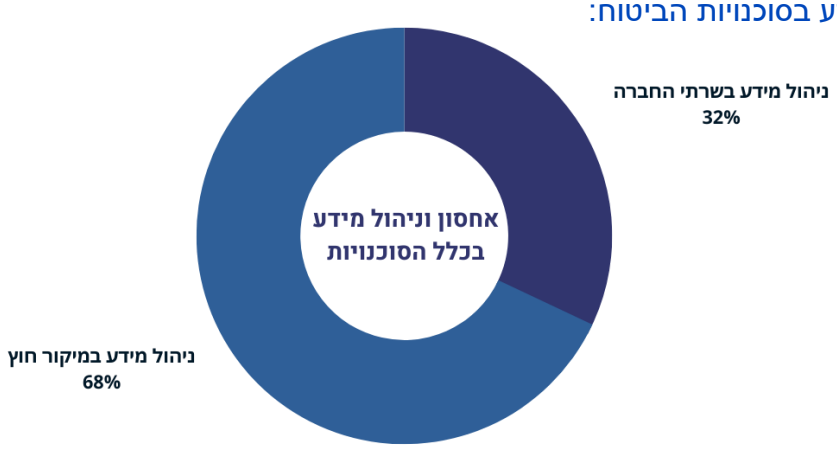
סוגי המידע הנשמרים במאגרי המידע:



התפלגות סיווג רמת אבטחת המידע הנדרשת במאגרים המוחזקים ומצויים בבעלות סוכנויות הביטוח:



אחסון וניהול המידע בסוכנויות הביטוח:



ניהול המאגרים בהתייחס למאפייניו הייחודיים של המגזר מחייב את סוכנויות הביטוח לעמוד ביתר שאת בדרישות החוק והתקנות, תוך הגנה על פרטיות לקוחותיהן, לרבות קיום חובות אבטחת המידע, קיום חובת השקיפות כלפי הלקוחות, התקשרות תקינה מול מי שמחזיק במידע במיקור חוץ וקיום בקרה ארגונית.

2.3. תהליך העבודה

תהליך העבודה של הליך פיקוח הרוחב כולל בתוכו מספר שלבים מובנים, ומתחיל בשלב בניית תכנית עבודה שנתית ובחירת מגזרי הפיקוח בהתאם לסקר הסיכונים שמבצעת הרשות. התכנית נבנית בהתחשב בקריטריונים הבאים: כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר או נושא מסוים, תלונות ספציפיות שהתקבלו ברשות, הצורך בבחינה מגזרית והבאת הגופים המשתייכים למגזר לרמת עמידה התואמת את דרישות החוק והתקנות.

הליך הפיקוח במגזר סוכנויות הביטוח כלל בסופו של דבר, 28 גופים. 8 גופים נדרשו לספק מידע, מסמכים והבהרות נוספות לרשות. בשלב הראשון, נבחרו על ידי הרשות 35 גופים על בסיס בחינת היקפי המידע המוחזקים, כמות הלקוחות ורגישות המידע במסגרת השירותים הניתנים ללקוחות. בשלב השני, נוכו גופים אשר סיימו או שינו פעילותם, וכן גופים אשר השיבו מענה מאוחד בשל פעילות עסקית מאוחדת, ניהול מאגר משותף או ניהול תשתית טכנולוגית משותפת (סה"כ נוכו 7 גופים).

בסוכנות אחת מתוך הגופים בהם בוצע הפיקוח הושלמו ואומתו ידיעות ומסמכים באמצעות פיקוח במשרדי הגוף המפוקח.

בסיום ההליך, נמצאו ב-26 גופים ליקויים הדורשים תיקון. הרשות הנחתה את הגופים לתקן את הליקויים שנמצאו, ולספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה בדבר הביצוע והשלמת התיקונים.

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:

- **בקרה ארגונית** - קריטריון זה בוחן את קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות ואת מינויים של גורמים בעלי אחריות בתחום;
- **ניהול מאגרי מידע** - קריטריון זה בוחן את אופן קבלת ההסכמה לשימוש במידע אישי, רמת התאמת השימוש במידע למטרה שלשמה נאסף, מתן זכות העיון במידע, עמידה בהוראות החוק בעניין דיוור ישיר, ואיסוף של מידע ביומטרי;
- **עיבוד מידע אישי במיקור חוץ** - לרבות בחינת ההתקשרויות של בעלי מאגרי המידע עם צדדים שלישיים המחזיקים במידע ומעבדים אותו, והאופן בו הם מבטיחים הגנה על המידע;
- **אבטחת מידע** - בחינת עמידת הגופים בהוראות תקנות אבטחת מידע בהתייחס לניהול המידע האישי שבבעלותם ובהחזקתם;

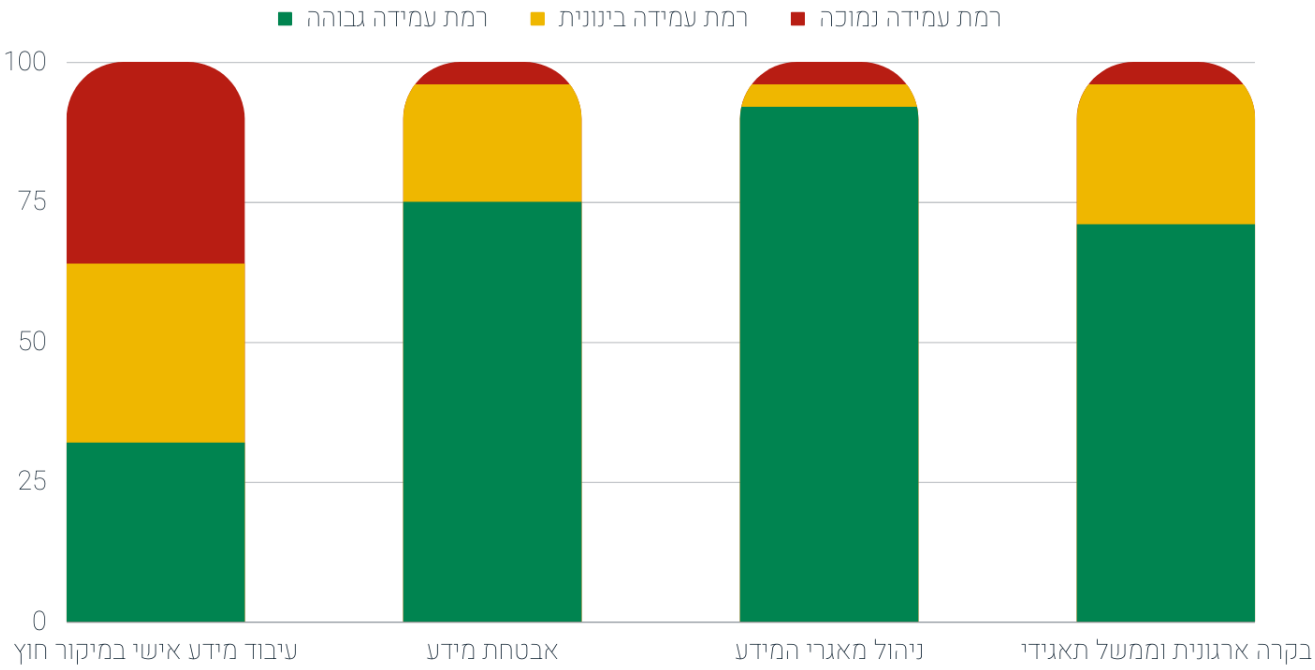
רמות העמידה ביחס לקיום הוראות חוק הגנת הפרטיות והתקנות מכוחו נקבעו בהתאם לשקלול הציונים שקיבלו סוכנויות הביטוח, וזאת בהתבסס על בחינת הרשות את תשובותיהן לשאלוני הביקורת והמידע שנאסף במסגרת ההליך:

- עמידה של בין 80% - 100% מהקריטריונים, מוגדרת כרמת עמידה גבוהה.
- עמידה של בין 50% - 80% מהקריטריונים מוגדרת כרמת עמידה בינונית/חלקית.

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

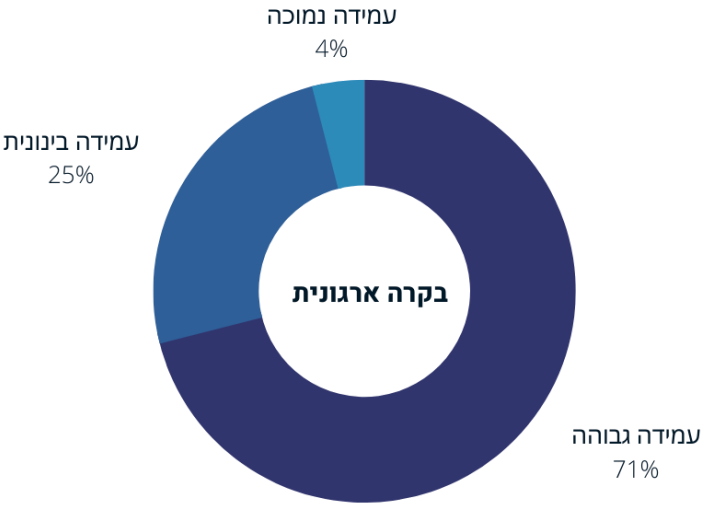
3. ממצאים – ליקויים מרכזיים לפי קריטריונים ומבט השוואתי

3.1. ריכוז הממצאים ברמת יעד פיקוח הרוחב, ולפי התחומים שנבדקו:



את טבלת הממצאים העיקריים שנמצאו במגזר וההנחיות שניתנו לתיקון הליקויים לגופים הספציפיים ניתן למצוא ב**נספח א'** להלן.

3.2. בקרה ארגונית



- במסגרת בחינת הקריטריונים הנ"ל, נמצא כי קיימת עמידה גבוהה בהוראות החוק והתקנות מכוחו. ניתן לראות כי 71% מהגופים במגזר סוכנויות ביטוח עמדו ברמה גבוהה בדרישות הוראות החוק. ניתוח מעמיק של התוצאות מעלה כי קיים מתאם בין גודל הסוכנות

(בהיקף הפעילות) לרמת הציון, כאשר ניתן לראות רמת עמידה בינוית-גבוהה בקרב הסוכנויות הגדולות, ורמת עמידה ברמה חלקית (בינונית/נמוכה) בקרב הסוכנויות הקטנות.

- עוד עלה מהממצאים כי למרות רמת העמידה הגבוהה יחסית, בחלק גדול מהמאגרים ברמת אבטחה בינונית וגבוהה, לא נכתבו נהלי אבטחת מידע המתייחסים אל כלל הסעיפים הנדרשים בתקנות. כן נמצא, כי לא נערכו סקרי סיכונים וביקורות בנושא אבטחת מידע בהיקף הנדרש.
- במסגרת פיקוח הרוחב נמצאו גופים ללא נהלי אבטחת מידע ותכנית עבודה שנתית לבקרה שוטפת על העמידה בדרישות התקנות, או שהנהלים שלהם אינם מספקים בכך שאינם מקיפים את כלל הדרישות בהוראות התקנות.
- בנוסף, נמצאו גופים בעלי מאגרי מידע שחלה עליהם רמת אבטחה גבוהה שלא ביצעו כלל או ביצעו באופן בלתי מספק מבדקי חדירות, שביצועם נדרש לפי התקנות.

3.3. ניהול מאגרי מידע

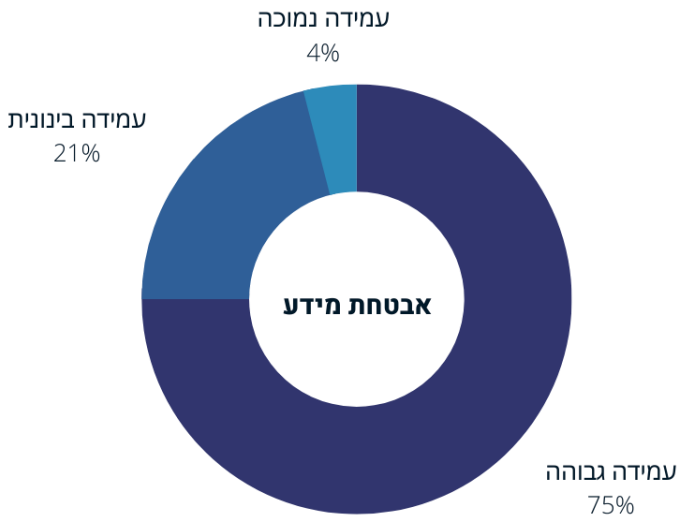
- במסגרת בחינת קריטריון זה, כ-92% מהגופים שנבדקו, נמצאו ברמת עמידה גבוהה בדרישות הוראות החוק בנוגע לניהול מאגרי מידע, נתון המעיד כי מגזר סוכנויות הביטוח מתנהל במידה רבה בהתאם לדרישות החוק בכל הקשור לאיסוף המידע והשימוש בו.
- על אף רמת העמידה הגבוהה, זיהתה הרשות כי ישנה אי-בהירות בקרב סוכנויות הביטוח באשר לשימושים שמותר להן לעשות במידע שהן אוספות על הלקוחות, כאשר הן משמשות כמחזיקות "גרידא" עבור חברות הביטוח
- בעניין זה עמדת הרשות היא כי בעסקת ביטוח טיפוסית כגון ביטוח חיים, בריאות, נכסים וכיוצ"ב, חברת הביטוח היא **בעלת** מאגר המידע, וסוכנות הביטוח משמשת כזרועה הארוכה של חברת הביטוח כמחזיקה גרידא, ואסור לה להשתמש במידע על הלקוחות למטרותיה של הסוכנות עצמה, ככל שהן חורגות מהמטרות שביחס אליהן ניתנה הסכמת הלקוח לחברות הביטוח. כלומר, **ההסכמה** הניתנת על-ידי המבוטח לחברת הביטוח למטרה המוצהרת (או למטרות המוצהרות), **אינה מהווה הסכמה לשימושים** נוספים, גם אם מטרתם דומה, **על ידי סוכנות הביטוח.**
- מובן, כי אין באמור כדי לשלול את אפשרותה של סוכנות הביטוח להקים מאגרי מידע בבעלותה, אך יובהר כי במקרים בהם מבקשת סוכנות הביטוח לעשות במידע שימושים החורגים ממטרות חברת

הביטוח עבורה אספה את המידע, באופן שיהפוך את הסוכנות לבעלת מאגר מידע, עליה לקבל את הסכמתו **הנפרדת** של הלקוח להצטרף למאגר הלקוחות של סוכנות הביטוח. זאת, תוך מתן הודעה בעת איסוף המידע לפי סעיף 11 לחוק, הכוללת התייחסות לשאלה האם חלה על הלקוח חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה. כך, בעת פניה בדיוור ישיר על סוכנות הביטוח לציין את הפרטים הנדרשים בהתאם להוראות החוק.

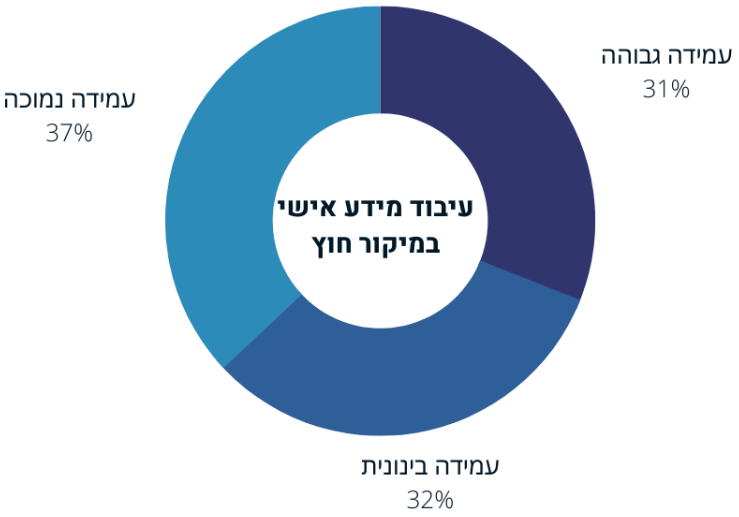
- במסגרת הפיקוח עלה כי חלקן של הסוכנויות סברו כי הן מחזיקות במאגר המידע עבור חברות הביטוח כאשר בפועל, הן נהגו במאגרים מנהג בעלים והשתמשו במאגר המידע למטרות החורגות ממטרת חברת הביטוח, וזאת מבלי לקבל הסכמה נפרדת של הלקוחות, כנדרש בהוראות חוק הגנת הפרטיות.

3.4. אבטחת מידע

- במסגרת בחינת קריטריון זה, נמצא כי כ-75% מהגופים, נמצאים ברמת עמידה גבוהה בדרישות הוראות החוק בנוגע לניהול מאגרי מידע.
- בחלק מגופים בהם נמצאה רמת עמידה בינונית ונמוכה (25%) נמצא כי:
  - ✓ לא בוצע תיעוד של אירועים המעלים חשש לאירוע אבטחה.
  - ✓ לא הוגבל השימוש בהתקנים ניידים או שלא בוצעה הצפנה בעת העברת מידע להתקן נייד.
  - ✓ לא נבנה כלל מנגנון הרשאות או שמנגנון ההרשאות הקיים אינו עומד בדרישות התקנות.



3.5. עיבוד מידע אישי במיקור חוץ



- מבין הגופים שנבדקו בקריטריון זה עלה כי פחות משליש (32%) מסוכנויות הביטוח שנבדקו עומדות בדרישות החוק בנושא עיבוד מידע אישי במיקור חוץ ברמת עמידה גבוהה, בעוד שב-68% מסוכנויות הביטוח נמצאה רמת עמידה בינונית-נמוכה.
- למעשה, בתחום זה קיים המספר הגבוה ביותר של גופים שלא עמדו בדרישות (יותר משליש מן הגופים). נתון זה גבוה משמעותית מהממצאים בתחומי הפיקוח האחרים, בהם אחוז הגופים שלא עמדו כלל בדרישות עמד על כ-4%, לכל היותר.
- רמת הציונים הנמוכה בתחום מיקור חוץ משקפת, בין היתר, תמונת מצב בה מרבית סוכנויות הביטוח משתמשות לצורך אחסון, אחזקה וניהול מאגרי המידע שברשותן בתוכנת מחשוב ענן ייעודית או בתוכנות מקבילות, אך חלקן לא ראות בשימוש זה כהעברת מידע למיקור חוץ.
- בשונה מאחסון מידע בחוות שרתים גרידא, לתוכנות ענן המציעות כאמור תוכנה אינטרנטית לניהול, ארגון ועיבוד המידע, קיימת אפשרות גישה למידע המועבר לידי ספקית התוכנה. על כן, התקשרות עם תוכנות ענן כאמור משמעה התקשרות עם ספק חיצוני, על כל המשתמע מכך בהתאם להוראות החוק ולתקנות אבטחת מידע.
- עוד עולה מהממצאים כי בתחום עיבוד מידע אישי במיקור חוץ, לא בוצעו כלל הפעולות הנדרשות בהתאם לתקנה 15, לא יושמו הנחיות רשם מאגרי המידע מס' 2/2011 (שימוש בשירותי מיקור חוץ לעיבוד מידע אישי), ובכלל זה נמצא כי סוכנויות ביטוח רבות לא נקטו באמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות, או שלא נכללו התייחסויות במסמך ההתקשרות לחובותיו ואחריותו של הספק, וזאת שלא בהתאם להוראות התקנות. יובהר, כי גם כאשר משמשת הסוכנות כמחזיקת מאגר עבור חברת ביטוח, יש לוודא עריכת הסכם מול כל גורם חיצוני נוסף שמחזיק במאגר, וזאת בהתאם להוראות תקנה 15(א)(2)(ז) לתקנות.

4. מסקנות/תמונת מצב והמלצות

מממצאי הליך פיקוח הרוחב עולה כי הגם שמרבית הגופים במגזר סוכנויות הביטוח בעלי היכרות עם דרישות החוק והתקנות, והטמיעו או מצויים בשלבי הטמעה של עיקרי הדרישות, **עדיין קיימים ליקויים משמעותיים באופן יישום הוראות החוק והתקנות. הנחיית הרשות היא כי על הגופים המשתייכים למגזר זה ליישם את הנקודות הבאות:**

4.1. בקרה ארגונית

- נוכח הליקויים שנמצאו בקריטריון זה, וכחלק ממכלול התיקונים הנדרשים כדי לעמוד בהוראות החוק והתקנות, נדרשים הגופים הפועלים במגזר זה, בין היתר, לוודא את רישום כלל מאגרי המידע שבבעלותם, לרבות התאמה בין זהות מנהל המאגר על פי מסמכי הארגון, לבין פרטיו הרשומים אצל רשם מאגרי המידע.[2]
- על הגופים לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות עדכון פרטי מנהל המאגר בפנקס המאגרים ככל שמונה כזה, ובכלל זה מינוי ממונה אבטחת המידע. בנוסף, יש לוודא שכתב המינוי כולל את כל הפרטים הנדרשים בהתאם להוראת סעיף 7 לחוק ולתקנה 4 לתקנות.
- בהתאם להוראות התקנות, יש לבצע הדרכות לכלל בעלי הרשאות הגישה בטרם יקבלו גישה למאגר מידע, ובמאגרי מידע בעלי רמת אבטחה בינונית או גבוהה יש לקיים הדרכה לבעלי הרשאות הגישה לפחות אחת לשנתיים. הדרכות אלו יבוצעו באמצעות חומרי הדרכה סדורים. תיעוד החומרים שהועברו וכן התיעוד לביצוע ההדרכות – יישמר.
- על הגופים לוודא כי קיימים נהלי אבטחת מידע בארגון. על הנהלים לכלול התייחסות לנושאים כגון אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, הוראות למורשי גישה, ניהול סיכונים, התמודדות עם אירועי אבטחת מידע והתקנים ניידים. בנוסף, יש לעדכן את נוהל אבטחת המידע ולבחון את עדכניותו אחת לשנה, כנדרש בתקנות (תקנה 4).
- כמו כן, יש לוודא קיומה של תכנית עבודה לבקרה שוטפת בדרישות התקנות ובכלל זה נושא אבטחת מידע והגנת הפרטיות, לרבות התייחסות לגורם אחראי ולוחות זמנים לביצוע, בהתאם לדרישות התקנות (תקנה 3(3)). ככל שמדובר בגוף שחלה עליו רמת האבטחה הגבוהה וככזה הוא חייב במבדקי חדירות, עליו לוודא כי מבדקי החדירות בוצעו וכי הם עומדים בדרישות התקנות .
- בנוסף, בהתאם לנדרש בתקנות אבטחת מידע (תקנה 7), על הגופים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או בעלי הרשאת גישה אחרים למאגר מידע או מערכת הכוללת

[2] לקריאה נוספת על רישום מאגר מידע ומטרותיו ר' - https://www.gov.il/he/Departments/Guides/registration_fqa.

מספר מאגרים, על מנת לברר שאין חשש כי בעל ההרשאה אינו מתאים קבלת גישה למידע המצוי במאגרים. זאת, בהתאם לרגישות המידע הנכלל במאגר, ולהיקף ההרשאה שצפוי להינתן.

4.2. ניהול מאגרי מידע

- מממצאי פיקוח הרוחב עלה כאמור כי ישנה אי-בהירות בקרב סוכנויות הביטוח בקשר לשימושים שמותר להן לעשות במידע שהן אוספות על הלקוחות, עבור בעלות המאגר שהן חברות הביטוח, להן הסוכנויות נותנות שירותים בגדר "מחזיק" גרידא.
- בעניין זה עמדת הרשות להגנת הפרטיות היא כי בעסקת ביטוח טיפוסית, חברת הביטוח היא **בעלת** מאגר המידע על אודות המבוטחים, וסוכנות הביטוח משמשת כזרועה הארוכה של חברת הביטוח גרידא, ואסור לה להשתמש במידע על הלקוחות למטרותיה של הסוכנות עצמה, ככל שהן חורגות ממטרות שביחס אליהן ניתנה הסכמת הלקוח לחברות הביטוח. כלומר, **ההסכמה** הניתנת על-ידי המבוטח לחברת הביטוח למטרה המוצהרת (או למטרות המוצהרות), **אינה מהווה הסכמה לשימושים** נוספים, גם אם מטרתם דומה, **על ידי סוכנות הביטוח**.
- מובן, כי אין באמור כדי לשלול את אפשרותה של סוכנות הביטוח להקים מאגרי מידע בבעלותה, אך יובהר כי במקרים בהם מבקשת סוכנות הביטוח לעשות במידע שימושים החורגים ממטרות חברת הביטוח עבורה אספה את המידע, באופן שיהפוך את הסוכנות לבעל מאגר מידע נפרד, עליה לקבל את הסכמתו הנפרדת של הלקוח להצטרף למאגר הלקוחות של סוכנות הביטוח. זאת, תוך מתן הודעה בעת איסוף המידע לפי סעיף 11 לחוק, הכוללת התייחסות לשאלה האם חלה על הלקוח חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה.[3]
- לצד הדרישות הקבועות בסעיף 11 לחוק, המפרטות את חובות מבקש המידע, על סוכנות הביטוח, כבעלת מאגר, להקפיד בכל פנייה בכתב, בדפוס, בטלפון, בפקס, בדוא"ל או באמצעי אחר, 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'.[4]

---

[3] להרחבה בנוגע לחובת היידוע לפי סעיף 11 לחוק הגנת הפרטיות, ראו מסמך בנושא "חובת יידוע במסגרת איסוף ושימוש במידע אישי" שפרסמה הרשות להגנת הפרטיות במאי 2022 להערות הציבור. המסמך זמין כאן.

[4] להרחבה בנוגע לדיוור ישיר ושירותי דיוור ישיר, ראו מסמך הנחיית רשם מאגרי מידע מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר", המסמך זמין כאן.

- על הגופים להקפיד לאפשר לנושאי המידע לעיין במידע על אודותיהם המוחזק במאגר מידע, בהתאם לסעיף 13 לחוק. לעניין זה, יודגש כי זכות העיון חלה גם כאשר מדובר במידע אשר נשמר באופן דיגיטלי לרבות שיחות טלפוניות מוקלטות, תכתובות צ'ט ושיחות המצולמות בווידאו.[5] כמו כן, יש להקפיד לאפשר לנושאי המידע לבקש לתקן או לשנות את המידע על אודותיהם המוחזק במאגר המידע, בהתאם לסעיף 14 לחוק.

4.3. אבטחת מידע

- על הגופים לוודא קיומם של נהלי אבטחת מידע אשר כוללים את כל הנושאים המפורטים בתקנה 4 לתקנות, וכן לוודא כי הנהלים נבחנים מעת לעת כנדרש בתקנות.
- 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 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.
- יש להטמיע מנגנון הרשאות המבוסס על הצורך לדעת (לפי רשימת ההרשאות התקפות) ולוודא תקופתית כי הרשאות הגישה הקיימות לעובדים תואמות עיקרון זה בהתאם לתקנות 8 ו-9 לתקנות.
- עוד יש לוודא כי פרק הזמן לשמירת תיעוד שמאפשר ביקורת על הגישה למערכות המאגר הוא 24 חודשים לפחות, כנדרש בתקנה 10 לתקנות.

4.4. עיבוד מידע אישי במיקור חוץ

- לעניין השימוש של סוכנויות הביטוח בתוכנות ענן ייעודית או בתוכנות מקבילות המאחסנות את המידע על שרתים חיצוניים, ומאפשרות עיבוד מידע על בסיס אותם נתונים, עמדת הרשות היא כי תוכנות אלו עונות להגדרת "מיקור חוץ" בתקנות.

---

[5] להרחבה בנוגע לזכות העיון, ראו מסמך בנושא "הנחיית רשם מאגרי המידע 1/2017 - תחולת הוראות חוק הגנת הפרטיות על זכות העיון בהקלטות קול, וידאו ומידע דיגיטלי נוסף", המסמך זמין כאן.

- בהתאם לתקנה 15 לתקנות על הגופים המסתייעים בגורם חיצוני כאמור 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 ההוראות המתחייבות על פי תקנה 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. יובהר, כי גם כאשר משמשת הסוכנות כמחזיקת מאגר עבור חברת ביטוח, יש לוודא עריכת הסכם מול כל גורם חיצוני נוסף שמחזיק במאגר, וזאת בהתאם להוראות תקנה 15(א)(2)(ז) לתקנות.

- 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.[6]

5. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

בסיום הליך פיקוח הרוחב, הגופים שבהתנהלותם נתגלו ליקויים הונחו להגיש לרשות בתוך זמן קצוב מסמך המפרט את אופן תיקון הליקויים, והתחייבות חתומה בידי נושא משרה בכיר בארגון לתיקון יתר הליקויים, על פי תכנית עבודה מסודרת של הארגון הכוללת לוחות זמנים לביצוע.

במהלך שנת 2020, נערך מעקב אחר תיקון ליקויים במגזר סוכנויות הביטוח, שבמסגרתו נדרשו הגופים המפוקחים לנקוט בגישה מבוססת סיכון, ומתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים ביתר הקריטריונים. בתוך כך, בוצעו על-ידי הרשות, באופן מדגמי, פיקוחי מעקב על חלק מהגופים בהם נמצאו ליקויים, במסגרתם נבחנה מידת העמידה בהתחייבות לתיקון הליקויים תוך שקלול מספר הליקויים, סוג הליקוי והמסמכים אותם נדרשו הגופים להציג לרשות. בעת פיקוחי המעקב בחנה הרשות את אופן התקדמות תיקון הליקויים אצל הגופים ואת העמידה בלוחות הזמנים שהגדירו ליישום התכנית ותיקון יתר הליקויים שטרם תוקנו.

במסגרת ביקורת מעקב שנעשתה בקרב 20% מהגופים שקיבלו הנחיות לתיקון ליקויים, נמצא כי מרבית הגופים שיפרו את העמידה בתקנות הגנת הפרטיות באופן משמעותי וכי **97% מהליקויים יושמו וטופלו**. בכוונת הרשות להגנת הפרטיות להמשיך ולפעול לאכיפת מדיניותה, ונשקלת האפשרות לשוב ולבחון

[6] הוראות דומות לעניין החובות המוטלות על בעל מאגר המסתייע במיקור חוץ של עיבוד מידע, מפורטות בהנחיית רשם מאגרי המידע מס' 2/2011 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי". ההנחיה זמינה כאן.

עמידתן של סוכנויות הביטוח בהוראת החוק ותקנותיו, תוך שביחס לגופים שיימצא כי לא מילאו אחר ההנחיה לתיקון ליקויים, תשקול הרשות להטיל סנקציות בהתאם לסמכויותיה מכוח החוק.

פיקוחי המעקב שבוצעו במגזר סוכנויות הביטוח מעידים באופן חד משמעי על כך כי עצם קיום הליכי פיקוח הרוחב מהווה תמריץ לגופים השונים לבצע הליך בחינה עצמית באשר לאופן הציות לחוק ולתקנות. אלה מעידים על שיפור משמעותי בעמידת הגופים המפוקחים ביישום הוראות הדין בתחום הגנת הפרטיות כתוצאה מהליך פיקוח הרוחב.

6. סיכום

בפעילות מגזר סוכנויות הביטוח טמונים סיכונים לא מעטים לפרטיות לקוחותיו, אשר נובעים מניהול מידע רב, מזוהה ורגיש, ומניהול קשר ישיר עם ציבור הלקוחות באמצעות הגופים ובאמצעות גופי מיקור חוץ. כל אלה דורשים הקפדה יתרה על הגנה על פרטיות נושאי המידע ועל אבטחת המידע, וזאת על ידי קיום הוראות החוק והוראות תקנות אבטחת מידע, שקיפות מול הלקוח, ובכלל זה מילוי החובות החלות מכוח פרק הדיווח הישיר בחוק הגנת הפרטיות.

הליך פיקוח הרוחב במגזר סוכנויות הביטוח העלה ממצאים המצביעים על ליקויים בעמידה בהוראות החוק, כאשר עיקר הליקויים נמצאו בתחום עיבוד המידע האישי באמצעות מיקור חוץ.

בנוסף, ממצאי פיקוח הרוחב עלה כי ישנה אי בהירות בקרב סוכנויות הביטוח באשר לסיווגן כמחזיקות או בעלות מאגרי מידע וכפועל יוצא מכך, בקשר לחובותיהן כבעלות מאגרי מידע כלפי לקוחותיהן.

בעניין זה עמדת הרשות להגנת הפרטיות היא כי בעסקת ביטוח טיפוסית, **חברת הביטוח** היא **בעלת מאגר המידע** על אודות המבוטח, **וסוכנות הביטוח** משמשת כזרועה הארוכה **כמחזיקה**, אך אינה רוכשת בעלות במידע על אודות המבוטח. משמעות הדבר היא כי **ההסכמה** הניתנת על-ידי המבוטח **לחברת הביטוח** למטרה המוצהרת, **אינה מהווה הסכמה לשימושים** נוספים **על ידי סוכנות הביטוח**. לפיכך, במקרים בהם מבקשת סוכנות הביטוח לקיים מערכת יחסים משפטית נפרדת מחברת הביטוח עם המבוטח, עליה להסדיר יחסים גלויים ונפרדים עם המבוטח. במקרה זה על סוכנות הביטוח לקבל את הסכמתו הנפרדת של הלקוח להצטרף למאגר הלקוחות של סוכנות הביטוח.

בתוך כך, על סוכנות הביטוח להחתים את הלקוח על הסכם התקשרות, המתיר לה לאסוף מידע אודותיו בהתאם לסעיף 11 לחוק. יובהר, כי ההסכם מול הסוכנות הוא הסכם נפרד מההסכם שנכרת עם החברה המבטחת, והוא מקים זכות עצמאית לסוכנות הביטוח לאסוף מידע ולעשות בו שימוש, לרבות דיווח ישיר בהתאם לסעיף 17 לחוק. עם זאת, כל עוד סוכנות הביטוח לא החתימה את הלקוח על הסכם נפרד, ניתן

יהיה לראות בה כמי שמשמשת כידה הארוכה בלבד של החברה המבטחת, ולכן אין ביכולתה לעשות שימוש במידע הנאסף על לקוחות מכוח הסכם עם החברה המבטחת. מובן, כי אין באמור כדי לשלול את אפשרותה של סוכנות הביטוח להקים מאגרי מידע בבעלותה, אך כאמור לעיל, יובהר כי ככל שברצונה לקיים מערכת יחסים נפרדת מחברת הביטוח עם המבוטח, עליה להסדיר יחסים גלויים ונפרדים עם המבוטח. במקרה זה על סוכנות הביטוח לקבל את הסכמתו מדעת של הלקוח להצטרף למאגר הלקוחות של סוכנות הביטוח.

במהלך הפיקוח, ניכר היה מתוך ההידברות עם הגופים, כי פיקוחי הרוחב הקודמים יצרו תודעה ציבורית ומודעות רחבה אשר הביאה חלק מן הגופים להיערך לקראת פיקוח אפשרי. יצוין כי חלק משמעותי יחסית מן הגופים במגזר סוכני ביטוח, מחזיק במאגרים בהם נדרשת רמת אבטחה גבוהה, והיערכות מתאימה לצורך עמידה בדרישות חוק הגנת הפרטיות, תקנותיו והנחיות הרשות ביחס למאגרים אלה היא בעלת חשיבות רבה. עם זאת, מפיקוחי המעקב אחר תיקון הליקויים עולה, כי קיים שיפור משמעותי בעמידת הגופים המפוקחים ביישום הוראות הדין בתחום הגנת הפרטיות, כתוצאה מהליך פיקוח הרוחב.

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלים ומחזיקים במאגרי מידע אישי 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 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 סוכנויות ביטוח, על ידי בחינת סוכנויות ביטוח נוספות, במועד שייקבע לאחר פרסום הדו"ח המגזרי.

7. נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
בקרה ארגונית וממשל תאגידי			
לא בוצע סקר סיכונים או ביקורות בנושא אבטחת מידע והגנת הפרטיות בשלוש השנים האחרונות.	השלמת התהליך בהקדם וביצוע ביקורת בנושא אבטחת מידע וכן סקר סיכונים. עריכת ביקורות בנושא אבטחת מידע והגנת הפרטיות מידי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה. לחלופין, במאגר ברמת אבטחה גבוהה - עריכת סקר סיכונים מידי 18 חודשים הכולל את דרישות הביקורת.	ביקורות תקופתיות תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 5, תקנה 16.	**סקר סיכונים/ ביקורת אבטחת מידע**
לא קיים נוהל אבטחת מידע או שנוהל אבטחת מידע כולל פחות מ- 50% מהסעיפים המפורטים בתקנות.	בחינת הצורך בעדכון מדיניות אבטחת המידע ועדכנה בהתאם לנוהל.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4.	**נהלי אבטחת מידע**
לא מונה מנהל מאגר.	יש למנות מנהל למאגר המידע. ולעדכן את רשם מאגרי המידע בהתאם.	פרטי מנהל המאגר חוק הגנת פרטיות, תשמ"א-1981 סעיף 7, הגדרות.	**מינוי מנהל מאגר**
לא קיימת תכנית עבודה שנתית.	בניית תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע והגנת הפרטיות המפרטת את הגורם האחראי ואבני דרך ברורות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3).	**תכנית עבודה שנתית**
לא הועבר תיעוד של נוהל אבטחת מידע.	יש לבחון האם נוהל אבטחת המידע עומד בהוראות תקנות הגנת הפרטיות.	נוהל אבטחת מידע תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 4.	**נהלי אבטחת מידע**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
אבטחת מידע			
קיימים מאגרים בהם לא קיים מנגנון ניתוק כאשר אין פעילות.	ברמת אבטחה בינונית ומעלה, נדרשת הגדרת ניתוק אוטומטי במערכות מאגרי המידע לאחר פרק זמן סביר של אי פעילות במערכת.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 9 (ב)(2).	**ניתוק אוטומטי**
קיימת אפשרות לחבר התקנים ניידים ואין הצפנה.	הגבלת או מניעת אפשרות לחיבור התקנים ניידים, ושימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 12	**התקנים ניידים והצפנה**
העברת מידע מכל מאגרי המידע ברשת ציבורית או האינטרנט אינה נעשית באמצעות שימוש בשיטות הצפנה מקובלות	בהתאם לתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 14 (ב), העברת מידע ממאגרי המידע ברשת ציבורית או האינטרנט תיעשה באמצעות שימוש בשיטות הצפנה מקובלות בלבד (TLS 1.2 ומעלה).	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 13 (ב)	**העברת מידע בין מאגרים**
לא קיים תיעוד של אירועי אבטחה.	יש לתעד 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. במאגר מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמה בינונית אחת לשנה) באירועי האבטחה ולבחון את הצורך בעדכון הנוהל.	תיעוד של אירועי אבטחה תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 11.	**תיעוד אירועי אבטחה**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
לא מנוהל מנגנון תיעוד אוטומטי שמאפשר ביקורת על הגישה למאגרים.	יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למאגרי מידע אשר יכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה. נתוני התיעוד של המנגנון יישמרו למשך 24 חודשים לפחות.	בקרה ותיעוד גישה תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 10.	**גישה מרחוק**
בכניסה למאגר על ידי עובד הארגון לא נעשה שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.	במאגרים שחלה עליהם רמת אבטחתה בינונית ומעלה, אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. כגון תעודה המכילה חתימה אלקטרונית מאובטחת, TOKEN וכדומה.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 9 (ב)(1).	**שימוש באמצעי פיזי מרחוק**
לא קיימים אמצעי הגנה מספקים אשר נותנים מענה לחדירה לא מורשית במאגרי המידע המחוברים לרשת האינטרנט או לרשת ציבורית אחרת, בהתאם לדרישה בתקנות.	יש לוודא 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.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 14 (א).	**אבטחת תקשורת**
לא קיימת הפרדה ברורה בין המאגרים הכוללים מידע אישי ליתר המאגרים.	יש לקיים הפרדה בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר בהתאם לתקנות.	ניהול מאובטח ומעודכן של מערכות המאגר תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 13 (ב).	**הפרדת מאגרים עם מידע שונה**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
ניהול מאגרי מידע			
לא ניתנת הודעה בהתאם לדרישות סעיף 11 לחוק.	מתן הודעה ללקוח בעת איסוף המידע. על נוסח ההודעה לכלול את כל המוגדר בסעיף 11 לחוק, ובכלל זה התייחסות לשאלה האם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו; המטרה אשר לשמה מבוקש המידע; ולמי יימסר המידע ומטרות המסירה.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 11.	**מתן הודעה לנושא המידע**
אין התאמה בין המאגרים המנוהלים לבין רישומם בפנקס המאגרים.	יש לפעול להסדרת רישום מאגרי המידע בפנקס המאגרים.	חוק הגנת הפרטיות תשמ"א – 1981, סעיף 8	**רישום המאגר אצל רשם**
לא נמסרו לנושא המידע פרטים בדבר שימוש במאגר לדיוור ישיר או לשירותי דיוור ישיר.	ניסוח הודעה לכל פניה בדיוור ישיר אשר תכיל את הנושאים הבאים: 1. ציון כי הפניה היא בדיוור ישיר, בצירוף ציון מספר הרישום של המאגר המשמש לשירותי דיוור ישיר בפנקס מאגרי מידע; 2. הודעה על זכותו של מקבל הפניה להימחק מן המאגר, בצירוף המען שאליו יש לפנות לצורך כך; 3. זהותו ומענו של בעל מאגר המידע שבו מצוי המידע שעל פיו בוצעה הפניה, והמקורות שמהם קיבל בעל המאגר מידע זה.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 17 ג', 17 ד', 17 ה', 17 ו'	**דיוור ישיר ושירותי דיוור ישיר**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
עיבוד מידע אישי במיקור חוץ			
לא עוגנו הסכמי התקשרות עם ספקי מיקור חוץ המכילים את מלוא הפרטים הנדרשים בהתאם לתקנות.	יש לפעול לעיגון במסמך ההתקשרות התייחסות לחובותיו ואחריותו של הספק, בהתאם להוראות התקנות, לרבות: 1. דיווח אודות אירועי אבטחת מידע. 2. מנגנוני אבטחת המידע הנדרשים. 3. שמירת המידע לאחר סיום תקופת ההתקשרות. 4. חובות גורם חיצוני בהעברת מידע לאחר.	מיקור חוץ תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 15. הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.	**מיקור חוץ**
לא ננקטות פעולות לוודא כי גורם חיצוני נוקט באמצעים הנדרשים בכדי להגן על מאגרי המידע כנדרש.	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.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 15.	**מיקור חוץ**