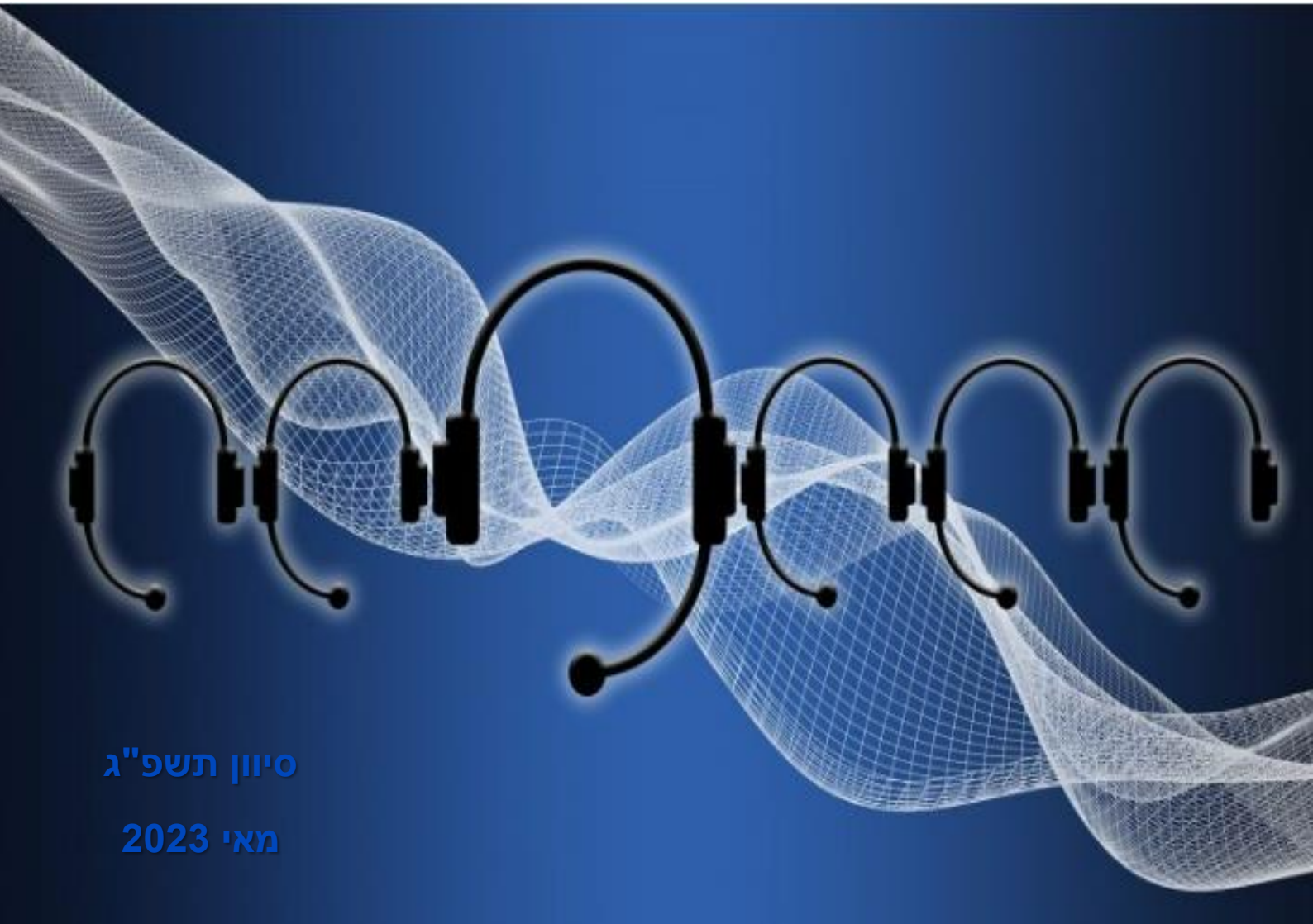
הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

דוח פיקוח רוחב

ממצאי הליך פיקוח הרוחב
בקרב מוקדים טלפוניים (Call Centers)



סיוון תשפ"ג

מאי 2023

תוכן

1. תקציר מנהלים 3

1.1. מגזר המוקדים הטלפוניים (Call Centers).....3

1.2. תהליך העבודה 4

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

2. מגזר יעד מוקדים טלפוניים (Call Centers) - תמונת מצב 8

2.1.כללי.....8

2.2. רקע על המגזר.....8

2.3. תהליך העבודה.....9

2.4. הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו.....10

3. ממצאים – ליקויים מרכזיים לפי קריטריונים ומבט השוואתי 11

3.1. בקרה ארגונית.....11

3.2. ניהול מאגרי מידע.....12

3.3. אבטחת מידע.....13

3.4. עיבוד מידע אישי במיקור חוץ..... 13

4. מסקנות/תמונת מצב והמלצות 13

4.1. בקרה ארגונית.....14

4.2. ניהול מאגרי מידע.....15

4.3. אבטחת מידע.....15

4.4. עיבוד מידע אישי במיקור חוץ 16

5. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב..... 16

6. סיכום 17

7. נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם..... 18

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

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, וקבלת תמונת מצב כלל-מגזרית לגבי עמידה בהוראות החוק והתקנות.

1.1. מגזר המוקדים הטלפוניים (Call Centers)

במסגרת סקר רוחבי במגזרי המשק שערכה הרשות להגנת הפרטיות, אשר בוחן את סיכוני הפרטיות במגזרים השונים, נקבע מגזר המוקדים הטלפוניים (Call Centers) כאחד מיעדי פיקוח הרוחב המשמעותיים. זאת בשל מאפייניו הייחודיים המהווים סיכון בהיבטי הפרטיות, ואשר באים לידי ביטוי במספר היבטים:

- מתן שירותים לאחרים המתאפיינים בקבלת מידע אישי ממבקשי השירותים (בעלי המאגרים), **כך שהמידע מנוהל על-ידי גופים אלו כמחזיק המאגר** (כהגדרתו בחוק).
- הגופים הפועלים במגזר זה נותנים שירותים למגוון רחב של חברות, עם אוכלוסיות מידע שונות, וכפועל יוצא מחזיקות במידע אישי מסוגים שונים, החל ממידע על אודות משק בית ועד למידע רפואי רגיש. נוכח האמור, לגופים הפועלים במגזר זה גישה למאגרי מידע בהיקפים עצומים על מיליוני נושאי מידע.
- החזקה של לפחות חמישה מאגרי מידע עבור אחרים המחייבת עמידה בדרישות פרטניות בדין.

המאפיינים הייחודיים של מגזר זה, מחייבים את הגופים המעניקים שירותי מוקדים טלפוניים, הן כבעלי המידע והן כמחזיקי המאגרים עבור אחרים, לעמוד בדרישות החוק והתקנות ביתר שאת, לרבות קיום חובות אבטחת המידע, קיום בקרה ארגונית והתנהלות תקינה בכל הנוגע לחובות המוטלות על מחזיקי מאגרים.

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

1.2. תהליך העבודה

על מנת לממש את אחריותה באופן המיטבי, למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, מקיימת הרשות להגנת הפרטיות 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 הכוללים סיכונים מיוחדים לפרטיות, וממקד את תחומי העיסוק העתידיים של הרשות ואת תשתית תכנית העבודה. מגזר השירותים הטלפוניים (Call Centers) הוגדר כאחד מהיעדים בהם תמקד הרשות פעילותה.

כחלק מפעילות הליך פיקוח הרוחב פנתה הרשות ל- 14 גופים המעניקים שירותי מוקדים טלפוניים, בדרישה למילוי שאלוני ביקורת. במסגרת בחירת הגופים נלקחו בחשבון היקפי המידע, כמות נושאי המידע ורגישות המידע האישי הנאסף. לאחר ניכוי גופים שאינם עובדים עם מערכות ממוחשבות וגופים אשר השיבו במשותף מענה מאוחד (בשל פעילות עסקית מאוחדת, ניהול מאגר משותף או תשתית טכנולוגית משותפת), ולאחר ששני גופים הועברו להמשך פעילות אכיפתית, נמצאו תחת פיקוח הרוחב 5 גופים. לגופים אלה נשלחו שאלוני הביקורת שבחנו ארבעה קריטריונים עיקריים בתחום הגנת הפרטיות: (1) בקרה ארגונית, (2) ניהול מאגרי מידע (3) אבטחת מידע, (4) אבטחת מידע 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 כל חמשת הגופים 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 4 מהגופים שקיבלו הנחיות לתיקון ליקויים. במסגרת ביקורת זו נמצא כי הגופים שיפרו את העמידה בתקנות הגנת הפרטיות באופן משמעותי וכי נכון למועד הביקורת 58.1% מהליקויים יושמו וטופלו. בכוונת הרשות להגנת הפרטיות להמשיך ולפעול לאכיפת מדיניותה, ונשקלת האפשרות לשוב ולבחון עמידתם של המוקדים הטלפוניים בהוראת החוק ותקנותיו. כאשר ביחס לגופים שיימצא כי לא מילאו אחר ההנחיה לתיקון ליקויים, תשקול הרשות להטיל סנקציות בהתאם לסמכויותיה מכוח החוק.

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

1.3. ליקויים, מסקנות והמלצות עיקריות

בקרה ארגונית - מממצאי פיקוח הרוחב עלה כי במגזר זה נמצאה רמת עמידה בינונית-נמוכה בתחום הבקרה הארגונית, אשר באה לידי ביטוי בעיקר באי מינויו של ממונה אבטחת המידע, או במינוי שאינו עומד בהוראות התקנות בדבר עצמאותו ואי תלותו של ממונה אבטחת המידע בקרב הגופים אשר מחויבים לכך על-פי החוק. בנוסף, נמצא תיעוד חלקי של נהלי אבטחת מידע ותוכנית בקרה שנתית שוטפת בנושא אבטחת מידע שאינם עומדים בדרישות החוק.

ניהול מאגרי מידע – נמצאה רמת עמידה בינונית-נמוכה בכל הקשור לניהול מאגרי מידע, הנובעת בעיקר מאי רישום מאגרים אלו בפנקס המאגרים, ואי מסירת דיווחים שנתיים לרשם בגופים המחזיקים לפחות חמישה מאגרי מידע. דיווחים אלו צריכים לכלול רשימה של מאגרי המידע שברשות הארגון, ציון שמות בעלי המאגרים ושמו של ממונה האבטחה, וכן תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים. כמו כן, אותר כשל בהליך איסוף המידע, הנוגע לאי מתן הודעה לנושא המידע בעת איסוף המידע בהתאם לחוק.

אבטחת מידע – נמצאה רמת עמידה בינונית-גבוהה, כאשר הכשלים העיקריים בתחום זה נבעו ממנגנוני הרשאות שאינם עומדים בתקנות 8 ו-9 לתקנות אבטחת מידע באופן שיבטיח הפרדת סמכויות, קרי בחובה להבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בין המחזיק לבין בעליו של אותו מאגר; בתחום זה אותר גם כשל ביחס להעברת מידע ברשת הציבורית באופן שאינו מוצפן דיו, ואי קיום תהליך מובנה ומסודר בנוגע לביטול הרשאות למאגר.

עיבוד מידע אישי במיקור חוץ – נמצאה רמת עמידה בינונית-נמוכה בכל הקשור לאופן התקשרות של בעלי מאגרי המידע עם צדדים שלישיים המחזיקים במידע ומעבדים אותו, ובנוגע לאופן שבו הם מבטיחים הגנה על המידע; וכן בנושא נקיטת פעולות בכדי לוודא שהגורם החיצוני נוקט באמצעים הנדרשים כדי להגן על מאגרי המידע.

לאור הממצאים שעלו מהליך פיקוח הרוחב, קיבלו כל 5 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.**

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل
הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

ממצאי הליך פיקוח רוחב
בקרב מגזר מוקדים טלפוניים
(Call Centers)

אתגרים ומאפיינים חיוניים של מגזר מוקדים טלפוניים



מתן שירותים לאחרים המתאפיין בקבלת מידע אישי ממבקשי השירותים (בעלי המאגרים), כך שהמידע מנוהל על-ידי גופים אלו כמחזיק המאגר.



הטרוגניות בין גופי היעד מבחינת: גודל המאגר, מספר הרשומות במאגר, מספר מורשי הגישה, מספר בעלי הרשאה לגשת למאגר ומספר המאגרים הקיימים בכל גוף.



החזקה של לפחות חמישה מאגרי מידע עבור אחרים המחייבת עמידה בדרישות פרטניות בדין.

התהליך שבוצע במספרים



14
שאלונים שהופצו



7
גופים שהוסרו מהפיקוח



2
גופים שהועברו להמשך טיפול אכיפתי



1
דרישות להשלמת מידע חסר בכתב*



5
הנחיות לתיקון ליקויים

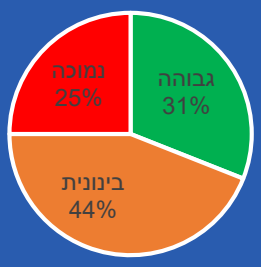
מתוכם על 4 גופים בוצע פיקוח מעקב

(*) נוכח משבר הקורונה בוצעו השלמות בכתב חלף פיקוחי שטח.

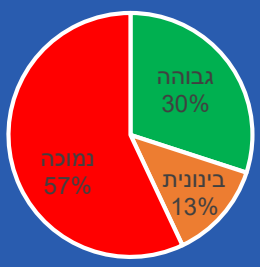
ממצאים – ליקויים מרכזיים

רמת עמידה גבוהה
רמת עמידה בינונית
רמת עמידה נמוכה

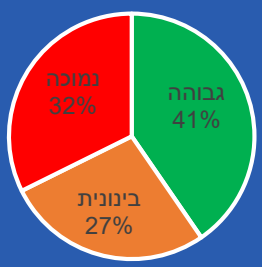
בקרה ארגונית



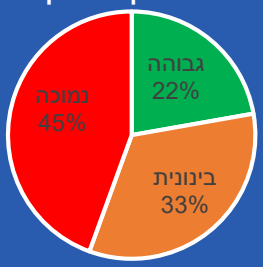
ניהול מאגרי מידע



אבטחת מידע



עיבוד מידע אישי במיקור חוץ



- בהתאם לתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע) על הגופים המסתייעים בגורמים המעניקים שירותי מוקדים טלפוניים לבחון, עוד בטרם ההתקשרות, 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). יובהר, כי גם כאשר בעל המאגר התיר למוקדים הטלפוניים לתת שירות הכרוך בגישה למאגר באמצעות גורם נוסף, על המוקדים הטלפונים לוודא עריכת הסכם מול הגורם הנוסף שיכלול את כלל ההתחייבויות המפורטות בתקנה 15, וזאת בהתאם לתקנה 15(א)(2)(ז) לתקנות
- על מחזיק בחמישה מאגרי מידע 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.
- יש לבחון את הצורך בעדכון מדיניות אבטחת המידע ולעדכנה בהתאם לנוהל.
- על הגופים להכין תכנית עבודה בנושא אבטחת מידע והגנת הפרטיות, לרבות התייחסות לנושא גורם אחראי ולוחות זמנים לביצוע, אשר תעמוד בדרישות תקנות הגנת הפרטיות (תקנה 3(ב)).



- על הגופים המחזיקים לפחות חמישה מאגרי מידע החייבים ברישום למסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשות הגוף, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על האבטחה.
- על הגופים לאפשר לנושאי המידע לעיין במידע אודותיהם המוחזק במאגר המידע בהתאם לבקשת בעל המאגר לאפשר למבקש את העיון. ככל שמתבצעת פניה ישירה של נושא המידע לגופים, עליהם להודיע לנושא המידע אם הם מחזיקים מידע עליו, וכן את שם בעל מאגר המידע ואת מענו, בהתאם לסעיף 13 לחוק. יש לתת הודעה לנושאי המידע בעת איסוף המידע, בהתאם לסעיף 11 לחוק, הכוללת התייחסות לשאלה האם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומהן מטרות המסירה.
- יש להטמיע מנגנון הרשאות המבוסס על הצורך לדעת ולוודא תקופתית כי ההרשאות הגישה הקיימות לעובדים תואמות עקרון זה.
- בהתאם לתקנה 14(ב) תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, , העברת מידע ממאגרי המידע ברשת ציבורית או האינטרנט תיעשה באמצעות שימוש בשיטות הצפנה מקובלות בלבד.
- בהתאם לתקנה 9 (ג) לתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, יש לבטל הרשאות בכל המאגרים לבעל הרשאה שסיים את תפקידו, מיד עם סיום תפקידו. לרבות לעניין מעבר תפקידים ככל שרלוונטי.

*3103 | 073-3928529 | ppa@justice.gov.il
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

2. מגזר מוקדים טלפוניים (Call Centers) - תמונת מצב

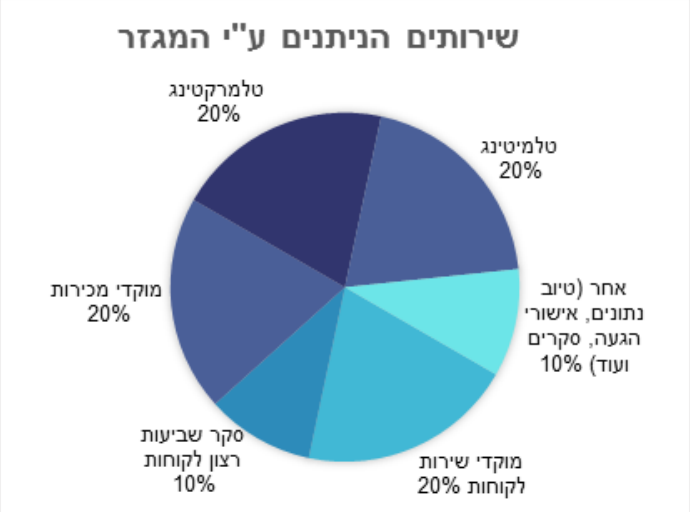
2.1 כללי

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

2.2 רקע על המגזר

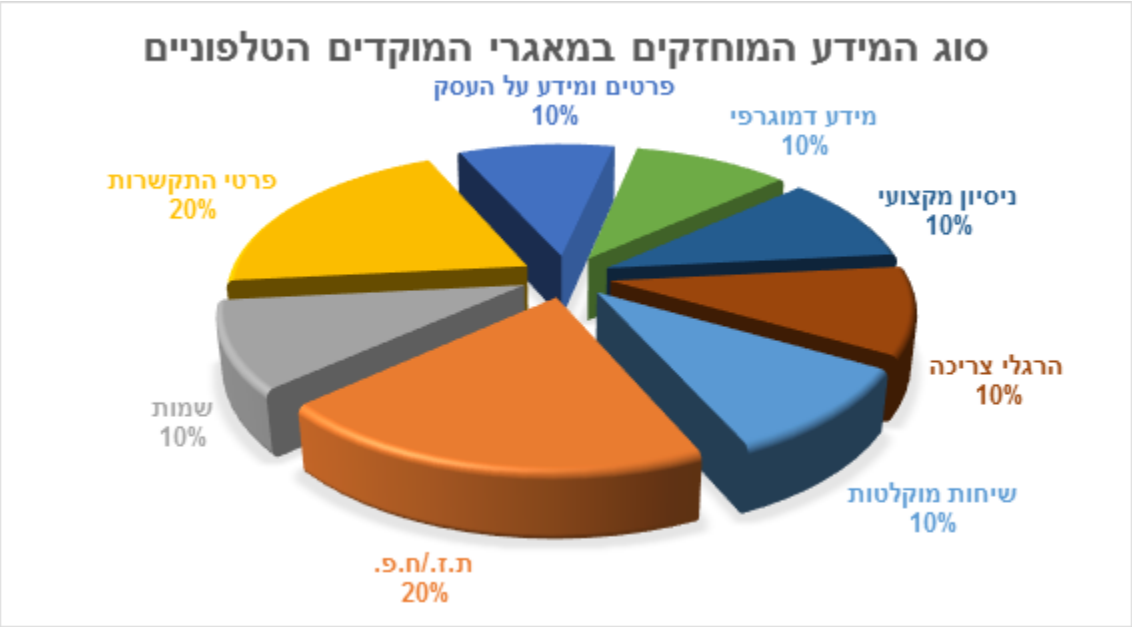
במסגרת סקר רוחבי במגזרי המשק שערכה הרשות להגנת הפרטיות, אשר בחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר המוקדים הטלפוניים כיעד פיקוח רוחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר, כדלהלן:

- מתן שירותים לאחרים המתאפיינים בקבלת מידע אישי ממבקשי השירותים (בעלי המאגרים), כך שהמידע מנוהל על-ידי גופים אלו כמחזיקי המאגר (כהגדרתו בחוק).
- הגופים הפועלים במגזר זה נותנים שירותים עבור מגוון רחב של חברות, העוסקות במגוון רחב של סוגי מידע, וכפועל יוצא מחזיקים במידע אישי מסוגים שונים, החל ממידע על אודות משק בית ועד למידע רפואי רגיש.
- מרבית הגופים מחזיקים עבור אחרים בחמישה מאגרי מידע לפחות, דבר המחייב עמידה בדרישות פרטניות בדין.



ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

ניהול המאגרים בהתייחס למאפייניו הייחודיים של המגזר מחייב את הגופים הפועלים במגזר זה לעמוד ביתר שאת בדרישות החוק והתקנות, תוך הגנה על פרטיותם של נושאי המידע, לרבות קיום חובות אבטחת המידע, קיום חובת השקיפות, התקשרות תקינה מול מי שמחזיק במידע במיקור חוץ וקיום בקרה ארגונית.



2.3. תהליך עבודה

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 הבאים: כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר או נושא מסוים, תלונות ספציפיות שהתקבלו ברשות, הצורך בבחינה מגזרית והבאת הגורמים המשתייכים למגזר לרמת עמידה נאותה התואמת את דרישות החוק והתקנות.

הליך פיקוח הרוחב במגזר המוקדים הטלפוניים כלל בסופו של דבר 5 גופים, כאשר גוף אחד נדרש לספק מידע, מסמכים והבהרות נוספות לרשות.[1] בשלב ראשון, נבחרו על ידי הרשות 14 גופים על בסיס בחינת היקפי המידע המוחזקים, כמות הלקוחות ורגישות המידע במסגרת השירותים שניתנים ללקוחות. בשלב השני, נוכו גופים אשר סיימו או שינו פעילותם, וכן גופים אשר השיבו

[1] נוכח משבר הקורונה בוצעו בהליך זה השלמות בכתב חלף פיקוחי שטח.

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

מענה מאוחד בשל פעילות עסקית מאוחדת, ניהול מאגר משותף או ניהול תשתית טכנולוגית משותפת.

בסיום ההליך, בכל 5 הגופים המפוקחים נמצאו ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות 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 המוקדים הטלפוניים, 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.

*3103 | 073-3928529 | ppa@justice.gov.il
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

3. ממצאים – ליקויים מרכזיים לפי קריטריונים ומבט השוואתי

ריכוז הממצאים ברמת יעד פיקוח הרוחב, ולפי התחומים שנבדקו

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

3.1. בקרה ארגונית

- במסגרת בחינת קריטריון זה, נמצא כי 44% מהגופים עמדו ברמה בינונית בהוראות החוק בנוגע לבקרה ארגונית, בעוד ש-25% מהגופים נמצאו כבעלי רמת עמידה נמוכה.
- בחלק מהגופים אשר מחויבים במינוי ממונה אבטחת מידע, נמצא כי ממונה אבטחת המידע ממלא תפקיד נוסף העלול להעמידו בחשש לניגוד עניינים במילוי תפקידו, בניגוד לדרישות התקנות בדבר עצמאותו ואי תלותו של ממונה אבטחת המידע.
- נמצאו גופים ללא נהלי אבטחת מידע וללא תכנית עבודה שנתית לבקרה שוטפת על העמידה בדרישות התקנות, או גופים שהנהלים שלהם אינם מספקים, בכך שאינם מקיפים את כלל הדרישות בהוראות התקנות.

3.2. ניהול מאגרי מידע

- במסגרת בחינת קריטריון זה, נמצא כי 70% מהגופים נמצאים ברמת עמידה בינונית או נמוכה, הבאה לידי ביטוי בליקויים באופן יישום הוראות החוק והתקנות.
- עיקר הליקויים נבעו מכך שגופים לא עמדו בדרישות החוק בנוגע לרישום מאגרי המידע שבבעלותם בפנקס מאגרי המידע. בגופים המחזיקים חמישה מאגרי מידע לפחות, לא נמסר לרשם מאגרי המידע, מדי שנה, דיווח הכולל רשימה של מאגרי המידע שברשותו, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו מורשי הגישה למאגר בהסכם בינו לבין בעל המאגר, ושמו של הממונה על האבטחה.
- עוד עולה מן הממצאים עלה כי בחלק מהגופים נמצאו ליקויים בכל הקשור לחובת השקיפות בנוגע למקור הסמכות לאיסוף המידע האישי, ואי עמידה בחובת יידוע נושאי המידע שעליהם מוחזק המידע, כנדרש לפי סעיף 11 לחוק, בעת פניה לאדם לקבלת מידע.

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

- כמו כן, במסגרת פניות הגופים לנושאי המידע בפנייה בדיוור ישיר, לא ציינו הגופים את 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'.

3.3. אבטחת מידע

- בקריטריון זה נמצאה רמת עמידה בינונית-גבוהה ב- 68% מהגופים בכל הקשור לאבטחת המידע, בעוד ש-32% מהגופים, נמצאו ברמת עמידה נמוכה.
- בין היתר, נמצאו ליקויים בניהול הרשאות הגישה למאגרים, בין אם בשל העובדה שלא נבנה כלל מנגנון הרשאות או מכיוון שמנגנון ההרשאות הקיים אינו עומד בדרישות התקנות.
- כמו-כן, נמצא כי בחלק מהגופים לא באו לידי ביטוי האמצעים בהם נקט הארגון כדי לוודא שקיימת הפרדה ברורה בין המאגרים הכוללים מידע אישי ליתר המאגרים.
- עוד עולה מהממצאים כי העברת מידע ממאגרי המידע ברשת ציבורית או ברשת האינטרנט בגופים שנבדקו, לא נעשית באמצעות שימוש בשיטות הצפנה מקובלות, או שלא הותקנו אמצעי הגנה מספקים אשר נותנים מענה לחדירה לא מורשית במאגרי המידע המחוברים לרשת האינטרנט או לרשת ציבורית אחרת, בהתאם לדרישה בתקנות.

3.4. עיבוד מידע אישי במיקור חוץ

- במסגרת בחינת קריטריון זה, נמצא כי כמחצית מהגופים נמצאו ברמת עמידה נמוכה בקריטריון זה (45%), 33% נמצאו ברמת עמידה בינונית ורק 22% מהגופים נמצאו ברמת עמידה גבוהה.
- מהממצאים עולה כי בתחום זה, הגופים בהם נמצאה רמת עמידה נמוכה לא ביצעו כלל את הפעולות הנדרשות בהתאם לתקנה 15, ולא יושמה הנחית רשם מאגרי המידע מס' 2/2011 בנושא שימוש בשירותי מיקור חוץ לעיבוד מידע אישי, בהתקשרויות עם ספקי מיקור חוץ כנדרש.[2]
- בנוסף, נמצא כי גופים אלו גם לא נקטו באמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות, או שלא נכללו התייחסויות בהסכם ההתקשרות ביחס לחובותיו ואחריותו של הספק, וזאת שלא בהתאם להוראות התקנות.

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

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

- יובהר, כי גם כאשר המוקדים הטלפוניים משמשים כמחזיקי מאגר עבור אחרים, עליהם לוודא עריכת הסכם מול כל גורם חיצוני נוסף שמחזיק במאגר, וזאת בהתאם להוראות תקנה 15(א)(2)(ז) לתקנות.

4. מסקנות / תמונת מצב והמלצות

ממצאי הליך פיקוח הרוחב עולה כי הגם שמרבית הגופים במגזר המוקדים הטלפוניים הינם בעלי היכרות עם דרישות החוק והתקנות, והטמיעו או מצויים בשלבי הטמעה של עיקרי הדרישות, **עדיין נמצאו ליקויים משמעותיים באופן יישום הוראות החוק והתקנות.**

<u>הנחיית הרשות היא כי על הגופים המשתייכים למגזר זה ליישם את הנקודות הבאות:</u>

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.[3]
- על הגופים לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות עדכון פרטי מנהל המאגר בפנקס המאגרים, ככל שמונה כזה, ומינוי ממונה אבטחת המידע ככל שהדבר נדרש לפי הוראת סעיף 17ב לחוק. בנוסף, יש לוודא שכתב המינוי כולל את כל הפרטים הנדרשים בהתאם להוראת סעיף 7 לחוק ולתקנה 4 לתקנות.
- 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 בנושא 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, וכזה הוא חייב במבדקי חדירות, עליו לוודא כי מבדקי החדירות בוצעו וכי הם עומדים בדרישות התקנות.

[3] לקריאה נוספת על רישום מאגר מידע ומטרותיו ראו קישור לאתר הרשות להגנת הפרטיות: https://www.gov.il/he/Departments/Guides/registration_faq.

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

4.2. ניהול מאגרי מידע

- על הגופים ליידע את בעל המידע בדבר המקור החוקי לאיסוף המידע על אודותיו, ובכל מקום שאין סמכות חוקית כזו, לקבל את הסכמתו לשמירת פרטיו במאגרים. זאת, תוך מתן הודעה בעת איסוף המידע בהתאם להוראות סעיף 11 לחוק, 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.[4]
- על הגופים המחזיקים ברשותם חמישה מאגרי מידע לפחות, החייבים ברישום לפי סעיף 8, למסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשותם, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו מורשי הגישה למאגר בהסכם בינו לבין בעל המאגר, ושמו של ממונה אבטחת המידע.
- על הגופים 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'.[5]
- על הגופים להקפיד לאפשר לנושאי המידע לעיין במידע על אודותיהם המוחזק במאגר מידע בהתאם לבקשת בעל המאגר, ובפניה ישירה של נושא המידע למסור אם הם מחזיקים מידע עליו, וכן את שם בעל מאגר המידע ואת מענו, בהתאם לסעיף 13 לחוק. לעניין זה, יודגש כי זכות העיון של אדם במידע שעליו חלה גם כאשר מדובר במידע כגון שיחות טלפוניות מוקלטות, תכתובות צ'ט, שיחות המצולמות בווידאו וכיו"ב, אשר נשמרות באופן דיגיטלי. כמו כן, יש להקפיד לאפשר לנושאי המידע לתקן או לשנות את המידע אודותיהם המוחזק במאגר מידע, 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.

[4] להרחבה בנוגע לחובת היידוע לפי סעיף 11 לחוק הגנת הפרטיות, ראו מסמך בנושא "חובת יידוע במסגרת איסוף ושימוש במידע אישי" (יולי 2022). המסמך זמין כאן.
[5] להרחבה בנוגע לדיוור ישיר ושירותי דיוור ישיר, ראו הנחיית רשם מאגרי המידע מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר". ההנחיה זמינה כאן.

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

- 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 אבטחת מידע.
- 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

- בהתאם לתקנה 15 לתקנות 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 שנותן שירות הכרוך בקבלת גישה למאגר, בו ייקבעו במפורש כל ההוראות המתחייבות על פי תקנה 15(א)(2) לתקנות, לרבות חובתו של הגורם החיצוני לדווח, לפחות אחת לשנה, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי התקנות וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה. יובהר, כי גם כאשר משמש המוקד הטלפוני כמחזיק מאגר עבור לקוחות, עליו 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]

[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.

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

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 תיקון ליקויים במגזר המוקדים הטלפוניים, 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, במסגרתם נבחנה מידת העמידה בהתחייבות לתיקון הליקויים, 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 התכנית, ותיקון יתרת הליקויים שטרם תוקנו.

במסגרת ביקורת המעקב שנעשתה בקרב 4 מהגופים במגזר המוקדים הטלפוניים שקיבלו הנחיות לתיקון ליקויים, נמצא כי נכון למועד הביקורת הגופים שיפרו את העמידה בתקנות הגנת הפרטיות באופן משמעותי וכי 58.1% מהליקויים יושמו וטופלו.

כמות הליקויים הראשונית עמדה על 62 ליקויים בכלל המפוקחים. כמות הליקויים שנותרה לאחר המעקב עמדה על 26 ליקויים, דהיינו 36 ליקויים - תוקנו.

נציין כי ביחס לגופים שיימצא כי לא מילאו אחר ההנחיה לתיקון ליקויים, רשאית הרשות להטיל סנקציות נוספות העומדות לרשותה מכוח החוק.

פיקוחי המעקב שבוצעו במגזר המוקדים הטלפוניים מעידים באופן חד משמעי על כך שעצם 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.

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

6. סיכום

בפעילות מגזר הגופים הנותנים שירותי מוקדים טלפוניים, קיימים סיכונים לא מעטים לפרטיות אשר נובעים מאחזקת מידע רב, מזוהה ורגיש, וניהול קשר אינטראקטיבי עם נושאי המידע באמצעות הגופים ובאמצעות מיקור חוץ. כל אלה דורשים הקפדה יתרה על קיום הוראות תקנות הגנת הפרטיות (אבטחת מידע), שקיפות מול נושא המידע, ומילוי החובות החלות מכוח פרק הדיווח הישיר בחוק הגנת הפרטיות.

ממצאי הליך פיקוח הרוחב במגזר המוקדים הטלפוניים מצביעים על ליקויים בעיקר בנוגע לעמידה בהוראות החוק בתחום עיבוד המידע האישי באמצעות מיקור חוץ, ובנוגע לאי עמידה בהוראות החוק בנוגע לניהול 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 ותכנית מסודרת לתיקונם.

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. בנוסף, 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 אם חל שינוי ברמת הציות להוראות החוק במגזר המוקדים הטלפוניים, וזאת בין היתר על ידי בחינת מוקדים טלפוניים נוספים, במועד שייקבע לאחר פרסום הדו"ח המגזרי.

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

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

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
בקרה ארגונית			
לא בוצע סקר סיכונים או ביקורות בנושא אבטחת מידע והגנת הפרטיות בשלוש השנים האחרונות.	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**
ממונה אבטחת המידע ממלא תפקיד נוסף העלול להעמידו בחשש לניגוד עניינים במילוי תפקידו	יש למנות כממונה אבטחת מידע אדם בעל הידע המתאים, שאינו ממלא תפקיד נוסף העלול להעמידו בחשש לניגוד עניינים במילוי תפקידו.	פרטי הממונה על אבטחת המידע חוק הגנת פרטיות, תשמ"א-1981 סעיף 17ב. תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 3.	**מינוי ממונה 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 ממונה אבטחת מידע.	בהתאם לסעיף 17ב לחוק, על מחזיק בחמישה מאגרי מידע החייבים ברישום לפעול למינוי ממונה על אבטחת המידע.	סעיף 17ב לחוק	**מינוי ממונה אבטחת מידע**
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**

*3103 | 073-3928529 | ppa@justice.gov.il
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

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**
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**

*3103 | 073-3928529 | ppa@justice.gov.il
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

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**
לא ננקטים אמצעים סבירים לצורך ווידוא כי הגישה למאגרים נעשית בידי בעלי ההרשאה בלבד למאגר המידע/מערכת מידע.	יש להטמיע מנגנון הרשאות המבוסס על הצורך לדעת (בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות) ולוודא תקופתית כי הרשאות הגישה הקיימות לעובדים תואמות עיקרון זה.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 8, תקנה 9 (א)	**מנגנון הרשאות**
לא ננקטו אמצעים מקובלים כדי לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות	יש להטמיע מנגנון הרשאות המבוסס על הצורך לדעת (בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות) ולוודא תקופתית כי הרשאות הגישה הקיימות לעובדים תואמות עיקרון זה.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017 תקנה 9	**ניהול הרשאות.**
בכניסה למאגר על ידי עובד הארגון לא נעשה שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.	במאגרים שחלה עליהם רמת אבטחה 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**

*3103 | 073-3928529 | ppa@justice.gov.il
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
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**
לא קיים תהליך שמירה או גיבוי ללוג אבטחת המידע, או שמשך שמירת הגיבוי לא תואם לתקנה.	במאגרים בעלי רמת אבטחה בינונית או גבוהה, יש לפעול להטמעת תהליכי גיבוי ללוג אבטחת מידע, וקביעת נהלים וביצוע גיבויים ללוג נתוני האבטחה במאגר באופן שיבטיח שניתן יהיה, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי בהתאם לתקנות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 17(ב) ותקנה 18	**גיבוי נתוני אבטחה**

*3103 | 073-3928529 | ppa@justice.gov.il
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
ניהול מאגרי מידע			
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 ניתנת הודעה בהתאם לדרישות סעיף 11 לחוק.	מתן הודעה לנושא המידע 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**
בגופים המחזיקים חמישה מאגרי מידע לפחות לא נמסר לרשם מאגרי המידע, מדי שנה, דיווח אודות המאגרים בהתאם לסעיף 17א(ב) לחוק	על גופים המחזיקים ברשותם חמישה מאגרי מידע לפחות החייבים ברישום לפי סעיף 8, למסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשות הגוף, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על האבטחה.	חוק הגנת הפרטיות, תשמ"א – 1981, סעיף 17א (ב)	**חובת מסירת דיווח שנתי לרשם, החלה על מחזיק בחמישה מאגרי מידע לפחות**

*3103 | 073-3928529 | ppa@justice.gov.il
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
לא ניתן לנושא המידע לעיין במידע על אודותיו כנדרש בסעיף 13 לחוק, או שניתנה לו אפשרות לעיין באופן חלקי בלבד	על הגופים לאפשר לנושאי המידע לעיין במידע על אודותיהם המוחזק במאגר מידע בהתאם לבקשת בעל המאגר, ובפניה ישירה של נושא המידע למסור אם הם מחזיקים מידע עליו, וכן את שם בעל מאגר המידע ומענו, בהתאם לסעיפים 13 ו-13א לחוק.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 13	**עיון במידע.**
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 - סעיפים 17 ג', 17 ד', 17 ה', 17 ו'	**דיוור ישיר ושירותי דיוור ישיר**

*3103 | 073-3928529 | ppa@justice.gov.il
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

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**

*3103 | 073-3928529 | ppa@justice.gov.il
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa