דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב
בקרב מגזר חברות כוח אדם והשמה



תוכן עניינים

1.תקציר מנהלים..... 4

1.1.מגזר חברות כוח אדם והשמה..... 4

1.2.תהליך העבודה..... 5

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

2.פיקוח חברות כוח אדם והשמה - תמונת מצב..... 8

2.1.כללי..... 8

2.2.רקע על המגזר..... 8

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 על-ידי גורם חיצוני..... 15

3.3.אבטחת

מידע..... 16

4.מעקב תיקון ליקויים 18

5.סיכום..... 19

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, איתור כשלים ענפיים וכלל-משקיים הדורשים התייחסות מוגברת של הרגולטור, וקבלת תמונת מצב כלל-מגזרית לגבי עמידה בהוראות החוק והתקנות.

1.1. מגזר חברות כוח אדם והשמה

במסגרת סקר רוחבי שערכה הרשות להגנת הפרטיות אשר בחן את סיכוני הפרטיות במשק, מגזר חברות כוח אדם והשמה בישראל אותר כאחד מיעדי פיקוח הרוחב המשמעותיים, וזאת בשל מאפייניו הייחודיים של מגזר זה בתחום הפרטיות, הבאים לידי ביטוי במספר היבטים:

1. סוג שירותים הנוגע למרבית האוכלוסייה, וכפועל יוצא - איסוף מידע על כמות גדולה במיוחד של נושאי מידע.
2. מאגרי מידע המכילים מידע אישי בהיקפים נרחבים במיוחד, אשר מנוהלים על ידי מספר רב של גופים וחברות הפועלים בתחום.
3. מנגנוני תפעול גדולים המאפשרים גישה בהיקף נרחב במיוחד למידע אישי.

ניהול מידע רגיש בהיקפים גדולים מחייב את החברות לעמוד בדרישות אבטחת המידע, לקיים מנגנון הרשאות גישה יעיל בהתאם לצורך לדעת ולקיים מעקב ובקרה בקרב ספקים חיצוניים המקבלים גישה למידע.

1.2. תהליך העבודה

בהליך פיקוח הרוחב במגזר זה, פנתה הרשות ל-31 חברות כוח אדם והשמה בדרישה למילוי שאלוני ביקורת. יצוין כי בהליך בחירת הגופים נלקחו בחשבון היקפי המידע ורגישות המידע הנאסף. בסופו של יום, השיבו 26 גופים המנהלים מאגרי מידע של עובדים ומועמדים לעבודה, כאשר שני גופים נוספים הועברו להמשך טיפול אכיפתי, ובשאר התברר כי סיימו פעילותם או שינו את תחום פעילותם, או שהשיבו מענה מאוחד בשל פעילות עסקית מאוחדת, ניהול מאגר משותף או תשתית טכנולוגית משותפת. שאלוני הביקורת בחנו שלושה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית, ניהול מאגרי מידע לרבות השימוש בגורם חיצוני, ואבטחת מידע. הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם, המעידים על רמת עמידתם בהוראות חוק הגנת הפרטיות ובתקנות מכוחו. לאחר קבלת השאלונים המלאים מהגופים המפוקחים, בחנה הרשות את המענה והמסמכים הנלווים. בסיום ההליך, נמצאו ליקויים הדורשים תיקון בכלל הגופים שנבדקו, ובהתאם דרשה הרשות מאותם גופים לתקן את הליקויים שנמצאו, ולספק תכנית מפורטת לתיקונם, בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים. כחלק מההליך, בדקה הרשות באמצעות ביקורת חוזרת את אופן תיקון הליקויים בחלק מן הגופים. ממצאי הביקורת החוזרת העלו כי הגופים שיפרו את עמידתם בהוראות החוק והתקנות באופן משמעותי.

1.3. ליקויים, מסקנות והמלצות עיקריות

במגזר חברות כוח אדם מרבית הגופים הציגו רמת עמידה חלקית בלבד בהוראות החוק והתקנות בשקלול כל התחומים שנבדקו, ורק כרבע מכלל הגופים נמצאו ברמת עמידה מלאה.

בשקלול הציונים שניתנו לגבי מידת העמידה בהוראות החוק והתקנות, נמצא כי הציון הממוצע של המגזר עומד על 64%.

ביתר פירוט, ממצאי הליך פיקוח הרוחב מלמדים על חוסר בקיאות מספקת בדרישות תקנות אבטחת מידע. יצוין, כי ממצאי פיקוח הרוחב העלו כי רמת העמידה בדרישות אבטחת המידע נמוכה באופן מובהק - כ-80% מן הגופים לא עומדים בדרישות התקנות במלואן, כאשר מחצית הגופים מצויים ברמת אי עמידה, והשאר בעמידה חלקית.

בתחום ניהול מאגרי מידע, פחות ממחצית הגופים מצויים ברמת עמידה מלאה. קרוב למחצית מן הגופים מצויים ברמת עמידה חלקית.

נוכח הממצאים שעלו מהליך פיקוח הרוחב, כל הגופים שנבדקו (26 גופים) קיבלו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם.

ממצאי הליך פיקוח רוחב
בקרב מגזר חברות כוח אדם והשמה

דו"ח פיקוח רוחב 2019-2020

אתגרים ומאפיינים ייחודיים של מגזר חברות כוח אדם והשמה

איסוף מידע על מספר גבוה במיוחד של נושאי מידע. תחום התעסוקה נוגע לרוב הגדול של האוכלוסייה, והזדקקות לשירותי חברות כח אדם והשמה הינה נפוצה מאוד. כפועל יוצא, חברות בתחום עשויות להחזיק במאגרי מידע בהיקף גדול במיוחד.

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

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

התהליך שבוצע במספרים

31 שאלונים שהופצו

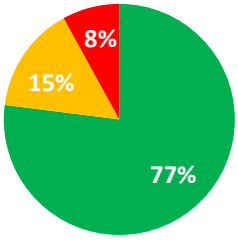
20 גופים שנדרשו להשלמת ידיעות ומסמכים

26 גופים שהשתתפו בפועל בהליך הפיקוח (ללא גופים שהוסרו מההליך או לא שיתפו פעולה)

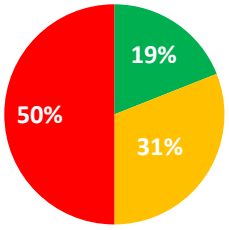
26 הנחיות לתיקון ליקויים

ממצאים – ליקויים מרכזיים:

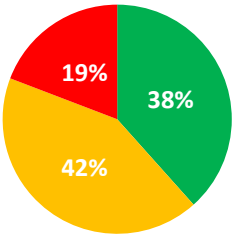
ממצאי ליקויים בחתך קריטריונים על פני פירוט עמידת מפוקחי המגזר



בקרה ארגונית



אבטחת מידע

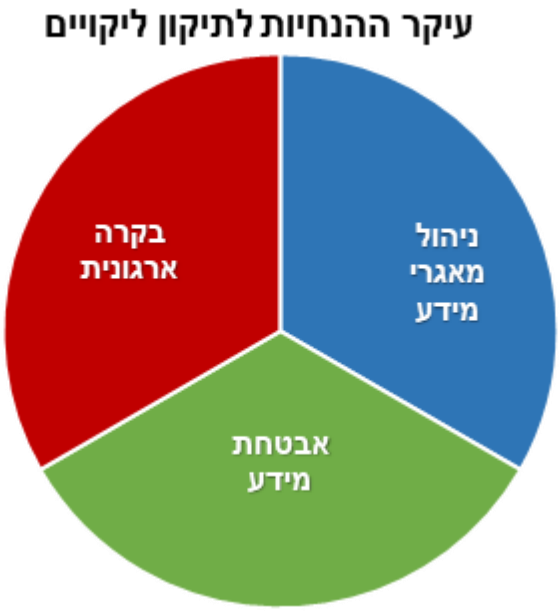


ניהול מאגרי מידע

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

- מיקור חוץ (עיבוד מידע על-ידי גורם חיצוני) - בהתאם לתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), יש לפעול לעיגון במסמך ההתקשרות התייחסות לחובותיו ואחריותו של גורם חיצוני, בהתאם להוראות התקנות.
- מיקור חוץ - ווידוא כי כל גוף צד ג' אשר נותן שרותים בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע מדי 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 אחרת הכפוף ישירות למנהל המאגר.
- עריכת ביקורות בנושא אבטחת מידע/הגנת הפרטיות מדי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה.



- יש להבטיח כי המערכות יישמרו במקום מוגן, המונע חדירה וכניסה ללא הרשאה התואמת את אופי פעילות המאגר ורגישות המידע בו. במאגרי מידע עליהם חלה רמת אבטחת מידע בינונית או גבוהה על בעל המאגר לנקוט בנוסף באמצעים לבקרה ולתיעוד של הכניסות והיציאות ושל כל הכנסה והוצאה אל מערכות המאגר ומהן.
- תיעוד כל אירוע המעלה חשש לאירוע אבטחה, בנוסף נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחה מידע.
- הגבלת או מניעת אפשרות לחיבור התקנים ניידים, ושימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.
- התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב במאגר המידע המחוברים לרשת האינטרנט או לרשת ציבורית אחרת בהתאם לדרישות התקנות.
- במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע מבדקי חדירה אחת לשנה וחצי, תוך בחינת הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת המבדקים.

2. חברות כוח אדם והשמה - תמונת מצב

2.1. כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2019 למאי 2020 במגזר יעד חברות כוח אדם והשמה, ולביקורות מעקב על פיקוחים אלו שבוצעו בתקופה שבין החודשים ינואר-מרץ 2021.

2.2. רקע על המגזר

תחום שרותי כוח-אדם מתאפיין בהיקף פעילות גדול במיוחד של חברות אשר מספרן עומד על כ-300, ובהן חברות גדולות במיוחד המחזיקות בנתח שוק מרכזי.

קיימים שני מודלים עיקריים לשירותים המסופקים על ידי חברות כוח האדם:

<u>שירותי כוח אדם</u>

במודל זה, חברת כוח האדם הינה מעסיקתו של העובד. החברה מבצעת איתור, גיוס, איוש, והצבת עובדים מקצועיים ומיומנים בתחומים שונים ובמגוון משרות במשק.

<u>מודל השמה</u>

במודל זה מספקת החברה ללקוחותיה שרותי איתור וגיוס עובדים לפי צרכי הלקוח. אוכלוסיית המועמדים כוללת מגוון רחב של תחומי תעסוקה החל מבלתי מקצועיים, בעלי מקצועות טכניים, סטודנטים בתקופת הלימודים, אקדמאים וכלה בעובדים בכירים. במסגרת זו מחזיקות החברות מידע רב מאוד על מי שאינם עובדי החברה.

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

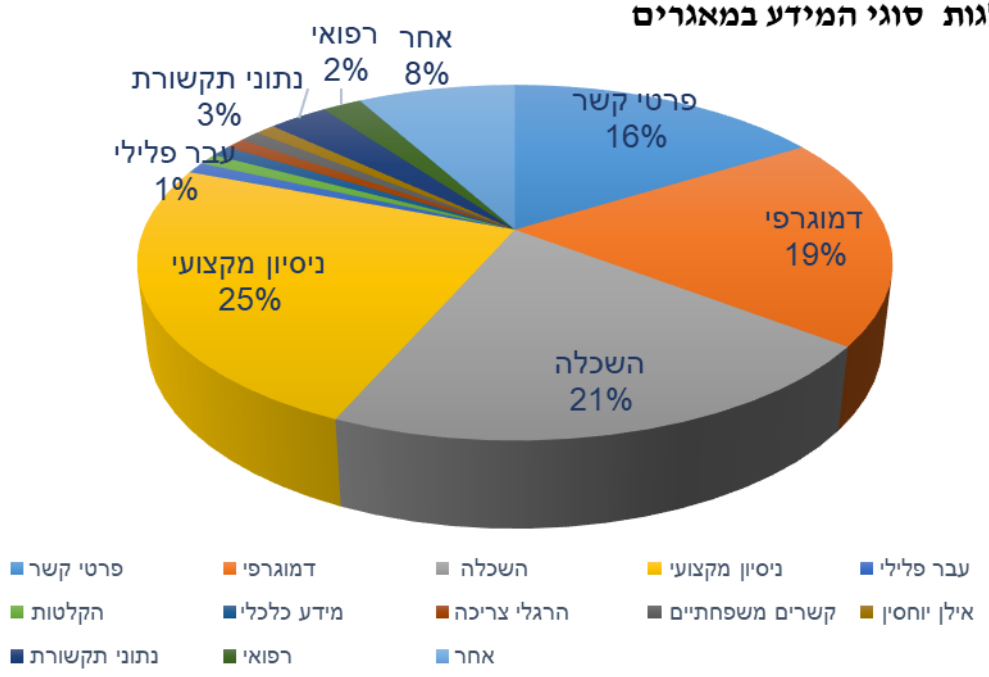
מאגרי מידע בהיקף גדול במיוחד

- מגזרי הפעילות של חברות כוח אדם מבוססים על מאגרי מידע הכוללים מאגרי עובדים בתחומים השונים.
- הזיקה של אוכלוסיות רחבות לשירותי תעסוקה, ומספרן הרב של החברות העוסקות בתחום, מביא לריכוז של מידע בהיקפים גדולים במיוחד.
- בחברות הגדולות, היקף המאגר עשוי לכלול מידע על מעל למיליון מועמדים.
- איסוף מידע אישי בהיקפים עצומים אלו, מהווה סיכון פוטנציאלי משמעותי לפרטיות המידע של הרשומים במאגרים.

רגישות המידע

- החברות הפועלות במגזר כוח אדם נדרשות לסווג את העובדים הקיימים במאגריהן על פי מספר מאפיינים, המצריכים אגירת מידע אישי רב, וברובו רגיש.
- פגיעה אפשרית במאגרי המידע, עלולה להיות משמעותית במיוחד לאור רגישות המידע השמור במאגרי החברות.

התפלגות סוגי המידע במאגרים



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. סקר סיכוני הפרטיות 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 האכיפה של הרשות. התוכנית נבנית בהתחשב בגורמים הבוחנים את כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר/נושא, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה מגזרית והבאתו לרמת עמידה נאותה.

הליך הפיקוח החל ב- 31 גופים המשתייכים למגזר חברות כוח אדם והשמה, שנבחרו על ידי הרשות. בסופו של יום, השיבו 26 גופים לשאלוני הפיקוח, כאשר שני גופים נוספים הועברו להמשך טיפול אכיפתי, ובשאר התברר כי סיימו פעילותם, שינו את תחום פעילותם, וחלקם השיבו מענה מאוחד בשל פעילות עסקית מאוחדת, ניהול מאגר משותף או תשתית טכנולוגית משותפת.

בסיום ההליך, בכל 26 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 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]

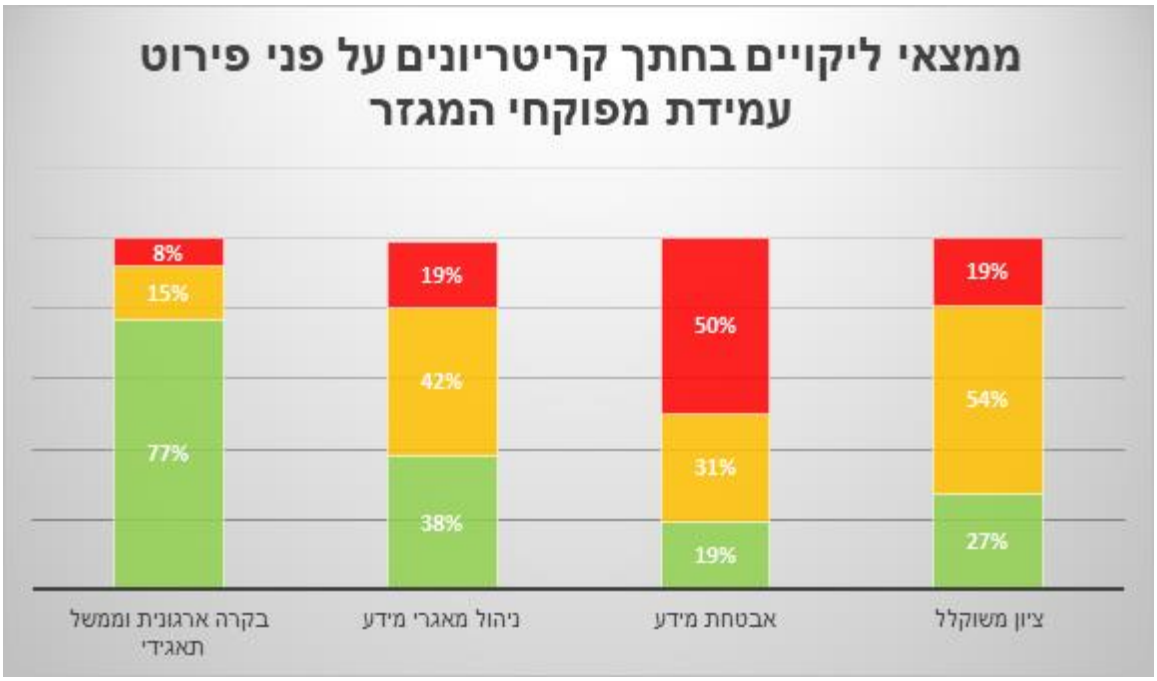


[1] קריטריון עיבוד מידע אישי על-ידי גורם חיצוני נבחן בהליך זה כקריטריון משנה תחת ניהול מאגרי מידע.

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 50% - 80% מוגדרת כרמת עמידה בינונית או חלקית;
- עמידה של מתחת ל-50% מוגדרת כרמת עמידה נמוכה.

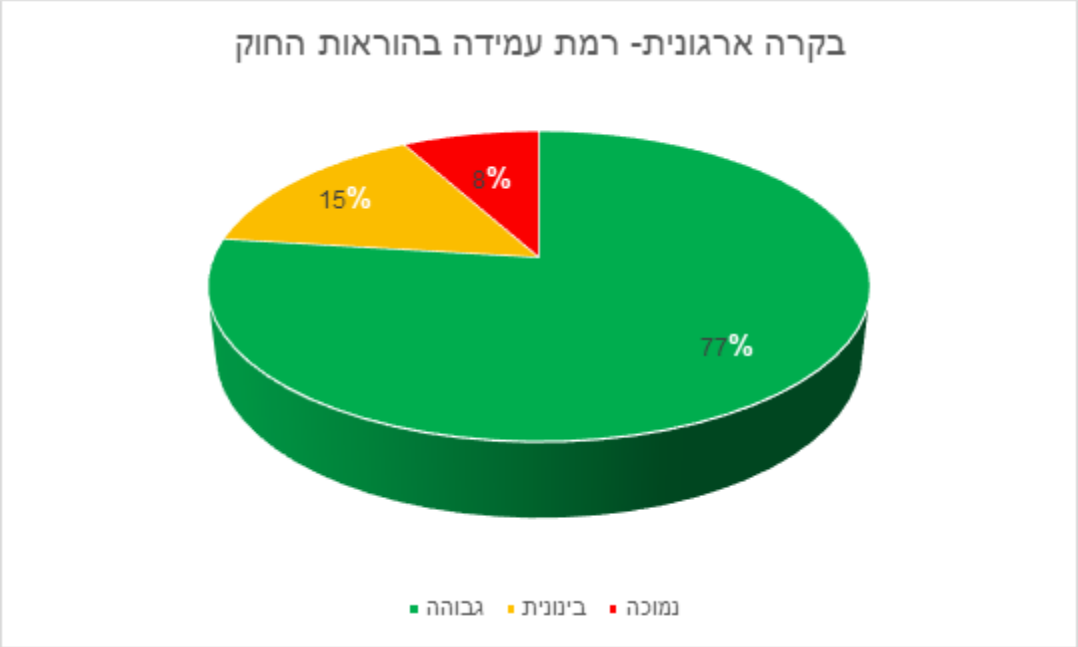
3. ממצאים – ליקויים מרכזיים לפי קריטריונים ובמבט השוואתי והמלצות:

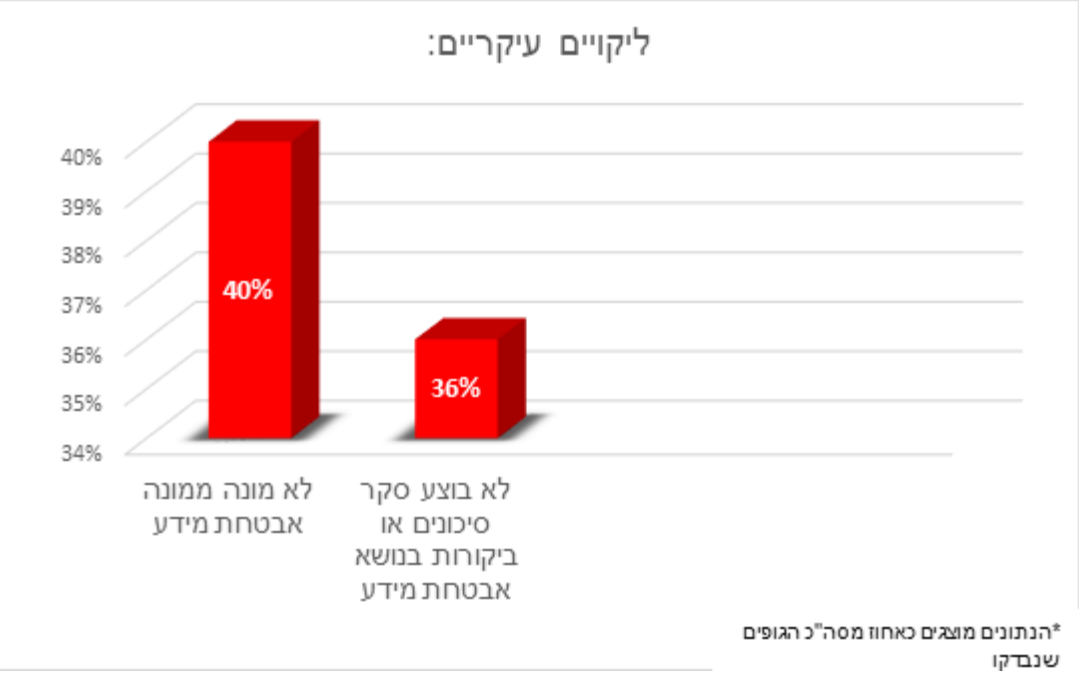


בתחום אבטחת מידע כ-80% מן הגופים לא עומדים בדרישות התקנות. מחצית הגופים מצויים ברמת עמידה נמוכה, וכשליש ברמת עמידה בינונית. בתחום ניהול מאגרי מידע, כרבע מהגופים מצויים ברמת עמידה מלאה, וקרוב למחצית מן הגופים מצויים ברמת עמידה בינונית. בציון המשוקלל, מרבית הגופים הציגו רמת עמידה בינונית בלבד.

בקרה ארגונית

ממצאים:





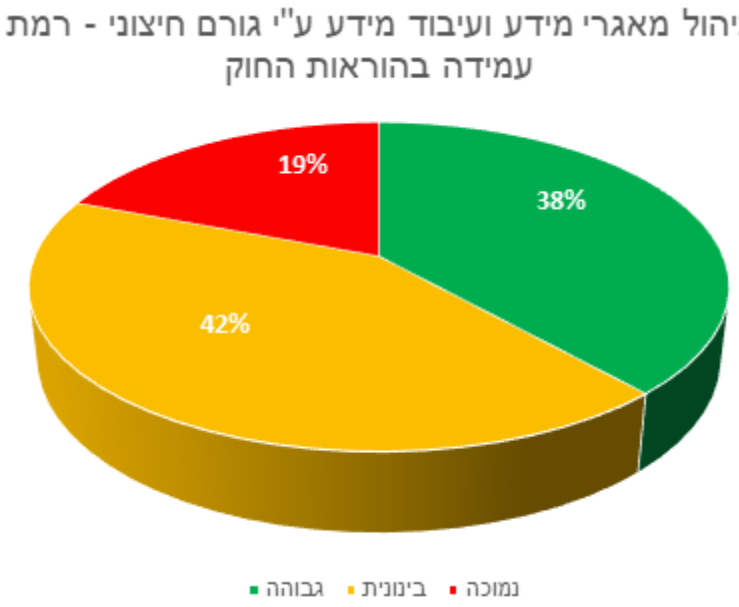
*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

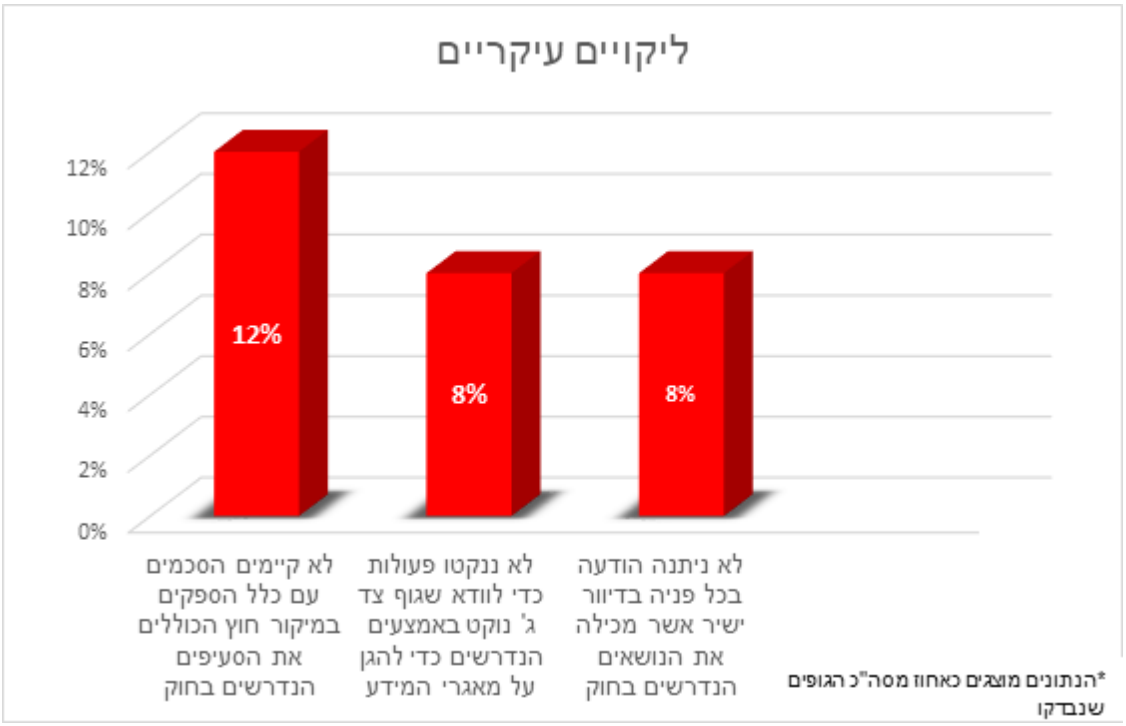
המלצות:

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

ניהול מאגרי מידע ועיבוד מידע על-ידי גורם חיצוני

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. יש לציין את המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה, בהתאם להוראת סעיף 11 לחוק.
- בהתאם לתקנה 15 לתקנות אבטחת מידע, על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות.
- בנוסף, על הגופים לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, בו ייקבעו במפורש כל הרכיבים המנויים בתקנה 15(א)(2) לתקנות, לרבות חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי התקנות וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה.
- בעניין זה יש לנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות, כנדרש בתקנה 15 ובהנחיית רשם מאגרי המידע מס' 2/2011.

3.1. אבטחת מידע

ממצאים:

המלצות:

- על הגופים לבצע בחינה עצמית לצורך סיווג רמת אבטחת המידע של מאגרי המידע בהתאם לקבוע בתוספת לתקנות. על הגופים לבדוק את סוג המידע שהם אוספים, את המטרות והשימושים שנעשים במידע הנ"ל. בעניין זה, עמדת הרשות היא כי רמת אבטחת המידע של מאגרי המידע לפי התקנות אינה משתנה, גם אם מאגרי המידע מנוהלים או מעובדים בצורה מפוצלת על גבי מספר מערכות טכנולוגיות שונות בעלות כמות שונה של בעלי הרשאה, שכן הבחינה לצורך סיווג רמת האבטחה הינה מהותית, ואינה תלויה בהיבטים הטכניים של אופן ניהול המידע. בהתאם לכך, מספר בעלי ההרשאה לצורך קביעת רמת האבטחה של המאגר הינו סך כל בעלי ההרשאה לכלל המערכות הטכנולוגיות המשמשות את מאגר המידע הרלוונטי.

- על הגופים לוודא כי תיעוד של אירועי אבטחת מידע יישמר, ויגובש נוהל עבודה סדור בנושא ,בהתאם לתקנה 11 לתקנות. בנוסף, על נוהל העבודה לכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח המיידי לרשות בהתאם[2] והליך הפקת לקחים במקרה של אירוע אבטחת מידע .במאגרי מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמת אבטחה בינונית אחת לשנה) באירועי האבטחה ולבחון את הצורך בעדכון הנוהל.
- על הגופים לבחון את הצורך בחיבור אמצעים נתיקים. ככל שיוחלט כי לא קיים צורך ממשי או שהצורך מינימאלי – מוצע להגביל השימוש למתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד למערכת, ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. במקרים בהם יוגדר כי קיים צורך בשימוש באמצעים נתיקים, יש להצפין הנתונים באמצעות שיטות הצפנה מקובלות.
- על הגופים לוודא שבכניסה לאתר האינטרנט המאפשר גישה למאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, בהתאם לתקנה 9(ב)(2) לתקנות, וכן לוודא קיום תיעוד עבור אירועי אבטחת מידע, בהתאם לתקנה 11 לתקנות.
- על הארגון לקבוע מדיניות סיסמאות חזקה הכוללת סיסמאות מורכבות המוחלפות בתדירות של עד 6 חודשים. כמו כן יש לעגן את מדיניות הסיסמאות בנוהל עבודה, כנדרש בתקנה 9 (ב) לתקנות.
- על הארגון לנהל מנגנון תיעוד אוטומטי, שיאפשר ביקורת על הגישה למערכות המאגר ויכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה, כנדרש בתקנה 10 . 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.

[2] להרחבת קריאה על דיווח מיידי על אירוע אבטחת מידע ר' בקישור זה

4. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

במהלך שנת 2021, נערך מעקב תיקון ליקויים במגזר חברות כוח אדם והשמה, 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 בנוגע לתיקון הליקויים. בעת פיקוח המעקב בחנה הרשות את אופן התקדמות תיקון הליקויים אצל הגופים, את העמידה בלוחות הזמנים שהגדירו ליישום התוכנית ותיקון יתרת הליקויים שטרם תוקנו.

במסגרת ביקורת המעקב שנעשתה בקרב 42% מהגופים במגזר חברות כוח אדם והשמה שקיבלו הנחיות לתיקון ליקויים, נמצא כי הגופים שיפרו את העמידה בתקנות הגנת הפרטיות באופן משמעותי וכי 56% מהליקויים יושמו וטופלו.

לגבי הגופים המפוקחים בכלל ולגבי הגופים בהם בוצע פיקוח מעקב 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 ואבטחת מידע כתוצאה מהליך פיקוח הרוחב.

5. סיכום

כאמור, בחברות מגזר כוח אדם והשמה מנוהלים נתונים רגישים אודות חלק ניכר מהאוכלוסייה. ממצאי הליך פיקוח הרוחב במגזר זה העלה ממצאים המצביעים על ליקויים, בעיקר בנוגע לעמידה בהוראות החוק בתחום אבטחת מידע וניהול מאגרי מידע.

יצוין כי חלק משמעותי יחסית מן הגופים במגזר חברות כוח אדם והשמה, מחזיק במאגרים בהם נדרשת רמת אבטחה גבוהה, וכי התמונה העולה מהליך הפיקוח מצביעה על כך שהמודעות במגזר זה לנושא אבטחת המידע והגנת הפרטיות אינה הולמת את רגישות המידע המוחזק בידי חברות במגזר, בהיקפים גדולים. ממצאי פיקוח הרוחב העלו כי המגזר מצוי ברמת עמידה בינונית בתחום ניהול מאגרי מידע, ומעבר לאיוש תפקידים והקפדה על מבנה ארגוני פורמלי כנדרש, דרישות שבהן עומדים מרבית הגופים, יישום פרקטיקות שוטפות הנדרשות לאבטחת המידע והגנת הפרטיות של נושאי המידע, לוקה בחסר. כ-80% מן המפוקחים שנבדקו מצויים ברמת עמידה נמוכה או בינונית

בתחומי אבטחת מידע וניהול מאגרי מידע. בעניין זה נמצאה חולשה רוחבית בנוגע לבחינת הסיכונים ופיקוח על רמת אבטחת המידע, שבאה לידי ביטוי ברמת מוכנות ומודעות בינונית עד נמוכה ובאי קיום של חובת ביצוע סקר סיכונים ובדיקת חדירות, אצל גופים רבים.
עם זאת, ניכר, כי עצם קיום הליך פיקוח הרוחב עורר אצל הגופים שנבדקו תהליך בחינה והנעה לשיפור אופן הציות לחוק ולתקנות, כאשר בסיום ההליך כאמור, הגופים שבהתנהלותם נתגלו ליקויים, נדרשו להציג לרשות התחייבות נושא משרה ותכנית עבודה לתיקון הליקויים.

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלי מאגרי מידע והמחזיקים בהם באמצעות הליך פיקוחי הרוחב, לרבות באמצעות ביקורות חוזרות בגופים שהונחו לתקן ליקויים, וזאת לשם הגברת עמידתם בהוראות החוק והתקנות, ועל מנת לחזק את ההגנה על הזכות החוקתית לפרטיות. במסגרת תכנית העבודה של הרשות ולשם בחינת ההשפעה שיצרה פעילות פיקוח הרוחב על המגזרים שנבדקו, תשקול הרשות לבחון את השינוי היחסי ברמת הציות להוראות החוק במגזר חברות כוח אדם והשמה, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.