מחלקת אכיפה

תאריך: 27/01/2021
י"ד שבט, תשפ"א

[redacted]

באמצעות: דוא"ל ודואר רשום

לכבוד,
מר צוריאל ימין
מנכ"ל חברת אלקטור תוכנה בע"מ
רחוב יריחו 5, אשקלון

הנדון: **קביעת הפרה של חוק הגנת הפרטיות, התשמ"א - 1981**

1. הרשות להגנת הפרטיות במשרד המשפטים (להלן: "**הרשות**") קיימה הליך פיקוח מתוקף הסמכות המוקנית לרשם מאגרי המידע ולמפקחים מטעמו בסעיפים 10(ג) ו-10(ה1) לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**החוק**") לבירור הפרות לכאורה של הוראות החוק לרבות חובת אבטחת מידע במסגרת מקרה דלף מידע מתוך פנקס הבוחרים ממערכות המידע של חברת אלקטור תוכנה בע"מ ח.פ. 515847051 (להלן: "**החברה**" או "**אלקטור**").

2. אלקטור סיפקה למפלגות "הליכוד" ו"ישראל ביתנו" (להלן: "**המפלגות**"), שירותים טכנולוגיים לניהול מערכת בחירות, באמצעות אפליקציית "אלקטור" (להלן: "**האפליקציה**") אגב מערכת הבחירות לכנסת ה-23. לצורך כך, המפלגות העבירו כל אחת לאלקטור עותק מפנקס הבוחרים לכנסת ה-23, אותו קיבלו ממשרד הפנים במסגרת הוראות חוק הבחירות.

3. פעולות הפיקוח אשר בוצעו על ידי הרשות פורטו במכתב ההפרה לכאורה אשר נשלח אל החברה ביום 12.8.2020 (סימוכין 008-2020-00014992) (להלן: "**מכתב ההפרה לכאורה**"), ביניהן:

3.1 הליך הפיקוח נפתח בעקבות מידע מיום 8.2.2020 על דליפתו לרשת האינטרנט של קובץ המכיל מידע מפנקס הבוחרים על אודות כ-6.5 מיליון בעלי זכות בחירה בישראל וכן של רשומות נוספות שמקורן במערכות המידע של המחזיקה. ביום 8.2.2020 יצרה הרשות קשר עם אלקטור באמצעות הבעלים ומנכ"ל אלקטור, מר צוריאל ימין, שהחלה - על פי הנחיות הרשות - לטפל בחולשות האבטחה שנתגלו במערכת.

3.2 מבדיקה שערכה הרשות ביום 9.2.2020 נמצא כי המידע מפנקס הבוחרים פורסם ברשת האפלה (Dark Web) (להלן: "**הרשת האפלה**"). מבדיקה נוספת שנערכה ביום 10.2.2020 נמצא כי המידע שפורסם ברשת האפלה עדכני ותואם למידע מתוך פנקס הבוחרים לכנסת ה-23.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

3.3 ביום 10.2.2020 ערכה הרשות פיקוח בחצרי אלקטור שכלל חיפוש מכוח צו חיפוש של בית משפט השלום בתל אביב-יפו, ואשר במהלכו התגלו ליקויי אבטחת מידע חמורים מאוד במערכות המידע של אלקטור ונתפסו חומרי מחשב שנמצאו על מחשביה.

3.4 מבדיקת הרשות עולה, כי הקובץ הנ"ל לא אותר כקובץ קיים ומוכן במערכת ובמחשבי אלקטור וכי על מנת לייצר את הקובץ, נדרשה גישה חופשית לבסיס הנתונים של אלקטור ושליפת המידע משם. המערכת אפשרה את יצוא המידע שבמערכת על ידי הפקת דו"חות לפי בקשת משתמש מכל אחת מהמפלגות, כאשר דו"חות אלה נגזרו ממאגר המידע המשמש את המפלגות. דו"חות אלה כללו מידע מפנקס הבוחרים בתוספת המידע אותו מזינים פעילי המפלגות כאמור. המערכת ייצאה את הדו"חות [redacted] שם נשמרו הדו"חות (להלן: "**הקונטיינר**"). מממצאי הפיקוח עלה, כי חולשת האבטחה החמורה אצל אלקטור אפשרה גישה גם לקונטיינר, ובכך חשפה גם את הדו"חות יחד עם כל תכולת הקונטיינר, אשר כללו מידע רגיש על אודות עשרות עד מאות אלפי בעלי זכות בחירה. אלקטור מחקה ביום 10.2.2020 את הקונטיינר על כל תכולתו.

3.5 בדיקות שנערכו במהלך הפיקוח במשרדי אלקטור העלו כי גם לאחר מחיקת הקונטיינר, ניתן היה עדיין לחדור למערכת המידע של אלקטור ולהגיע אל מידע אישי שמצוי בה. לאור זאת, הנחתה הרשות את אלקטור להפסיק לאלתר את השימוש באפליקציה עד לתיקון ליקויי האבטחה והשימוש במערכת הופסק ביום 10.2.2020.

3.6 ביום 11.2.2020 מסרה אלקטור עדכון לרשות ולפיו ממצאים קריטיים וממצאים בדרגות חומרה שונות שעלו במהלך הפיקוח במשרדי אלקטור טופלו, אולם ציינה כי טרם נבדקה המערכת והאפליקציה במבדקי חדירה על ידי גורם חיצוני כפי שנדרש. ביום 11.2.2020 הופעלה המערכת מחדש לצרכי מבדקי חדירות אשר בוצעו על ידי החברה הבודקת.

3.7 לאחר ביצוע מבדקי חדירות כאמור, בדיקות נוספות של הרשות הראו כי חולשות אבטחה עודן קיימות במערכת, ועל כן השימוש במערכת הופסק בשנית ביום 12.2.2020. רק לאחר שטיפלה אלקטור בליקויי האבטחה עליהם הצביעה הרשות, המערכת הועלתה שוב לאוויר ביום 13.2.2020.

4. ממצאי הפיקוח פורטו בהרחבה במכתב ההפרה לכאורה, והביאו למסקנות אשר פורטו גם הן במכתב ההפרה לכאורה, ביניהן הקביעה כי המידע אשר דלף ממערכות המידע של אלקטור נמצא עדכני ותואם למידע מתוך פנקס הבוחרים לכנסת ה-23.

5. נוסף על המידע מתוך פנקס הבוחרים על כל בעלי זכות הבחירה בישראל, כלל המידע שדלף קודים פנימיים אשר ניתנו על ידי אלקטור לכל אחת מהרשומות, ובכ-25,000 רשומות נמצאו גם מספרי טלפון.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

6. בנוסף, מידע שהחזיקה אלקטור ממאגר המפלגות ודו"חות אשר נוצרו במערכות המידע של אלקטור לצורך עיבוד מידע מפנקס הבוחרים, היו חשופים לתקיפה במערכת אלקטור. דו"חות אלה כללו, נוסף על המידע מפנקס הבוחרים, גם מידע אשר אספו המפלגות באמצעות האפליקציה, כגון מספרי טלפון של בעלי זכות בחירה, כתובות דוא"ל, מידע על אודות מצבו האישי הרפואי של אדם ומידע על היותו של בעל זכות בחירה "תומך" או "לא תומך" במפלגה ועוד.

7. לאור האמור לעיל, וכמפורט במכתב ההפרה לכאורה, קבעה הרשות כי פנקס הבוחרים, הן בפני עצמו והן בצירוף עם סוגים נוספים של מידע, הינו מאגר מידע כהגדרתו בחוק, כי המפלגות הינן בעלות המאגר וכי אלקטור הינה המחזיקה במאגר מטעם כל אחת מהמפלגות, כל זאת בהתאם להוראות החוק. אשר על כן, קבעה הרשות כמפורט במכתב ההפרה לכאורה כי אלקטור, כמחזיקה במאגר מטעם המפלגות, הפרה לכאורה את הוראות החוק ותקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: "**התקנות**"), כמפורט להלן:

7.1 אלקטור הפרה לכאורה את הוראות סעיף 17 לחוק אשר על פיו נקבע כי אלקטור כמחזיקה אחראית לאבטחת המידע במאגר. כמו כן, נקבע כי אלקטור הפרה לכאורה את הוראות תקנות 3, 4(א) עד4(ו), 5(א) עד 5(ה), 7(א) עד 7(ג), 8, 9, 10, 11, 13, 14, 16, 18(א) לתקנות.

7.2 בנוסף, נקבע במכתב ההפרה לכאורה כי אלקטור ביצעה לכאורה שבע הפרות לכאורה של הוראות סעיף 8(ב) לחוק, והפרה לכאורה את הוראות סעיפים 17א(א), 17א(ב) ו-17ב(א)(1) לחוק.

<u>מענה החברה למכתב ההפרה לכאורה</u>

8. ביום 11.11.2020 התקבל מכתב מענה מטעם החברה למכתב ההפרה לכאורה (להלן: "**המענה**"). הרשות נתנה לחברה באמצעות ב"כ החברה הזדמנות להשלים את טיעוניה ולקיים שימוע בעל פה והחברה הודיעה לרשות כי היא מוותרת על קיום השימוע.

9. כל טיעוני החברה, כפי שעלו מהמענה, נשקלו בידי הרשות. להלן יובאו עיקרי הטיעונים:

9.1 החברה טענה כי היא סיפקה את שירותיה למתמודדים לרשויות מוניציפליות, למתמודדים ללשכת עורכי הדין ולמפלגות שהתמודדו בבחירות לכנסת ה-21 וה-22 וכי באף מערכת בחירות קודמת לא התרחש אצלה אירוע אבטחה, וכי אירוע האבטחה שהתרחש במסגרת הבחירות לכנסת ה-23 המתואר במכתב ההפרה לכאורה הינו המקרה הראשון בו נפגעה החברה מאירוע כזה, וכי אירוע זה נגרם מטעות אנוש נקודתית, חד פעמית, ולא מליקוי בנהלים, מרשלנות או מזלזול והוא אינו משקף את רמת האבטחה ארוכת השנים של מערכת אלקטור.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

9.2 החברה טענה כי יש להימנע מלנקוט נגדה בהליכים מנהליים אלא להסתפק בפרסום הצעדים שעליה לנקוט בכדי לתקן את הליקויים שנמצאו בפעולותיה, כפי שנהגה הרשות בדו"ח פיקוח הרוחב בקרב מגזר חברות אחסון ועיבוד מאגרי מידע בישראל אשר פרסמה הרשות בחודש אוקטובר האחרון (להלן: "**דו"ח פיקוח הרוחב**").

9.3 החברה טענה כי הרשות עשתה שימוש לרעה במידע פרטי וסודי של החברה שנמסר לרשות במסגרת הפיקוח, ושאינו נוגע, לטענת החברה, לאירוע האבטחה, בכך שהרשות העבירה מידע זה למפלגות במסגרת מכתב ההפרה לכאורה שנשלח גם אליהן.

9.4 החברה טענה כי היא אינה נחשבת למחזיקה במאגר מאחר והמידע אינו מצוי בידיה דרך קבע והיא אינה רשאית לעשות בו שימוש ומעולם לא עשתה בו שימוש, ועל כן אין להתייחס אליה כאילו חלים עליה החובות החוקיות המתייחסות למחזיקי מאגר.

9.5 החברה טענה כי היא מאשרת באופן חלקי את קיומו של אירוע האבטחה שבכל מקרה לא הוביל לדליפת כל מסד הנתונים כפי שתואר במכתב ההפרה לכאורה, וכי הרשות לא הציגה ולו ראשית ראיה לכך שהקובץ שנמצא ברשת האפלה אכן דלף מהחברה. החברה טענה כי בדיקת הרשות העלתה כי לא קיים קובץ כאמור במחשבי החברה וכי הדבר מעיד על כך שמקור הדליפה אינו בחברה.

החברה טענה כי מסד הנתונים של החברה הכיל במועד אירוע האבטחה למעלה מ-100,000 מספרי טלפון, ועל כן טענת הרשות כי המידע שדלף כלל רק 25,000 מספרי טלפון מוכיחה כי אירוע הדלף לא התרחש ממערכת אלקטור.

החברה הכחישה את קביעת הרשות לפיה מערכת אלקטור שומרת מידע על מצב רפואי, וטענה כי קביעה זו של הרשות מעלה את החשש כי הרשות נסמכת על כתבות שפורסמו באמצעי התקשורת ללא כל סימוכין.

עוד טענה החברה, כי גם אם דלף מידע מהמערכת, הוא נעשה על ידי תוקף עם כוונת זדון שפעל מתוך אינטרסים מסוימים הנוגעים ככל הנראה ללקוחות החברה המשתתפים בהליך הפוליטי רווי האינטרסים.

9.6 החברה טענה כי משרד הפנים מוסר לבעלי המאגר – המפלגות המתמודדות בבחירות לכנסת – עותק של קובץ פנקס הבוחרים וכי רק בבחירות לכנסת ה-23 נמסרו לכ-30 מפלגות 60 עותקים של ספר הבוחרים. החברה טענה כי כל [redacted], וכי המעבר למדיניות הסיסמאות של אלקטור שדרג באופן דרמטי את מדיניות הסיסמאות המקורית שעמה הגיע פנקס הבוחרים.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

החברה ציטטה את דבריו של יו"ר ועדת הבחירות המרכזית, כב' השופט הנדל[1], הנוגעים בין היתר בצורך בשינויי חקיקה ובקביעת הסדרים חדשים הנוגעים לדיני הבחירות, הפרטיות, הטכנולוגיה וכיו"ב, ובקדמה הטכנולוגית המאפשרת למפלגות לעשות שימושים דיגיטליים מתקדמים בפנקס הבוחרים, וטענה בין היתר כי מערכת אלקטור ודומותיה הינן רק כלים טכנולוגיים בהם משתמשות המפלגות במטרה לשנע את תומכיהן אל הקלפיות.

בנוסף, טענה החברה כי הזכות לבחור ולהיבחר הינן זכויות יסוד חוקתיות בעלות מעמד על חוקי המהוות תנאי לקיומו של משטר דמוקרטי. עוד טענה החברה כי מטרות השימוש במערכת אלקטור הינן הגברת אחוז ההצבעה במערכת בחירות, שזוהי אחת ממטרותיה של כל מדינה דמוקרטית, ולצורכי התמודדות בבחירות או לצורכי קשר עם הבוחרים בהתאם לסעיף 39 לחוק הבחירות לכנסת.

החברה טענה כי במסגרת השירותים שהיא מספקת למפלגות היא מייתרת את הצורך שבשכפול פנקס הבוחרים [redacted],
וכך הופכת פעולת הביעור לפשוטה, מידית וסופית.

9.7 החברה הכחישה את מרבית הקביעות המועלות במכתב ההפרה לכאורה בכל הנוגע לאבטחת המידע במערכותיה. בהקשר זה מפרטת החברה בסעיפים 70 – 91 למענה את טענותיה, אשר נבחנו על ידי הרשות ועיקריהן מובאים כאן להלן:

9.7.1 החברה טענה כי הדו"חות אשר הופקו מהמערכת ונשמרו [redacted] לא כללו מידע מפנקס הבוחרים וכי אין כל תיעוד כי המידע מהדו"חות נחשף.

9.7.2 החברה טענה כי בזמן שדרשה הרשות מהחברה להפסיק את פעילות המערכת, טענו נציגי החברה כי אין סיבה לעשות זאת מלבד לפרסומים לא מבוססים בכלי התקשורת והחברה אף שלחה לרשות דו"ח של חברת אמאזון העולמית, המבהיר כי פרצות כמו אלה שתוארו בכלי התקשורת אינן אפשריות. למרות זאת, טענה החברה, הרשות דרשה להפסיק את השימוש במערכת כאמור ובכך הוסיפה לפגיעה הדרמטית, לדברי החברה, שכבר נגרמה לחברה ללא כל צורך.

9.7.3 החברה טענה כי סיפקה קבצי לוג רבים לרשות וזאת בניגוד לקביעת הרשות לפיה החברה לא המציאה לה קובץ לוגים מספק לתיעוד האירוע.

[1] **תב"כ 14/23 בן-מאיר ואח' נ' הליכוד – תנועה לאומית ליברלית ואח'** (18.02.20).

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

9.7.4 החברה טענה כי היא חוותה ניסיונות פריצה וחדירה רבים ([redacted] והצליחה להדוף את כולם ולעמוד בהם איתנה, דבר המלמד על חסינות המערכת ואבטחתה.

החברה טענה כי היא עונה על רוב דרישות התקנות וכי נראה שמצבה ביחס לחברות אחרות, לאור ממצאי דו"ח פיקוח הרוחב, טוב יותר משמעותית בכל הנוגע לאבטחת המידע והיא מפרטת בסעיף 14 למענה את הסיבות לכך.

החברה טענה כי בעולם התוכנה אין אפשרות לחסינות מלאה מאירועי אבטחה, ודאי לא כאלה שנובעים מטעויות אנוש. החברה מציינת כי זו אף הייתה עמדת הרשות כפי שנמסרה בתגובה לעתירה לבג"ץ 1311/20 אשר הוגשה נגד השימוש במערכת אלקטור. ולכן המדד הנכון לבחינת רמת האבטחה, לטענתה, הינו המהירות שבה מאותרת פרצת האבטחה ומנוטרלת, והחברה, לדבריה, נקטה בצעדים מהירים ומידיים לסגירת הפרצה תוך דקות ספורות מרגע גילויה.

החברה טענה כי היא הגיבה מהר לאירוע האבטחה, רעננה נהלים על מנת למנוע הישנות מקרים מעין אלו והוסיפה אמצעי אבטחה והגנה. עוד טענה החברה, כי אירוע האבטחה הביא תוקפים רבים, בייחוד ביום הבחירות לכנסת ובימים שקדמו לו, לנסות ולחדור למערכת אלקטור וכי ניסיונות אלה העלו חרס, מה שמלמד על חוסן אבטחתי גבוה של המערכת.

9.7.5 החברה טענה כי גם במסגרת הבדיקות שביצעו מערך הסייבר הלאומי וחברת אבטחת המידע הפרטית אותה שכרה אלקטור לצורך בדיקת האירוע (להלן וכאמור במכתב ההפרה לכאורה: "**החברה הבודקת**"), לא הצליחו לחדור אל מערכת אלקטור מבחוץ באופן שאיפשר הגעה לספר הבוחרים. לכן, טענה החברה, הגדרה כגון "בעיית אבטחה קשה/קריטית" בה השתמשו גורמים אלה, אינה מגובה בפעילות ממשית שהצליחה לסכן את המידע שבמערכת, להבדיל מבעיות בחוויית המשתמש, שחלקן תויגו במכתב ההפרה לכאורה כבעיות אבטחה.

בהתייחסה לאמור בסעיפים 6.15 – 6.16 למכתב ההפרה לכאורה, שם קבעה הרשות כי דו"ח החברה הבודקת היה חלקי בלבד ולא סיפק תמונה מלאה על אודות האירוע וכי הדו"ח גילה חולשות אבטחה במערכת החברה, טענה החברה כי בעולם אבטחת המידע ומערכות בדיקה תמיד ניתן יהיה למצוא אספקטים הניתנים לשיפור וכי מרגע אירוע האבטחה הראשוני לא נחשף מידע למרות ניסיונות רבים.

9.7.6 החברה טענה כי קביעת הרשות שלפיה [redacted] וכל לקוח יכול היה להיחשף למידע על לקוחות אחרים אינה מדויקת וכי זוהי אפשרות תיאורטית בלבד שלא הוכחה.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

9.7.7 החברה טענה כי על אף שלא הייתה מחויבת לכך, היא אפשרה לרשות הסייבר גישה למערכות הענן שלה ולא קיבלה עד לקבלת מכתב ההפרה לכאורה שום היזון חוזר, וזאת על אף בקשתו של ב"כ החברה בזמן אמת.

9.7.8 החברה טענה כנגד קביעת הרשות על כי מנגנון ההזדהות באפליקציה איננו מוודא את סוג הקלט כראוי [redacted] וכי חולשה זו אפשרה הרצת פקודות אשר יכולות היו לחשוף מידע הקיים בבסיס הנתונים של החברה או לבצע מתקפות אחרות. החברה טענה כי [redacted] ועל כן, משתמע מכך כי לא מדובר בחולשה כפי שקבעה הרשות, וכי גם אם לא כך היה הדבר, לא ברור כיצד טענה זו עלולה לפגוע במידע.

9.7.9 החברה טענה כי בניגוד לקביעת הרשות, לחברה הייתה ויש מערכת WAF.

החברה טענה כי בניגוד לקביעת הרשות, כאשר ישנם מספר ניסיונות התחברות שגויים, קיימים במערכת החברה מנגנוני אבטחה החוסמים משתמשים ברמת אפליקטיבית וברמת ה-WAF. [redacted]

בהתייחסה לקביעת הרשות שלפיה לא בוצע סינון כתובות IP לצורך התרעה על פעילות חריגה, טענה החברה כי היו חסימות אוטומטיות הן ברמת WAF, והן ברמה אפליקטיבית, בעת זיהוי דפוסי פעולה בעייתיים.

9.7.10 החברה הכחישה את קביעת הרשות לפיה לא יושם מנגנון למניעת ניסיון פריצת סיסמאות או ניחושן וכי למערכת החברה ולמנהליה לא היו היכולות לגלות ולחסום מתקפות על המערכת וזאת מאחר ולא נמצאו מנגנון ניטור, בקרה והתרעה על ניסיונות מסוג זה. החברה טענה כי די היה בהקשת מספר סיסמאות שגויות כדי שהמערכת תחסום את המשתמש וכי ראיה לכך היא שבמקרים רבים משתמשים לגיטימיים נחסמו עקב רגישות המערכת וכי יעידו על כך עובדי המטה הלגיטימיים שנחסמו לעיתים קרובות במפלגות השונות.

9.7.11 החברה טענה כי לא ברורה קביעת הרשות שלפיה נעשה על ידי החברה שימוש בפורטים פתוחים אשר החברה לא סיפקה הסבר לגבי הצורך בהם. החברה טענה כי מעולם לא הועלתה דרישה מהרשות לספק הסברים על פורטים אלה וכי ערוצי תקשורת אלו נפוצים מאד למנהלי מערכת לצורך גישה לשרתיהם.

9.7.12 החברה אישרה את קביעת הרשות שלפיה בקשות API היו חשופות במערכת אולם היא מכחישה כי לא הייתה דרישה להזדהות וטענה כי על מנת להשתמש בכל אחת מבקשות אלה נדרשה הזדהות.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

9.7.13 בהתייחסה לקביעת הרשות כי נחשף מידע רגיש ב- [redacted], טענה החברה כי ככל הידוע לה, מידע רגיש לא הועבר באמצעי זה.

9.7.14 בהתייחסה לקביעת הרשות שלפיה מדיניות הסיסמאות של החברה נמצאה כחלשה ולא מאובטחת באמצעי פיזי נוסף, טענה החברה כי המערכת אפשרה לכל לקוח לבחור עבור משתמשיו את הסיסמאות וכי היא לא אכפה מדיניות סיסמאות למשתמשיו נמוכי ההיררכיה של כל לקוח, אולם המשתמשים הגבוהים בהיררכיה קיבלו סיסמאות חזקות וכי מדיניות הסיסמאות הוקשחה במהלך הקמפיין גם למשתמשים נמוכי היררכיה.

9.7.15 בהתייחסה לקביעת הרשות שלפיה החברה פעלה תחת הרשאות "משתמש על" לכלל ההתקשרויות והשירותים במערכת, אשר אפשרו גישה לתוקף שהשיגן, למידע ולשירותים השונים במערכת, טענה החברה כי שימוש ב-"משתמש על" אינו פעולה בלתי חוקית או בעייתית, כי יש Best Practice וכי אין עניין הרשות בזוטות שכאלו.

9.7.16 החברה הכחישה את קביעת הרשות שלפיה מערך מחשבי החברה במשרדיה לא היה מאובטח וטענה כי הרשת הפנימית כללה סיסמאות לכל המחשבים, Firewall פעיל של ווינדוס וסיסמה מורכבת ל-WiFi.

9.7.17 החברה הכחישה את קביעת הרשות שלפיה החברה לא ביצעה בדיקת חוסן לתשתיות המשמשות את האפליקציה וכי ביצעה סקרי סיכונים פנימיים חדשות לבקרים, ולראיה חוסנה עד מקרה זה של אירוע האבטחה וכי היא התייעצה בעניין עם מומחה אבטחת מידע.

9.7.18 החברה הכחישה את קביעת הרשות שלפיה לא ביצעה החברה עד למועד האירוע כל בדיקה מקצועית בלתי תלויה לרמת הקוד שנכתב על ידה וטענה כי בוצעו בדיקות פנימיות לאורך כל הדרך וכי תהליך הפיתוח בחברה חייב "סקירת קוד" על ידי עוד זוג עיניים אחד לפחות.

9.7.19 בהתייחסה לקביעת הרשות שלפיה החברה לא בדקה [redacted] האם יכול לקוח אחד להיחשף למידע על לקוחות אחרים, טענה החברה כי קביעה זו של הרשות אינה נכונה וכי החברה ביצעה ומבצעת בדיקות רבות וכי בכל מקרה אין שום תיעוד לטענתה זו של הרשות.

9.8 החברה הכחישה באופן מלא את קביעות הרשות במכתב ההפרה לכאורה, לפיהן, המערכת אפשרה לגורמים לא מורשים לגשת למידע. בהקשר הזה מפרטת החברה בסעיפים 40 – 48 למענה את מדיניות ההרשאות שלה, ועיקריהן מובאים כאן להלן:

9.8.1 החברה טענה כי מערכת אלקטור [redacted] מייתרת את הצורך בשכפול פנקסי הבוחרים, ומנגישה אותו למורשים בלבד. בכך, טענה החברה, גם פעולת הביעור הופכת לפשוטה, מידית וסופית.

קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL
PPA@justice.gov.il | 02-6467064 | 073-3928555

מחלקת אכיפה

9.8.2 החברה הכחישה את קביעת הרשות שלפיה המערכת אפשרה לגורמים לא מורשים לגשת למידע.

9.8.3 החברה טענה כי למערכת אלקטור יש מערכת הרשאות נוקשה: האפשרות לבצע חיפושים חופשיים במידע ניתנת רק למשתמש אחד, [redacted] יתר המשתמשים מוגבלים לעד 50 חיפושים.

9.8.4 החברה טענה כי היא מוסרת לכל לקוח משתמש אחד בלבד, הגבוה ביותר בהיררכיה, וכי פתיחת משתמשים נוספים בדרגות נמוכות יותר בהיררכיה אינה מתבצעת על ידי החברה אלא באופן ידני על ידי הלקוח.

9.8.5 החברה טענה כי לצורך קבלת גישה למערכת יש לבקש הרשאה מסודרת מהמשתמש הראשי, במקרה זה המפלגות, למסור מספר טלפון סלולרי ממנו ניתן ליצור משתמש אחד בלבד ואליו יישלח מסרון להפעלת המשתמש, ולאשר את תנאי השימוש של המערכת הכוללים פסקה על התחייבות לחוק הגנת הפרטיות.

9.8.6 החברה טענה כי משתמש במערכת יכול לבצע כאמור מספר מוגבל של חיפושים, באמצעות שם מלא או מספר תעודת זהות ולקבל בתוצאת החיפוש מידע חלקי ללא תעודת זהות. כמו כן, טענה החברה כי למשתמש זה אין אפשרות לייצא מידע לדו"חות מודפסים.

9.8.7 החברה טענה כי מלבד הקמת המידע הראשונית המערכת, היא אינה עוסקת בטיוב הנתונים וכי ככל שמתבצעות פעולות טיוב, הן מבוצעות על ידי הלקוח ובאמצעות המשתמשים שהלקוח פתח במערכת.

9.8.8 החברה טענה כי המידע, יחד עם כל מסד הנתונים, מבוער בסיום מערכת הבחירות.

9.9 החברה טענה כי היא ביערה את הרוב המוחלט של קבצי הלקוחות שהיו ברשותה, וכי אי ביעור הקבצים שמצאה הרשות על מחשבי החברה אינו מעיד על דפוס אלא על טעות אנוש. עוד טענה החברה כי הקבצים שלא בוערו נשכחו בתתי תיקיות על גבי המחשבים בלבד וכי הם נמחקו מהשרת בעת סיום הבחירות הרלוונטיות אליהם.

בנוגע לקביעה כי נמצאו במחשבי החברה שלושה עותקים של הנגזרת הראשונה של פנקס הבוחרים לכנסת ה-23, טענה החברה כי היא לא הצהירה על ביעור ולא הכירה כי יש לבער את הנגזרות טרם הבחירות עד לאישור המפלגות.

9.10 בנוגע לפעולות המתקנות אשר נדרשה החברה במכתב ההפרה לכאורה לבצע, טענה החברה כי היא נקטה בפעולות שונות ומגוונות בהמשך לשיפור אבטחת המידע, אף אם אלה שונות מההנחיות אותן הנחתה אותה הרשות לבצע, בשל הבדלי סגנונות בצורת הפיתוח.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

9.11 החברה טענה כי היא מינתה ממונה אבטחת מידע וכי היא הסדירה זאת בהסכם כתוב בין מייסדי החברה, וכי ממונה אבטחת מידע אמון על נושאי אבטחת המידע בחברה.

10 <u>קביעת הרשות וסיכום ממצאי הפיקוח</u>

10.1 הרשות קובעת כי העובדות שפורטו במכתב ההפרה לכאורה מלמדות שבמאגר המידע שאלקטור החזיקה עבור המפלגות, לא קוימו כל החובות הדרושות על פי דין ושאלקטור לא מילאה אחר כל החובות המוטלות עליה על פי דין, כמפורט להלן:

10.2 לעניין הטענה כי אירוע האבטחה מושא הליך זה הינו המקרה הראשון בו התרחש אירוע כזה מסוגו בחברה, ומבלי להתייחס לאמיתות הטענה, יצוין כי אין בכך כדי לגרוע מחומרת האירוע ומהשלכותיו או מאחריותה של החברה, כפי שפורט במכתב ההפרה לכאורה.

10.3 לעניין התייחסותה של החברה לדו"ח פיקוח הרוחב, יצוין כי הליך האכיפה הרוחבי בקרב מגזר חברות אחסון ועיבוד מאגרי מידע בישראל היה הליך יזום ורוחבי בו נקטה הרשות, אשר נועד לבחון את רמת עמידתן של חברות האחסון בהוראות החוק והתקנות, להעלות את המודעות להוראות החוק בקרב חברות האחסון וליתן להם כלים לשפרן, מבלי שיהיה בכך לגרוע מסמכות הרשות לפתוח ולנהל הליכי פיקוח ספציפיים נגד מי מהחברות שנסקרו, במקרים שיחייבו זאת. זאת בשונה מהליך פיקוח זה, אשר מתנהל כנגד החברה בעקבות אירוע אבטחה חמור, שאירע עקב אי-עמידת החברה בהוראות החוק, והוא אינו קשור להליך פיקוח הרוחב וממצאיו.

10.4 **הרשות דוחה את טענת החברה לפיה המידע שנכלל בהפרה לכאורה לא היה צריך להיות מועבר למפלגות.** המפלגות, כבעלות המאגר, נדרשות לפי תקנה 15 לתקנות להכיר ולבדוק לעומק את מערך אבטחת המידע שננקט על ידי החברה, ובמסגרת מכתב ההפרה לכאורה המופנה אליהן, זכאיות להכיר את כל הראיות המצביעות לכאורה על ההפרות שבוצעו, ושהאחריות להן מונחת כאמור גם לפתחן, זאת כדי שיוכלו לטעון כנגד ראיות אלה. ליקויי האבטחה שנמצאו בפעילותה של החברה ובמערכת אלקטור, והראיות ביחס אליהם, אינם מתקיימים רק במישור היחסים שבין הרשות לחברה בלבד, אלא גם במישור הליך הפיקוח הננקט אל מול המפלגות, כבעלות המאגר. אשר על כן, לא רק שלא נפל כל פגם בהעברת הממצאים הנוגעים לרמת האבטחה ו/או לממצאי הבדיקות שבוצעו ביחס לאפליקציה למפלגות כבעלות המאגר, אלא שהרשות מחוייבת להעבירם במסגרת כללי המינהל התקין.

PPA@justice.gov.il | 02-6467064 | 073-3928555
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

10.5 **הרשות דוחה את טענת החברה לפיה היא אינה "מחזיק".** יובהר, כי כאשר גורם כלשהו מחזיק או מנהל אוסף של נתוני מידע שמתקיימת בו הגדרת "מאגר מידע" בחוק - הרי שתחול עליו אחריות של בעל מאגר או של מחזיק במאגר. לפי הוראות החוק לא יתכן מצב בו גורם כאמור אינו חב כלל באחריות ביחס למאגר המידע. לפי מכלול הנסיבות הרלוונטיות למאגר המידע נושא מכתב ההפרה לכאורה, יש לראות בחברה כ"מחזיקה במאגר מידע" ביחס למאגרי המפלגות אשר כללו את נגזרות פנקס הבוחרים שנמסרו לה על ידי המפלגות[2].

הרשות קבעה כי ספקי שירות חיצוני, כגון אלקטור, הם "מחזיק" כהגדרתו בחוק, אף אם משך מתן השירות מוגבל לתקופת הבחירות או אף לפרק זמן קצר יותר.

בפועל, פנקס הבוחרים היה מצוי ברשות המפלגות וברשות אלקטור מטעמן לתקופת הבחירות אשר נמשכה מספר חודשים, במסגרתה אלקטור הייתה רשאית ואף ביצעה בו את השימושים אותם ביקשו המפלגות. אשר על כן, יש לראות באלקטור "מחזיק" במאגר המידע מטעם המפלגות, דרך קבע, שכן לא מדובר בגישה אקראית או חד-פעמית למידע, אלא לתקופה מתמשכת כאמור.

אשר על כן, החברה אחראית על כשלי אבטחת המידע אשר אותרו אצלה, כמפורט בסעיפים 8 ו-10 למכתב ההפרה לכאורה, בהיותה מחזיקה במאגר מטעם המפלגות, ובכך נכנסה בגדר דרישות סעיף 17 לחוק אשר קובע כי בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר.

10.6 **הרשות דוחה את טענות החברה כי לא דלף מידע מהמאגרים שהחזיקה.** ממצאי הרשות קובעים באופן מלא וברור כי מקורו של הקובץ שדלף אל הרשת, הינו במערכותיה של החברה. כמפורט במכתב ההפרה לכאורה, הקובץ אשר נמצא ברשת האינטרנט כלל בין היתר קוד מזהה פנימי וחד-חד ערכי שנוצר על ידי החברה עבור כל רשומה במאגר לקוחות החברה בעת העלאת המידע למערכותיה (להלן: "**הקוד הפנימי**"). במהלך הפיקוח במקום, ביצעו חוקרי הרשות השוואה של הקוד הפנימי ביחס למספר רשומות אשר דלפו לרשת, אל מול הקוד הפנימי ברשומות המקבילות במאגר מפלגת הליכוד במערכות אלקטור, ונמצאה התאמה מוחלטת בין הקודים הפנימיים במערכות החברה עבור מאגר מפלגת הליכוד, לבין אלה שנמצאו במידע שדלף. יצוין כי הקוד הפנימי לכל רשומה, אשר נוצר במסגרת תהליכים אותה מבצעת החברה בעת הכללתם של רשומות חדשות בבסיס הנתונים שלה, הינו קוד ייחודי וחדש לכל רשומה ורשומה [redacted], כך שגם כשיוכנסו שני פנקסי בוחרים זהים (עבור שני הלקוחות של החברה) לבסיס הנתונים שבמערכת החברה, שתי הרשומות של אותו בוחר תקבלנה כל אחת קוד פנימי ייחודי ושונה בכל אחד מהמאגרים השונים בהם מחזיקה החברה.

---

[2] הרשות להגנת הפרטיות, "ריענון הוראות חוק הגנת הפרטיות בעניין מגבלות השימוש במידע מפנקס הבוחרים ומגבלות השימוש במידע אישי", 02.02.2020; הרשות להגנת הפרטיות, "קווים מנחים בעניין שימוש באפליקציות ובספקים חיצוניים לצורך ניהול מערכת בחירות", 11.02.2020; הרשות להגנת הפרטיות, "ריכוז דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה-24: מגבלות השימוש בפנקס הבוחרים ובמידע אישי אחר ואחריות המפלגות על אפליקציות וספקים חיצוניים", 03.01.2021;

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

בהתייחס לטענת החברה שהמידע שדלף הכיל רק 25,000 מספרי טלפון מתוך 100,000 שהיו במסד הנתונים של החברה, תציין הרשות כי מעבר לעובדה שהמידע כלל כאמור רשומות עם קוד פנימי ייחודי למאגר החברה, הרי שאין בכך כדי לבסס את טענת המפלגה כי לא מדובר באותו מאגר, אלא בכך שהתוקף בחר שלא להוריד את כלל המידע ממערכות החברה, על אף שהייתה לו היכולת לברור את המידע שברצונו לדלות מתוך מסד הנתונים. כאמור ועל פי הממצאים התוקף בחר לדלות מידע המזוהה בקוד פנימי המשמש את מפלגת הליכוד, דבר אשר משקף את יכולתו של התוקף לגשת באופן מלא לבסיס הנתונים ואת חומרת האירוע.

בהתייחס לטענת החברה שהמידע לא כלל מידע רפואי, יצוין כי המידע שהתווסף על ידי משתמשי האפליקציה למאגרים שהוחזקו על ידי החברה, כלל בין היתר גם מידע רגיש על אודות בוחרים, במסגרתו הוזן גם מידע רפואי על אודות צדדים שלישיים אשר עשויים להיות מעוניינים מסיבות שונות בהסעה אל הקלפי, ובין היתר בגלל מגבלות רפואיות.

באשר למידע המטוייב, פרסמה הרשות הנחיות בדבר האיסור שחל על שימוש במידע אישי במקרים בהם לא ניתנה לגביו הסכמה תקפה ומספקת של האדם עליו המידע נאסף, או מבלי שהוסברו לו מטרות השימושים ולמי המידע יימסר. איסור זה חל גם על איסוף ושימוש במידע ביישומים או במאגרי המידע של המפלגות.

בהתייחס לטענת החברה בדבר כוונת הזדון והאינטרסים של התוקף, הרי שאלה אינם רלוונטיים לאחריות החברה לאבטחת המידע אותו היא מחזיקה.

10.7 ביחס לטענת החברה באשר לאופן הנגשת הפנקס, הרשות אמנם הבהירה את עמדתה בדבר הסיכונים הקיימים בפרקטיקה הקיימת להעברת פנקס הבוחרים למפלגות או למי מטעמן, והיא פועלת באופן שוטף ומזה שנים רבות לשם קידומם של הסדרים חדשים אשר יאפשרו רמת אבטחת מידע גבוהה יותר למידע הפנקס. אולם, כל עוד לא נקבעו הסדרים חדשים כאלה, קל וחומר שחלים לפחות דיני הפרטיות הקיימים על ניהול מאגרי המידע, לרבות פנקס הבוחרים, אגב מערכת הבחירות ולצורך התמודדות בה.

למעלה מן הצורך יוזכר כי יו"ר ועדת הבחירות המרכזית, כב' השופט הנדל, קבע כי "המחוקק קבע גורם המוסמך לדון בסוגיית הפרטיות של היחיד, גם בשדה הבחירות, והוא הרשות להגנת הפרטיות. כולי תקווה כי הרשות תמצה את הליכי הבדיקה והפיקוח, ביעילות וביסודיות הנדרשת בסד הזמנים של מערכת הבחירות ועל הצד הטוב ביותר".[3]

חוק הגנת הפרטיות והתקנות שמכוחו חלים במלואם על מאגרי המידע שמנהלות המפלגות ועל אלה שהן מוסרות לספקי שירות חיצוני לצורך עיבוד, טיוב או אחסון, גם בכל הנוגע לעותק פנקס הבוחרים הנמסר לידיהן, וכך גם הבהירה הרשות, במסמכים שפורסמו על ידה פעמים רבות.

---

[3] **תב"כ 14/23 בן-מאיר ואח' נ' הליכוד – תנועה לאומית ליברלית ואח'** (18.02.20).

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

אין חולק בדבר חשיבותן ומעמדן של הזכות לבחור ולהיבחר וכן בחשיבות רצון המפלגות להעלות את אחוזי ההצבעה במערכת הבחירות. הרשות גם ערה לצורך בעיבוד מידע ולשימושים הלגיטימיים בו למטרת קידום אינטרסים חשובים אלה. עם זאת, העובדה שבשנים האחרונות הערכות המפלגות לבחירות, ושמירת הקשר עם הבוחר מתקיימות בעיקר באמצעות אמצעים דיגיטליים ומדיה חברתית, גרמה ליצירת סיכונים רבים וחמורים שלא התקיימו בעבר ובדיוק בשל כך ולאור דרכי ההתקשרות הנרחבים יותר עם הבוחר בעידן הנוכחי, הוראות הדין קובעות שכל מי שמקבל לידיו את פנקס הבוחרים לצורך התמודדות בבחירות ויצירת קשר עם הבוחר, נדרש לגלות זהירות יתרה בכל הנוגע לשימוש בו ולעמוד באופן מלא בהוראות החוק והתקנות.

10.8 **הרשות דוחה את טענות החברה כי לא היו כשלי אבטחת מידע במערכותיה ולחילופין כי לא הייתה אחראית לכשלי אבטחת המידע שאותרו אצלה.**

הרשות קובעת כי גם אם לא ניתן להבטיח כי העולם הרשתי יהיה חסין לחלוטין מפני אירועים של דליפת מידע או פריצה בלתי מורשית למערכות, הרי שעל פי הוראות החוק - בעל מאגר ומחזיק מטעמו נדרשים לנקוט באמצעים מקובלים להגנה מקסימלית על המידע, וכפי שפורט בסע' 7 למכתב ההפרה לכאורה, ממצאי הפיקוח העלו כי החברה לא נקטה באמצעים מספיקים לאבטחת המידע טרם התרחשותו של אירוע האבטחה, דבר אשר אפשר את התרחשותו.

יצוין כי במסגרת ממצאי הבדיקות שנערכו בשיתוף עם מערך הסייבר, וכפי שעלה מדו"ח החברה הבודקת, נתגלו ליקויים וכשלים אשר אפשרו גישה למערכות החברה וחשפו את המידע שבהן.

בנוסף, ממצאי הפיקוח העלו, כמפורט במכתב ההפרה לכאורה, כי גם לאחר האירוע הראשוני, ולאחר שהחברה העלתה את המערכת לאוויר בהנחיית הרשות, עדיין זוהו ליקויים באבטחת המידע במערכות החברה אשר אפשרו את חשיפתו, כמפורט להלן:

- הרשות דוחה את טענת החברה על כי הדו"חות בקונטיינר הנפרד לא כללו מידע פנקס. כפי שפורט במכתב ההפרה לכאורה, הקונטיינר הלוגי הנפרד הכיל דו"חות אשר נגזרו באמצעות מערכת אלקטור ממסד הנתונים של החברה, דו"חות אלו כללו מידע מפנקס הבוחרים וכחלק מאירוע האבטחה היו חשופים לתוקף ולכל משתמש בעל סיסמא של פעיל ליכוד באפליקציה אשר יכול היה להגיע לתכולת הקונטיינר. לוגים שהופקו מהמערכת מוכיחים גישה והורדה של דו"חות מהקונטיינר בהיקפים של מאות אלפי רשומות, כפי שציין מנכ"ל החברה במהלך הפיקוח.

- בהתייחס לטענת החברה בדבר ההנחיה להפסקת פעילות המערכת, יצוין כי, בזמן הפיקוח במשרדי החברה ומבדיקות שבוצעו, נוכחו חוקרי הרשות כי מערכות החברה היו חשופות לתקיפות והמידע שבהן לא היה מוגן כלל. פעולות החברה לא יצרו הגנה מספקת במניעת חשיפת המידע לתקיפה, ועל כן דרשה הרשות במסגרת סמכויותיה, להפסיק את פעילות המערכת עד לתיקון הליקויים שגרמו לחשיפת המידע.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

הרשות התירה לחברה להפעיל מחדש את המערכת לצורך ביצוע מבדקי חדירות על ידי החברה החיצונית הבודקת, אולם לאחר ביצוע המבדקים כאמור, בדיקות נוספות של הרשות הראו כי חולשות אבטחה עודן קיימות במערכת, ועל כן השימוש במערכת הופסק בשנית. רק לאחר שטיפלה החברה בליקויי האבטחה עליהם הצביעה הרשות, אושרה העלאת המערכת שוב לאוויר. כפי שפורט בהרחבה במכתב ההפרה לכאורה, חולשות האבטחה אשר התגלו הן בדו"ח החברה הבודקת והן מבדיקות הרשות ומערך הסייבר, היו אלו אשר אפשרו במקור גישה למידע שבמערכות החברה וסיכנו אותו.

- בהתייחס לטענת החברה בדבר המצאת קובץ לוגים מספק, תציין הרשות כי נכון להיום ולמרות דרישותיה, טרם התקבל מהחברה קובץ לוגים המתעד את כל אשר התרחש במסגרת אירוע האבטחה. במהלך הפיקוח במשרדי החברה טענה החברה בפני נציגי הרשות כי היא מחקה את הקונטיינר הלוגי הנפרד אשר כלל גם קבצי לוג, וכך לא נשמר גם התיעוד המוגדר כברירת המחדל. מבדיקה מול יחידת אבטחת המידע באמזון אשר בוצעה במהלך אירוע האבטחה עלה כי לא הוגדרו הגדרות אבטחה לניטור ולתיעוד בניגוד להנחיות של אמזון. הניטור והתיעוד הוגדרו בהגדרות ברירת מחדל ולא על פי ה-Best Practice של אמזון. על כן, הלוגים החלקיים אשר הועברו לבקשת הרשות לא אפשרו ביצוע חקירה והתחקות שלמים אחר מהלכי התוקף.

- דו"ח החברה הבודקת אותו העבירה החברה במסגרת הליך הפיקוח, כפי שנקבע במכתב ההפרה לכאורה, היה חלקי בלבד ולא סיפק תמונה מלאה על אודות אירוע האבטחה. המבדק ואיכותו נקבעים על פי קריטריונים מקצועיים מקובלים, ביניהם הבנת איום הייחוס, המערכות הנבדקות, מבנה הבדיקה והיקפה, סוג הבדיקה (אפליקטיבי\תשתיתי), מתודולוגיית הבדיקה, פירוט הכלים בהם נעשה שימוש לביצוע הבדיקה, ציון הרכיבים שנבחנו, פירוט הממצאים, המלצות לסילוק איומים בהתאם לממצאים וכיו"ב. דו"ח החברה הבודקת אשר הועבר לרשות כלל מידע על ליקויים רבים אשר אותרו במערכות החברה, אולם מידע זה היה חלקי בלבד שלא על פי הקריטריונים המקובלים ועל כן הוא לא שיקף כלל בדיקה מקיפה ומקצועית כנדרש באירועים מהסוג של אירוע האבטחה.

- [redacted] יכול היה להיחשף למידע על לקוחות אחרים. בהקשר הזה יצוין כי השימוש בהרשאות [redacted] לאורך כל השדרה האפליקטיבית מתחילתה ועד סופה איפשר בפועל גישה לכלל הרכיבים האפליקטיביים, כמו גם למידע בבסיס הנתונים.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

- בהתייחס לטענת החברה כי עד לקבלת מכתב ההפרה לכאורה לידיה היא לא קיבלה היזון חוזר בהתאם לתוצאות הבדיקה שהיא אפשרה לרשות הסייבר לבצע במערכות הענן שלה, תציין הרשות כי הליך הפיקוח מתחילתו ועד לשלב הזה, כלל פירוט מלא של כל אחד מהממצאים שעלו ממנו אשר הובאו בפני החברה מהר ככל הניתן, וזאת בעיקר לצורך עצירת דלף המידע ומניעת הישנות אירוע האבטחה, הן באמצעות הנחיות לתיקון ליקויים אשר ניתנו לחברה כבר ביומו הראשון של הפיקוח ובימים שאחריו, והן באמצעות מכתב ההפרה לכאורה.

  אשר על כן, ובנסיבות בהן הביאה הרשות לידיעת החברה, בכל אחד מהשלבים של הפיקוח את חומרת האירוע ואת שנדרש ממנה לעשות כדי לתקן את הליקויים ולמנוע הישנות האירוע, ובמסגרת מגבלות העברת המידע למפוקח מתיק אכיפה מתנהל, יש לדחות טענה זו.

- החברה טענה כי מנגנון ההזדהות באפליקציה מאפשר התחברות גם באמצעות כתובת דוא"ל [redacted], וכי בניגוד לקביעת הרשות לא מדובר בחולשת אבטחת מידע. עוד טענה החברה, כי גם אם כך היה הדבר, לא ברור לחברה כיצד מידע יכול היה להיפגע מכך. בהתייחס לטענתה זו של החברה, ובהמשך לאמור במכתב ההפרה לכאורה, הרשות תציין כי מנגנון ההזדהות בו נעשה שימוש באפליקציה לא פותח על פי מתודת פיתוח מאובטח מקובלת, [redacted] המאפשרות חדירה למאגר הנתונים, חשיפת המידע שבו ושליפתו על ידי גורמים לא מורשים.

- באשר לטענות החברה בקשר לרכיב אבטחה WAF, קיומו של רכיב זה אינו מעיד בהכרח על קיומה של הגנה או על איכותה. לשם אבטחת המידע, נדרשת בנוסף לקיומו, גם הגדרת חוקים וטיובם השוטף, ניטור וכן תיעוד והתרעה במקרה של התנהגות זדונית. כל אלה לא בוצעו כנדרש על ידי החברה [redacted]

- [redacted]. כמו כן, רכיב ה-WAF לא הוגדר לחסום גישה בהתאם לנתונים גאוגרפיים וכך יכול היה התוקף להשתמש בכתובת בחו"ל לצורך החדירה למערכות החברה.

- קיומם של [redacted] שירותים פעילים שאינם נדרשים לפעילות החברה מעיד על כך שלא בוצעה כל הקשחה למערכת וכי עצם השארתם פתוחים היוותה פרצה המאפשרת לתוקף לחדור דרכה למערכות החברה.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

[redacted]בהתייחס לטענת החברה כי לא הועבר מידע רגיש ב[redacted], תציין הרשות את הדברים כפי שהובאו בדו"ח החברה הבודקת: [redacted]

במהלך הבדיקה שנעשתה נמצא כי לאחר ביצוע ההתחברות למערכת, צד הלקוח מבצע פניה לשרת עם מידע רגיש [redacted]. המידע כולל את [redacted] המזהה הייחודי של הלקוח אל מול השרת ואת מזהה המשתמש באפליקציה והרשאותיו. [redacted] חשיפה זו מאפשרת לתוקף בעל גישה לכל אחד מהמקורות שהוזכרו להיחשף למידע רגיש אודות משתמשי המערכת ולבצע מגוון פעולות זדוניות כגון הונאה וגניבת זהות."

- החולשות אשר אותרו במערכות החברה במהלך הפיקוח לא נבחנו טרם התרחשות אירוע האבטחה במסגרת מבדקי חדירות מקצועיים חיצוניים, בדיקות חוסן לתשתיות ובדיקות מקצועיות ובלתי תלויות לרמת הקוד שנכתב על ידה. ולכן חולשות אלה מעולם לא הוצפו ולא תוקנו בהתאם, דבר אשר אפשר לתוקף לחדור למערכות החברה ולעשות שימוש במידע שבבסיס הנתונים שלה. בהקשר הזה יצוין כי לא הומצאה לרשות כל אסמכתה לביצוע מבדקים כאמור. בדיקות וסקרי סיכונים פנימיים אשר החברה טענה שביצעה, ככל שאכן בוצעו, לא הציפו את הליקויים שנמצאו ואשר על כן לא תוקנו. יוזכר, כי סקרי סיכונים פנימיים, גם אם נבחנים בזוג עיניים נוסף כדברי החברה, אינם מהווים תחליף למבדקים מקצועיים המבוצעים על פי שיטות ואמצעים מקובלים ובידי בעל מקצוע מיומן ושזהו תחום התמחותו.

10.9 **הרשות דוחה את טענות החברה לפיה המערכת לא אפשרה לגורמים לא מורשים לגשת למידע.** כפי שפורט במכתב ההפרה לכאורה, מנגנון ניהול ההרשאות של מערכת אלקטור יושם בדרך לקויה אשר אפשרה גישה לא מורשית לכל המידע אשר היה מצוי בבסיס הנתונים של אלקטור וכלל בין היתר גם את המידע מפנקס הבוחרים, כמפורט להלן:

- שימוש ב"משתמש על" נוגד כל תפיסה באבטחת מידע. ברגע שתוקף מצליח לשים ידו על הרשאה מסוג זה, הוא יכול לעשות במערכת כבשלו. על החברה היה להשתמש בהרשאות משתמש מינימליות המאפשרות את ביצוע הפעולות הנדרשות וכמו כן, ליצור משתמשים שונים בעלי סיסמה מוקשחת והרשאות מינימום לכל שירות.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

- באשר לטענת החברה כי היא מוסרת משתמש אחד בלבד לכל לקוח, [redacted] אשר מאפשר ללקוח פתיחת משתמשים נוספים [redacted], קובעת הרשות כי העובדה שהחברה מטילה את האחריות על הלקוח, אינה פוטרת אותה מהאחריות לוודא כי מדיניות ההרשאות שלה וזו שהיא מאפשרת ללקוח במערכותיה, עומדת בדרישת החוק והתקנות.

יתר על כן, העובדה שפונקציית רשימת המשתמשים במערכת [redacted] היתה חשופה [redacted], ואפשרה בפועל השגה קלה של פרטי ההתחברות של כל משתמשי [redacted] וללא צורך בהזדהות כלל, אפשרה לכל מי שהשיג פרטים אלה להיכנס למערכת ולעשות במידע הכלול בה כבשלו.

- בהתייחס לטענת החברה שלפיה הרשת הפנימית כללה סיסמאות לכל המחשבים, Firewall פעיל של ווינדוס וסיסמה מורכבת ל-WiFi, תציין הרשות כי הרשת הפנימית של החברה אכן כללה סיסמאות לכל המחשבים, Firewall פעיל של ווינדוס וסיסמה ל- WIFI. ואולם, אלו הם רכיבי ברירת מחדל של מחשבי קצה אשר כבר קיימים במערכת ההפעלה, וניהול סיסמאות סטנדרטי ברמת אבטחה ביתית המאפשרת חשיפת הרשת למתקפות. הגנות אלה יושמו ברמת משתמש פרטי ועל מחשבי קצה בלבד. לא נמצאה הגנה רוחבית כלשהי מקובלת ומתאימה לאבטחת מידע בארגונים, עליהם נמנית החברה, המחזיקים במידע רב, בחלקו אישי ורגיש, ומנגישים אותו ללקוחותיהם באמצעים דיגיטליים.

- פעולות לחשיפת שמות משתמשים ולניחוש סיסמאות יכולות להימשך פרקי זמן ארוכים ובהפרשי זמן גדולים ומאפשרים לעקוף הגדרות אבטחה בסיסיות שהגדירה החברה. על מנת למנוע פעולות אלה, מקובל לעשות שימוש במנגנון אימות כדוגמת CAPTCH ומנגנון 2FA /MFA/OTP ולהגדיר הגדרות למניעת מתקפה מסוג זה ב-WAF. בזמן האירוע החברה לא ביצעה פעולות אלה כנדרש. בנוסף יוזכר כי מנגנון הסיסמאות מלכתחילה הוגדר על ידי החברה באופן לא מאובטח. על כן נמצא כי החברה לא חסמה בכלים המקובלים את האפשרות לחשוף שמות משתמשים וסיסמאות.

- מדיניות הסיסמאות בה נקטה החברה נמצאה כחלשה ולא מאובטחת באמצעי פיזי נוסף, דבר אשר אפשר קביעת סיסמאות חלשות על ידי לקוחות המחזיקה, שימוש בו-זמני של מספר משתמשים באותם פרטי גישה ועוד. מאחר וסיסמאות ניתנות להעברה ומאחר ולא הוגדר כל מנגנון לזיהוי ואימות נוסף ואף לא מנגנון ניטור, לא ניתן היה לאכוף כל פיקוח על ההתחברות למערכת ועל הפעולות במערכת.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

10.10 **הרשות דוחה את טענות החברה ביחס לביעור המידע החלקי אשר ביצעה.** בטענות החברה ביחס לשמירת הקבצים אשר היו אמורים להיות מבוערים, אין הסבר או צידוק להפרה של הוראות החוק וההסכם עם לקוחותיה.

כפי שפורט בהרחבה בסעיף 7.5 למכתב ההפרה לכאורה, כל גורם באשר הוא, לרבות בעל מאגר או מחזיק במאגר, אשר מקבל לידיו עותק מפנקס הבוחרים במסגרת הבחירות לכנסת, מחויב לבער כל מידע מתוך פנקס הבוחרים אשר השימוש בו במסגרת הבחירות הסתיים. כלומר, חלה חובה על המפלגות ועל מי שמחזיק מטעמן בפנקס הבוחרים לבער את הפנקס עם קבלת נגזרת חדשה שלו או עם סיום הליך הבחירות.

10.11 **הרשות דוחה את טענת החברה ממנה משתמע כי החברה תתקן רק את הליקויים כפי שהיא רואה לנכון לתקן או באופן שהיא מבינה כי נכון לתקנן.** הנחיית הרשות לתיקון הליקויים כפי שעלתה במכתב ההפרה לכאורה אינה בגדר המלצה והרשות דורשת מהחברה לקיים את הנחייתה זו, ככל הנדרש לקיום הוראות החוק והתקנות. אי מילוי הוראות הרשם ודרישותיו עלולות להוות בסיס להפעלת סמכויות רשם מאגרי המידע כפי שהן מפורטות בסעיף 10(ו) לחוק, בדבר התליית מאגרי המחזיקה או ביטולן.

10.12 במכתב ההפרה לכאורה קבעה הרשות כי החברה הפרה לכאורה את הוראות סעיף 17ב(א)(1) לחוק בכך שלא מינתה ממונה אבטחת מידע. אולם לאחר בחינה מחודשת של הממצאים ולאחר עיון במענה החברה, הרשות חוזרת בה מקביעה זו.

11 <u>קביעת הפרת הוראות החוק והתקנות</u>

לאור כל האמור לעיל וכמפורט במכתב ההפרה לכאורה, ולמעט הקביעה ביחס להפרה לכאורה של סעיף 17ב(א)(1) לחוק, והואיל ובקשר עם העתק פנקס הבוחרים לכנסת ה-23 שנמסר לחברה על ידי המפלגות, החברה היא המחזיקה במאגר המידע ואחראית לאבטחת המידע בו, הרשות קובעת בזאת כי החברה הפרה את הוראות החוק והתקנות כמפורט להלן (להלן – "**סעיפי הקביעה**"):

11.1 החברה ביצעה שבע הפרות של הוראות סעיף 8(ב) לחוק.

11.2 החברה הפרה את הוראות סעיף 17 לחוק.

11.3 החברה הפרה את הוראות סעיף 17א(א) לחוק.

11.4 החברה הפרה את הוראות סעיף 17א(ב).

11.5 החברה הפרה את הוראות תקנות 3, 4(א) עד4(ו), 5(א) עד 5(ה), 7(א) עד 7(ג), 8, 9, 10, 11, 13, 14, 16, 18(א) לתקנות.

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

מחלקת אכיפה

12 **<u>הטלת קנס בגין הפרת הוראות החוק</u>**

בהתאם להוראות סע' 31א(א)(5) לחוק ולהוראות תקנות העבירות המנהליות (קנס מנהלי - הגנת הפרטיות), התשס"ד – 2004, הפרות של הוראות סעיפי הקביעה, מהווה עבירות מנהליות לגביהן קבוע קנס מנהלי.

הודעה על הטלת קנס מנהלי קצוב לפי סעיף 8 לחוק העבירות המנהליות, התשמ"ו-1985 וכן הוראות לגבי אופן ומועדי תשלום הקנס, בקשה לביטולו או בקשה להישפט המצויות בגב ההודעה, יועברו לחברה במועד שיקבע.

13 קביעה זו תפורסם באתר האינטרנט של הרשות.

בכבוד רב,

קלדרון עלי, עו"ד
מנהל מחלקת אכיפה
הרשות להגנת הפרטיות

073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL