7 ינואר 2021
כ"ג טבת תשפ"א

דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה – 24:
מגבלות השימוש בפנקס הבוחרים ובמידע אישי אחר
ואחריות המפלגות על אפליקציות וספקים חיצוניים

מבוא

1. בהליכי בחירות, בוודאי בעידן הדיגיטלי, קיימים היבטים של פרטיות ואבטחת מידע, שיש לתת עליהם את הדעת, וזאת על מנת לצמצם את האפשרות לפגיעה בפרטיות בוחרים, לזליגת פנקס הבוחרים ולפגיעה בהליך עצמו.

2. לקראת הבחירות לכנסת ה-24, הרשות להגנת הפרטיות מבקשת להזכיר למפלגות ולציבור הרחב את המגבלות החלות על שימוש במידע מפנקס הבוחרים ובסוגים אחרים של מידע אישי שאוספות המפלגות במסגרת הקמפיין, בהתאם להוראות חוק הבחירות לכנסת [נוסח משולב], התשכ"ט-1969 (להלן: "**חוק הבחירות**") וחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**" או "**החוק**").[1]

3. במיוחד נבקש להדגיש את חובות אבטחת המידע, את המטרות המוגבלות לשמן מותר השימוש במידע, את התנאים לרכישת מידע מסוחרי מידע, וכן את האחריות המשפטית המלאה של המפלגות על הפרות ועבירות המבוצעות בידי קבלנים וספקים הפועלים מטעם המפלגות או עבורן.

רקע – דיגיטציה של מערכת הבחירות

4. כמו תהליכים אחרים, גם עולם ניהול הקמפיינים לקראת מערכת הבחירות הפך בשנים האחרונות לדיגיטלי, ובזמן כל מערכת בחירות קמות חברות המתמחות באספקת פלטפורמות לניהול הקשר עם הבוחרים.

5. גם בישראל פועלות חברות אשר עוסקות במתן שירותים למפלגות וליחידים לקראת מערכות בחירות. אם בעבר, חברות אלו הוקמו סמוך לבחירות, או לחילופין היוו פרויקט זמני מטעם חברה או מפלגה, הרי שבשנים האחרונות אנו עדים לגידול משמעותי בפעילות בתחום, וכניסתן של חברות אלה גם לעולם האפליקציות לטלפונים הניידים ולמכשירי הקצה החכמים האחרים.

[1] מסמך זה הוא גרסה מעודכנת ומשולבת של פרסומים קודמים של הרשות בעניין "ריענון הוראות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה – 23" ובעניין קווים מנחים לשימוש באפליקציות ובספקים חיצוניים לצורך ניהול מערכת בחירות": לצפייה במסמך.

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

6. אפליקציות אלו מציעות שירותים ושימושים שונים, ובין היתר:

6.1. הנגשת פנקס הבוחרים למערכת ניהול ידע נוחה לשימוש.

6.2. הוספת שדות מידע ממקורות שונים לשם "טיוב" המידע אודות בוחרים, כגון פרטי קשר, גילאים, שפות, מגדר וכו'.

6.3. הצלבת נתונים עם מאגרי מידע פתוחים ברשת, כגון רשתות חברתיות ומאגרים שנרכשים מחברות אחרות.

6.4. אפשרות יצירת קשר עם הבוחר לצרכי תמיכה במפלגה, התנדבות, סיוע למצביעים להגיע לקלפיות ועוד.

6.5. אפשרות יצוא נתונים לצרכי ניהול הקמפיין, ניהול הקשר עם המתפקדים והמתנדבים, שליחת דיוור ישיר, סקרים וכד', או שימוש כאמור במסגרת אפליקציה.

6.6. הצגת מידע סטטיסטי ומידע בזמן אמת ביום הבחירות, לצורך קבלת תובנות אסטרטגיות בנוגע לקבוצות בוחרים או לבוחרים ספציפיים.

<u>רקע נורמטיבי</u>

<u>תחולת הוראות חוק הגנת הפרטיות וחוק הבחירות לכנסת</u>

7. האינפורמציה הנוגעת לאנשים יחידים, הנאספת ומנוהלת בידי המפלגות במסגרת קמפיין הבחירות, בעצמן או באמצעות נותני שירות או אפליקציות חיצוניות, היא "**מאגר מידע**" כהגדרתו בחוק הגנת הפרטיות. רמת האבטחה של מאגר המבוסס על מידע פנקס תהיה לפחות ברמת האבטחה הבינונית, כפי שהיא מוגדרת בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 (להלן: "**תקנות האבטחה**").

8. על ניהול מאגר מידע חלות הוראות פרק ב' לחוק הגנת הפרטיות ותקנות האבטחה. המפלגות הן "**בעל המאגר**" כמשמעותו בחוק, ולכן הן הנושאות באחריות העיקרית לקיום הוראות החוק והתקנות שמכוחו.

9. השימוש בנתונים שמקורם בפנקס הבוחרים, כפוף גם למגבלות המחמירות שמטיל חוק הבחירות.

10. **להסרת ספק, מובהר שהוראות חוק הגנת הפרטיות ותקנות האבטחה חלות במלואן על מאגרי המידע שהמפלגות וספקיהן מנהלים ומעבדים, וזאת <u>בנוסף</u> לחוק הבחירות ובמקביל להוראותיו[2].**

[2] סעיף 25 לתקנות האבטחה קובע במפורש כי הוראות התקנות "יחולו **<u>נוסף</u>** על הוראות בעניין אבטחת מידע בחיקוקים אחרים, זולת אם יש סתירה ביניהן".

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

<u>הוראות החוק הרלבנטיות</u>

11. חוק הגנת הפרטיות קובע בסעיף 2(9) את עקרון צמידות המטרה, דהיינו שהשימוש במידע ייעשה רק למטרה שלשמה נמסר. כמו כן, סעיף 8(ב) לחוק קובע, כי "לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר". עקרון צמידות המטרה קיבל ביטוי אף בסעיף 39(ג) לחוק הבחירות הקובע, כי אסור למפלגה או לסיעה לעשות במידע שימוש אחר שאינו קשור להתמודדות בבחירות ולקשר עם הבוחר, לרבות העברתו לצד שלישי לשימושים אחרים.

12. שימוש במידע הפנקס, כגון רשימת הבוחרים למטרות אחרות מאלה שפורטו בחוק, מהווה עבירה שדינה מאסר שנתיים, לפי סעיף 118א לחוק הבחירות. בנסיבות מסוימות הדבר יהווה גם עבירה של פגיעה בפרטיות שדינה חמש שנות מאסר, או עבירה של שימוש במאגר מידע שלא למטרה לשמה הוקם שדינה שנת מאסר[3].

13. לפי סעיף 17 לחוק הגנת הפרטיות, מוטלת על המפלגות גם האחריות לאבטחת המידע המוחזק אצלן. תקנות האבטחה מפרטות את עקרונות אבטחת המידע הקשורים בניהול ובשימוש במידע השמור במאגרי מידע, דוגמת פנקס הבוחרים.

14. תקנות האבטחה קובעות 3 רמות של מאגרי מידע, עליהן חלות רמות אבטחה שונות, בהתאם לסיכוני האבטחה שהם מייצרים (בסיסית, בינונית וגבוהה). התקנות מפרטות את החובות החלות בהתאם לרמת האבטחה של המאגר. רמת האבטחה של מאגר המבוסס על מידע פנקס הינו לפחות ברמת האבטחה הבינונית.

15. על מאגרי מידע ברמת האבטחה הבינונית והגבוהה חלה חובת דיווח לרשות להגנת הפרטיות (רשם מאגרי המידע) במקרה של אירוע אבטחה חמור, כפי שמוגדר בתקנה 1 לתקנות האבטחה[4].

16. כמו כן, נזכיר כי סעיף 16 לחוק הגנת הפרטיות קובע שגילוי מידע שהגיע לאדם בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, שלא לצורך ביצוע עבודתו - הוא עבירה של הפרת חובת סודיות שדינה חמש שנות מאסר.

<u>פרטיות ואבטחת מידע בהליכי בחירות - דגשים והמלצות</u>

עד כאן פורטו הוראות החוק הכלליות. להלן יפורטו הדגשים והמלצות של הרשות בנושא:

<u>פירוט דרישות החוק</u>

[3] סעיפים 5 ו – 31א לחוק הגנת הפרטיות.

[4] מידע נוסף בנושא ניתן למצוא באתר הרשות להגנת הפרטיות: <u>לינק לצפייה באתר</u>.

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

17. מבלי לגרוע מכלליות האמור, מוטלת על המפלגות האחריות המשפטית הישירה:

17.1. להימנע מלעשות במידע מפנקס הבוחרים שימוש שאינו קשור להתמודדות בבחירות לכנסת ה- 24 וליצירת קשר עם הבוחר, לרבות הימנעות מהעברתו לצד שלישי לשימושים אחרים[5].

17.2. להימנע מלעשות במידע מכל סוג שימוש שלא ניתנה לגביו הסכמה של האדם הרלבנטי, או שימוש החורג מההסבר שחובה לתת לאדם ממנו אוספים מידע, בדבר מטרת השימוש ולמי יימסר[6]. **ככל שלא ניתנה הסכמתם של האזרחים להזנת פרטים אודותיהם ביישומים או במאגרי המידע של המפלגה, במיוחד אינדיקציות בדבר תמיכתם או אי תמיכתם במפלגה כזו או אחרת, מדובר לכאורה בשימוש בלתי חוקי המפר את הוראות סעיף 2(9) לחוק הגנת הפרטיות.**

17.3. להימנע מלעשות שימוש במידע אשר הגיע מפנקס בוחרים שאינו הפנקס העדכני אשר קיבלה המפלגה מהמפקחת על הבחירות לצורך בחירות אלה. **אין לעשות שימוש בפנקסי עבר, מפנקסי בחירות לרשויות המקומיות וכד'.**

17.4. לקיים את כל הוראות תקנות האבטחה הנוגעות למאגר ברמת אבטחה גבוהה או בינונית, לרבות –

17.4.1. תקנות 8 ו- 9 - הגבלת הגישה למידע רק למורשי הגישה החיוניים בהתאם להגדרות תפקידם ובמידה הנדרשת לביצוע תפקידם בלבד.

17.4.2. יש לקבוע הרשאות גישה למאגר לכל עובד, רק במידה הנדרשת לו לצורך ביצוע תפקידו ולנהל רישום מעודכן של התפקידים, של בעלי ההרשאות ושל ההרשאות שניתנו להם.

17.4.3. יש לוודא שמי שניגש למידע במאגר הוא עובד מורשה, ולכן יש לאמת את זהותו לפחות באמצעות סיסמא חזקה.

17.4.4. אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.

17.4.5. יש לשמור תיעוד (לוגים) של כל פעולות הצפייה/ ההורדה/ עדכון המידע המצוי במאגר המידע.

17.4.6. תקנה 6 - אבטחה פיזית של מערכות המידע המכילות את המאגר.

17.4.7. תקנה 7 - מיון והדרכת כוח אדם: דווקא בשל העומס הרב שמאפיין את תקופת הבחירות והשימוש בעובדים ובמתנדבים ארעיים, על המפלגה מוטלת האחריות

[5] סעיפים 2(9) ו – 8(ב) לחוק הגנת הפרטיות וסעיף 39(ג) לחוק הבחירות.

[6] סעיפים 1 ו – 11 לחוק הגנת הפרטיות.

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

לוודא כי גישה למידע תינתן רק לאחר נקיטת אמצעים סבירים המקובלים בהליכי מיון עובדים, וכי הרשאות גישה למידע הפנקס יינתנו רק למי שעבר הליך מיון מסודר ונמצא מתאים וזאת לאחר ביצוען של הדרכות בנושא החובות החלות לפי החוק והתקנות.

17.4.8. תקנה 11 - דיווח מיידי לרשות להגנת הפרטיות על אירועי אבטחה חמורים.

17.4.9. תקנה 12 - מניעת העתקה וחיבור של התקנים ניידים.

17.4.10. תקנה 14 - אבטחת תקשורת ורשתות.

17.4.11. תקנה 15 - עריכת בחינה מוקדמת של התאמת האפליקציות והספקים לציות להוראות הדין, חתימה על הסכם התקשרות מסודר עימם, ופיקוח ובקרה בפועל על פעולותיהם[7]. מומלץ כי דרישה מקדמית של כל התקשרות בין המפלגה לנותן השירות, תהיה קבלתו של דו"ח ביקורת או סקר סיכונים בנושא אבטחת מידע מהמחזיק.

17.4.12. תקנות 5 ו- 16 - ביצוע ביקורות וסקרי סיכוני אבטחה פנימיים למערכות המפלגה.

17.5. הגשת בקשה לרישום מאגר המידע המנוהל באפליקציה או בידי ספק השירות בפנקס מאגרי המידע ברשות להגנת הפרטיות.

17.6. קיום דרישות חוק הגנת הפרטיות בנושא דיוור ישיר - חוק הגנת הפרטיות קובע כי כל פנייה בדיוור ישיר תכיל ציון לפיו, הפנייה נעשתה בדיוור ישיר, זהות השולח והמקורות שמהם קיבל בעל המאגר מידע זה ואת זכותו של הנמען להימחק מהמאגר שעל פיו בוצעה הפנייה. עוד קובע החוק, כי כל אדם זכאי לדרוש, בכתב, מבעל מאגר המידע המשמש לדיוור ישיר, שמידע המתייחס אליו יימחק ממאגר המידע. דהיינו, יש לבצע הסרה מוחלטת של פרטי הקשר וכל נתון אחר אודות מבקש המחיקה. להרחבה ראו הנחיית רשם מאגרי מידע מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר"[8], וכן ראו "קוים מנחים לרכישת מידע לצרכי דיוור ישיר" שפרסמה הרשות[9].

17.7. **בתום הבחירות יש לבער את כל עותקי המידע שמקורו בפנקס הבוחרים שנמצא אצל המפלגה ולוודא ביעור המידע אצל כל הספקיות במיקור חוץ של המפלגה, ושל כל נגזרת של מידע פנקס אשר הגיע לידם.**

<u>שימוש במידע מפנקס הבוחרים</u>

[7] סעיף 15 לתקנות אבטחת המידע והנחיית רשם מאגרי המידע 2/2011 בעניין שימוש בשירותי מיקור חוץ: לינק לצפייה באתר.

[8] לינק לצפייה באתר

[9] לינק לצפייה באתר.

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

18. סעיף 26(א) לחוק הבחירות קובע, כי לקראת מועד בחירות יוכן פנקס בוחרים (להלן: "**הפנקס**"), שיכלול כל אדם שהוא אזרח ישראלי ורשום, הוא ומענו, במרשם האוכלוסין כתושב. תנאי נוסף להיכללות בפנקס הוא מי שיום הולדתו ה-18 חל לא יאוחר מיום הבחירות. על פי הגדרות חוק הבחירות, הפנקס כולל את כלל רשימות הבוחרים.

19. המידע הנכלל ברשימות הבוחרים נגזר ממרשם האוכלוסין והוא כולל את שם המשפחה של כל בוחר, שמו הפרטי, שם אביו או אמו, שנת לידתו, מענו ומספר זהותו במרשם האוכלוסין וכן מידע על אודות מיקום הצבעתו בקלפי ביום הבחירות. מידע נוסף שניתן ללמוד מקובץ זה הוא העובדה שכל הרשומים בו הם מעל גיל 18, ובין החיים (להלן: "**מידע פנקס**").

20. לקראת הבחירות, מוסר משרד הפנים למפלגה או לסיעה בכנסת, באמצעי אלקטרוני או מגנטי מידע פנקס, בהתאם להוראות סעיף 39 לחוק הבחירות. שר הפנים רשאי להורות, כי באמצעי האלקטרוני או המגנטי ייכלל אמצעי הגנה, לרבות הוספת מידע לזיהוי הקובץ.

21. סעיף 39(ה) לחוק הבחירות קובע, כי שר הפנים יודיע לרשם מאגרי מידע לאילו מפלגות או סיעות נמסר הפנקס.

22. עם תום תקופת הבחירות, על המפלגה או הסיעה להחזיר את מידע הפנקס ליחידת הפיקוח הארצי על הבחירות.

23. ניסיון העבר מלמד, כי בפועל השימושים בפנקס כוללים העברת מידע למטות הבחירות ולפעילים, טיוב הנתונים והשלמתם על ידי רכישת מידע מפולח ומאופיין ומספרי טלפון, ביצוע סקרים, משלוח הודעות מוקלטות לבוחרים, הדרכת בוחרים לגבי מיקום הקלפי, המרצת אנשים להגיע לקלפי ועוד.

<u>אחריות המפלגות על פעולות האפליקציות ונותני שירות חיצוניים</u>

24. ספקי השירות החיצוני העוסקים בעיבוד או באחסון גרידא של נגזרות פנקס הבוחרים ושל הנתונים האחרים המצורפים אליהן הם "**מחזיק**" כהגדרתו בחוק הגנת הפרטיות, אף אם משך מתן השירות מוגבל לתקופת הבחירות, או לפרק זמן קצר יותר.

25. **הרשות מבהירה כי האחריות לקיום הוראות חוק הגנת הפרטיות וחוק הבחירות מוטלת בראש וראשונה על המפלגות עצמן. המפלגות הן "בעלי המאגר" אשר עלולות לשאת באחריות פלילית או אזרחית, גם להפרות שיבוצעו באפליקציה או בידי ספק שירות חיצוני עבור המפלגות או מטעמן.**

26. **לאור הרגישות הגבוהה של מידע הפנקס והנזקים החמורים העלולים להיגרם מדליפתו לידי גורמים בלתי מורשים, על המפלגות לנקוט את כל האמצעים הנדרשים ואמצעי האבטחה המחמירים הנדרשים בהוראות החוק ותקנות האבטחה, הן ביחס לעמידתן בדרישות החוק בעצמן והן ביחס לספקים אליהם יועבר המידע, בכל הנוגע לטיפול בפנקס.**

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

דגשים והמלצות ממערכות בחירות קודמות

27. בשים לב להיבטים האמורים, ומבלי לגרוע מכלליות האמור במסמך זה ומן החובה לקיים את מלוא הוראות החוק ותקנות האבטחה, מפורטים להלן בנספח המצורף דגשים והמלצות של הרשות, לעניין אמצעי האבטחה הבסיסיים אותם על מפלגה לנקוט בעת שימוש באפליקציית בחירות או בהסתייעות בספקי מיקור חוץ לצורך ניהול הקמפיין.

28. לצורך השלמת התמונה, מופנות המפלגות לדו"ח ממצאי הליך פיקוח הרוחב שפרסמה הרשות להגנת הפרטיות, זאת בהמשך להליך פיקוח רוחב מתוכנן שביצעה בחודש פברואר 2020 אצל המפלגות שהתמודדו בבחירות לכנסת ה- 23, שתוצאותיו פורסמו לציבור וזמינות באתר הרשות[10], וכן לדו"ח[11] בעניין "ממצאי הליך פיקוח הרוחב בקרב מגזר חברות אחסון ועיבוד מאגרי מידע בישראל"[12].

[10] לינק לצפייה באתר
[11] לינק לצפייה באתר
[12] יצוין כי הרשות מקיימת הליך אכיפה מנהלי פרטני למול מספר מפלגות וספק השירות שלהן לאחר שהתגלה אירוע אבטחה חמור באחת מאפליקציות הבחירות.

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

נספח דגשים והמלצות אבטחת מידע –

לשימוש המפלגות באפליקציות ולהסתייעות בספקי שירותי עיבוד

1. מפורטים להלן דגשים והמלצות לשימוש המפלגות באפליקציות ושירותים חיצוניים ולהסתייעות בגורמים במיקור חוץ במסגרת קמפיין בחירות.
2. בנספח זה "**אפליקציה**" או "**שירות**" יתייחסו לכל מערכת אשר מנגישה את מידע הפנקס לצרכי קמפיין הבחירות של מפלגה, בין אם הדבר נעשה בתצורה של אתר אינטרנט, אפליקציית מובייל, תוכנת מחשב, מבוסס שרתים מקומי או מרוחק או שירותי ענן, ובין אם הוא מסופק או נתמך על ידי ספק חיצוני או פנימי של המפלגה.
3. **מומלץ כי נותני השירות הרלוונטיים יהיו מוסמכים בתקן iso 27001 ובתקן ISO 27032, וכי דרישה מקדמית של התקשרות בין המפלגה לנותן השירות, תהיה קבלתו של דו"ח ביקורת או סקר סיכונים בנושא אבטחת מידע מהמחזיק.**
4. יש לוודא כי השירות עבר מבדק חדירות אפליקטיבי ותשתיתי והליקויים שנמצאו בו (ככל ונמצאו) תוקנו.
5. **דרישות פיתוח:**

5.1. על המפלגות לוודא כי השירות פותח מתחילתו ועד סופו על פי מתודולוגיית פיתוח מאובטח, באמצעות חברה בעלת רקורד ומוניטין בפיתוח תוכנה.

5.2. יש לוודא כי מוגדר מנגנון ניהול הרשאות היררכי קפדני על בסיס הצורך לדעת (Need To Know) והצגת מינימום המידע הדרוש.

5.3. על המפלגה לוודא כי בטרם מתן גישה למידע אישי, כל בעל הרשאה הינו מתאים לקבל גישה למידע בהתאם לתפקידו וכי קיבל הדרכה בנושא החובות על פי חוק הגנת הפרטיות ותקנותיו.

5.4. יש לוודא כי בכל גישה למידע אישי מיושמת מדיניות סיסמאות מוקשחת (מומלץ לעשות שימוש במנגנון אימות MFA/2FA/OTP).

5.5. יש להגדיר מנגנון ניטור ותיעוד לכלל הפעולות המבוצעות על ידי המשתמשים ללא אפשרות ביטולו.

5.6. יש להגביל אפשרות ייצוא נתונים/דוחות למינימום הנדרש (לרבות מניעת אפשרות צילום מסך).

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

6. הגדרות אבטחת מידע מומלצות:

6.1. הגדרת הארכיטקטורה בהתאם לסיכוני אבטחת מידע.

6.2. הגדרת אבטחת שירות הענן על פי ה- Best Practice של הספק (AWS\Azure\Google).

6.3. קביעת בקרות אבטחה וביצוע סקר סיכונים ומבדקי חדירות (אפליקטיביים ותשתיתיים) וטיפול בליקויים ובפערים שנמצאו.

6.4. התקנת השרת האפליקטיבי באופן מוקשח ומאובטח (Web Application FW).

6.5. התקנת בסיס הנתונים באופן מוקשח, מוצפן ומאובטח (DataBase FW).

6.6. יש להטמיע מנגנון אבטחה אנטי-וירוס (Next Generation) ו\או פלטפורמת הגנה רב-שלבית (EDR) בכל השרתים ועמדות הקצה הקשורות לשירות.

6.7. יש להטמיע מערכת זיהוי ומניעה (IPS\IDS).

6.8. יש להטמיע מנגנון ניטור, תיעוד והתרעה (למערכות האבטחה).

6.9. יש להגדיר מדיניות סיסמאות מוקשחת.

6.10. יש לוודא כי כלל המערכות מעודכנות בגרסאות ובעדכוני האבטחה האחרונים.

6.11. יש לוודא כי תווך התעבורה מוצפן.

6.12. יש להגדיר בקרה לביעור המידע ועותקיו לצמיתות בסיום השימוש.

7. דרישת חובה כתנאי להתקנת האפליקציה על מכשיר הקצה (יובנה ביישום):

7.1. יש לוודא כי מכשיר הקצה לא עבר פריצה (JailBreak\Root).

7.2. יש לוודא כי במכשיר מוגדרת נעילת אבטחה (ביומטרי\סיסמה\תבנית\קוד).

8. דרישת חובה עם הפעלת האפליקציה במכשיר:

8.1. יש לוודא הצגת גילוי נאות טרם פתיחת היישום בדבר האחריות האישית וחובת שמירת הסודיות של המשתמש.

8.2. לצורך גישה למידע, הפעלת אמצעים לזיהוי המשתמש ואימות הרשאתו כנדרש בתקנות, ולפחות באמצעות אמצעי פיזי נתון לשליטה\אימות (MFA/2FA/OTP).

9. התחברות מרחוק למערכות מידע

לאור משבר הקורונה, והגבלות התנועה וההתקהלות, יתכן כי מערכת הבחירות הקרובה תצריך שימוש מוגבר בהתחברות מרחוק למערכות מידע. להלן מספר דגשים בנושא:

9.1. <u>בעת גישה למערכות ליבה ולמידע רגיש:</u>

9.1.1. אישור הגישה מרחוק יתאפשר רק ממכשיר קבוע, מוכר ומאובטח.

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

9.1.2. גישה תוענק על בסיס מדיניות הרשאות קפדנית והצורך לדעת בלבד (Need To Know).

9.1.3. יש להגדיר מראש מדיניות סיסמאות מוקשחת.

9.1.4. הגישה מרחוק תנוטר, תתועד ותופעל תחת מגבלת זמן (התנתקות אוטומטית בחלוף פרק זמן מוגדר ועבודה בשעות הפעילות המוגדרות).

9.1.5. אימות הגישה יעשה באמצעות אמצעי פיזי נתון לשליטה\אימות כפול (MFA/2FA/OTP).

9.1.6. בעת ההתחברות מומלץ לחסום את אפשרות הגלישה במכשיר שלא דרך רשת הארגון.

9.1.7. יש לחסום גיאוגרפית אפשרות חיבור מחו"ל.

9.1.8. יש לוודא שכלל המכשירים המשמשים להתחברות מרחוק עברו בדיקה מקדמית אשר כולל וידא גרסאות מעודכנות של מערכות ההפעלה, וידוא כי המכשיר אינו פרוץ, התקנת אנטי-וירוס, נעילת מכשיר וכו'.

9.1.9. מומלץ לנהל את מערך ההתחברות מרחוק באמצעות תוכנת ניהול (EMM/MDM), לעבודה תחת קונטיינר מאובטח, לצורך אכיפת דרישות הקדם שלעיל ולאפשר מחיקה או פרמוט מרחוק במקרה של אובדן או גניבה.

9.1.10. ביצוע הדרכת מודעות לפעילים טרם מתן אישור לחיבור מרחוק.

9.2. <u>בעת גישה לאפליקציות מתפקדים</u>:

9.2.1. חובת הגדרת נעילת המכשיר באמצעות סיסמה חזקה/אמצעי ביומטרי/קוד או תבנית.

9.2.2. יש להגדיר נעילה אוטומטית לאחר 30 שניות.

9.2.3. הפעלה והגדרת אימות דו שלבי לצורך התחברות.

9.2.4. יש לוודא כי המחשב/מכשיר סלולרי/טאבלט עובדים בגרסת מערכת ההפעלה האחרונה ומעודכנים בעדכוני האבטחה האחרונים.

9.2.5. יש להימנע ככלל משימוש ברשתות Fi-Wi פתוחות ויש לעבוד באמצעות הרשת סלולרית או באמצעות רשת ווירטואלית פרטית (VPN).

9.2.6. במידה ומתחברים מרשת ה-Fi-Wi הביתית יש לוודא כי הרשת פרטית ומוגדרת סיסמת התחברות מוקשחת, אשר לא בוצע בה שימוש בחשבון אחר וסיסמת ברירת המחדל של הנתב הוחלפה בסיסמה מוקשחת.

9.2.7. אין להשאיר את מכשיר הקצה ללא השגחה.

9.2.8. יש לעבוד עם סיסמאות מוקשחות ושונות לכל שרות כך שאינן חוזרות על עצמן.

9.2.9. לדווח מידית למנהלי הקמפיין על כל חשש לחדירה, העתקה או דליפה של מידע או דבר אחר שאינו שיגרתי.

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