דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה – 25:
מגבלות השימוש בפנקס הבוחרים ובמידע אישי אחר
ואחריות המפלגות על אפליקציות וספקים חיצוניים

מבוא

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

2. לקראת הבחירות לכנסת ה-25, 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**").

3. במיוחד נבקש להדגיש את חובות אבטחת המידע, את המטרות המוגבלות לשמן מותר השימוש במידע, 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. בדומה לתהליכים אחרים, גם עולם ניהול הקמפיינים לקראת מערכת הבחירות הפך בשנים האחרונות לדיגיטלי, ומדי מערכת בחירות קמות חברות המתמחות ביצירת פלטפורמות לניהול הקשר עם הבוחרים.

5. גם בישראל פועלות חברות אשר עוסקות במתן שירותים למפלגות וליחידים לקראת מערכות בחירות. אפליקציות אלו מציעות שירותים ושימושים שונים, ובין היתר:

   5.1. הנגשת פנקס הבוחרים למערכת ניהול ידע נוחה לשימוש.

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

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

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

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

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

רקע נורמטיבי

תחולת הוראות חוק הגנת הפרטיות וחוק הבחירות לכנסת

6. אינפורמציה 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 מתוך פנקס הבוחרים תהיה לפחות ברמת האבטחה הבינונית, כפי שהיא מוגדרת בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 (להלן: "**תקנות אבטחת מידע**").

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

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

9. **להסרת ספק, מובהר שהוראות חוק הגנת הפרטיות ותקנות אבטחת מידע חלות במלואן על מאגרי המידע שהמפלגות וספקיהן מנהלים ומעבדים, וזאת בנוסף לחוק הבחירות ובמקביל להוראותיו[1].**

הוראות החוק הרלבנטיות

10. חוק הגנת הפרטיות קובע בסעיף 2(9) את עקרון צמידות המטרה, דהיינו שהשימוש במידע אישי 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.

11. שימוש במידע מתוך פנקס הבוחרים, כגון רשימת בעלי זכות הבחירה, למטרות אחרות מאלה שפורטו בחוק, מהווה עבירה שדינה שנתיים מאסר, לפי סעיף 118א לחוק הבחירות. בנסיבות

[1] תקנה 25 לתקנות אבטחת מידע קובעת במפורש כי התקנות "יחולו **נוסף** על הוראות בעניין אבטחת מידע בחיקוקים אחרים, זולת אם יש סתירה ביניהן".

מסוימות הדבר יהווה גם עבירה של פגיעה בפרטיות לפי סעיף 2 לחוק הגנת הפרטיות, שדינה חמש שנות מאסר, או עבירה של שימוש במאגר מידע שלא למטרה לשמה הוקם, שדינה שנת מאסר[2].

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

13. התקנות מחלקות את כלל מאגרי המידע האישי במשק ל-3 רמות אבטחה שונות, בהתאם לסיכוני האבטחה שהם מייצרים (רמת אבטחה בסיסית, בינונית או גבוהה). התקנות מפרטות את החובות החלות בהתאם לרמת האבטחה של המאגר. מאגר המבוסס על מידע מתוך פנקס הבוחרים **יהיה לכל הפחות ברמת האבטחה הבינונית** לפי התקנות.

14. על מאגרי מידע ברמת האבטחה הבינונית והגבוהה חלה חובת דיווח לרשות להגנת הפרטיות במקרה של אירוע אבטחה חמור, כהגדרתו בתקנה 1 לתקנות אבטחת מידע[3].

15. 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 הוראות החוק הכלליות. להלן יפורטו דגשים והמלצות של הרשות בנושא:

<u>פירוט דרישות החוק</u>

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

16.1. להימנע מלעשות במידע מפנקס הבוחרים שימוש שאינו קשור להתמודדות בבחירות לכנסת וליצירת קשר עם הבוחר, לרבות הימנעות מהעברתו לצד שלישי לשימושים אחרים[4].

16.2. להימנע מאיסוף מידע אישי ומכל שימוש בו, אשר חורגים מן המטרות להן הסכים האדם (נושא המידע) בעת שמסר את המידע על אודותיו.

16.3. ניתן לאסוף שמות של צדדים שלישיים כתומכים פוטנציאליים במפלגה, לרבות באמצעות אפליקציה. אולם, כאשר המידע על התומך הפוטנציאלי מבוסס על מידע

[2] סעיפים 5 ו-31א לחוק הגנת הפרטיות.

[3] תקנה 11(ד)(1) לתקנות אבטחת מידע.

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

שהתקבל מהאדם עצמו (נושא המידע), נדרשת הסכמתו לכך שהמפלגה תאסוף מידע אודותיו, בין אם בדרך של הסכמה מפורשת כי המידע יועבר למפלגה, לאחר שהוסברו לו המטרות והשימושים שייעשו במידע[5], ובין אם בדרך אחרת ממנה ניתן להסיק בבירור על הסכמה משתמעת למסירת המידע, כגון במקרה בו אדם הביע באופן פומבי תמיכה מובהקת ומפורשת במפלגה מסוימת בפרופיל הפתוח שלו ברשת חברתית.

16.4. ככל שמפלגה מעוניינת לבצע איסוף מידע אישי אודות תומכים פוטנציאליים באמצעות אפליקציה, עליה להבהיר לכלל המשתמשים באפליקציה כי חלה חובה לקבל את הסכמתו של כל תומך פוטנציאלי לאיסוף המידע אודותיו ולשימושים בו (אלא אם מדובר במידע שלא נמסר על ידי התומך עצמו, אלא נגזר למשל מניתוח של המידע שהתקבל מפנקס הבוחרים). על מנת לאפשר הליך הסכמה ברור, הן למשתמשי האפליקציה והן לנושאי המידע, ושלא להכשיל את משתמשי האפליקציה בעבירה על הוראות חוק הגנת הפרטיות, מוצע לשקול לשלב דרך טכנולוגית שתאפשר ביצוע בקשת וקבלת ההסכמה כנדרש.

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

16.6. לקיים את כל הוראות תקנות אבטחת מידע הנוגעות למאגר ברמת אבטחה גבוהה או בינונית, ובכלל זה ההוראות הבאות –

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

16.6.2. 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. כל שינוי בתפקידים והרשאות חייב להיות מתועד ביומן ההרשאות.

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

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

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

16.6.6. תקנה 6 – יש לוודא את האבטחה הפיזית של מערכות המידע המכילות את המאגר.

[5] סעיף 11 לחוק הגנת הפרטיות.

16.6.7. תקנה 7 - דווקא בשל העומס הרב שמאפיין את תקופת הבחירות והשימוש בעובדים ובמתנדבים ארעיים, על המפלגה מוטלת האחריות לוודא כי גישה למידע תינתן רק לאחר נקיטת אמצעים סבירים המקובלים בהליכי מיון עובדים, וכי הרשאות גישה למידע מתוך פנקס הבוחרים יינתנו רק למי שעבר הליך מיון מסודר ונמצא מתאים, לאחר ביצוען של הדרכות בנושא החובות החלות לפי החוק והתקנות.

16.6.8. תקנה 11 – חובת דיווח מיידי לרשות להגנת הפרטיות על אירועי אבטחה חמורים.[6]

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

16.6.10. תקנה 14 - אבטחת תקשורת ורשתות.

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

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

16.7. קיום דרישות סימן ב' לפרק ב' בחוק הגנת הפרטיות בנושא דיוור ישיר. זאת בשים לב גם לתיקון שנחקק לאחרונה לחוק הבחירות (דרכי תעמולה), תשי"ט-1959 האוסר פרסום של תעמולת בחירות מבלי לנקוב בשם האדם האחראי להזמנתה.[8] להרחבה ראו

---

[6] לדוגמאות מהם אירועי אבטחה חמורים ראו: לדוגמאות באתר הרשות

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

[8] סעיף 2א1 לחוק הבחירות (דרכי תעמולה), התשי"ט-1959, שנחקק לאחרונה, קובע כך:

2א1. (א) לא יפרסם אדם מודעת בחירות בלי שהיא נושאת את שמו של האדם האחראי להזמנתה ואת הדרכים ליצירת קשר עימו, ולגבי מודעה מודפסת – גם את שמו של המדפיס אותה והדרכים ליצירת קשר עימו, ואם פעל האדם האחראי להזמנתה מטעם מתמודד בבחירות או גוף אחר – תישא המודעה את שם המתמודד או הגוף כאמור, את האות או הכינוי של הסיעה או את רשימת המועמדים ושמה של המפלגה שהגישה את רשימת המועמדים.

(ב) בסעיף זה –

"מודעת בחירות" – כל אחד מאלה:

(1) תעמולת בחירות שנעשית על ידי מתמודד בבחירות, גוף הקשור לסיעה או גוף פעיל בבחירות או מי מטעמם;

(2) תוכן של תעמולת בחירות שפורסם בעבור תשלום;

"מתמודד בבחירות" – כל אחד מאלה:

(1) מפלגה או רשימת מועמדים בבחירות לכנסת או בבחירות לרשות מקומית ולראש רשות מקומית;

(2) מי שנכלל ברשימת מועמדים כאמור בפסקה (1);

(3) מועמד בבחירות לראש רשות מקומית;

(4) סיעה של מועצה יוצאת, כמשמעותה בסעיף 25 לחוק הרשויות המקומיות (בחירות);

(5) נבחר הציבור, כהגדרתו בסעיף 28א לחוק המפלגות.

הנחיית רשם מאגרי מידע מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיווח ישיר ושירותי דיווח ישיר"[9].

16.8. **בתום הבחירות יש לבער את כל עותקי פנקס הבוחרים שנמצאים אצל המפלגה, ולוודא ביעור עותקי הפנקס אצל כל הספקיות של המפלגה הפועלות במיקור חוץ.**

שימוש במידע מפנקס הבוחרים

17. 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 ההגדרות בחוק הבחירות, הפנקס כולל את כלל רשימות הבוחרים.

18. 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**").

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

20. סעיף 39(ה) לחוק הבחירות קובע, כי שר הפנים יודיע לרשות להגנת הפרטיות לאילו מפלגות או סיעות נמסר הפנקס.

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

אחריות המפלגות על פעולות האפליקציות ונותני שירות חיצוניים

22. 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.

(ג) סעיף זה יחול גם על תעמולה בבחירות מקדימות, בשינוי זה: בפסקה (1) להגדרה "מודעת בחירות", במקום "מתמודד בבחירות, גוף הקשור לסיעה או גוף פעיל בבחירות או מי מטעמם" יקראו "מועמד בבחירות מקדימות או מטעמו".

[9] הנחיות דיווח ישיר

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

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

<u>דגשים והמלצות ממערכות בחירות קודמות</u>

25. בשים לב להיבטים האמורים, ומבלי לגרוע מכלל האמור במסמך זה ומן החובה לקיים את מלוא הוראות החוק ותקנות אבטחת מידע, מפורטים להלן **בנספח המצורף** דגשים (בלתי ממצים) לעניין האופן בו יש ליישם את ההוראות המחייבות של החוק והתקנות ולעניין אמצעי האבטחה הבסיסיים אותם יש לנקוט בעת שימוש באפליקציית בחירות או בהסתייעות בספקי מיקור חוץ לצורך ניהול קמפיין הבחירות, והמלצות נוספות בעניינים אלה.

דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה – 25:
מגבלות השימוש בפנקס הבוחרים ובמידע אישי אחר
<u>ואחריות המפלגות על אפליקציות וספקים חיצוניים</u>

<u>נספח דגשים והמלצות אבטחת מידע</u>

דגשים למימוש הוראות התקנות	המלצות נוספות
תקנה 6 – יש לוודא את האבטחה הפיזית של מערכות המידע המכילות את המאגר.	
תקנה 7 - בשל העומס הרב שמאפיין את תקופת הבחירות והשימוש בעובדים ובמתנדבים ארעיים, על המפלגה מוטלת האחריות לוודא כי גישה למידע תינתן רק לאחר נקיטת אמצעים סבירים המקובלים בהליכי מיון עובדים, וכי הרשאות גישה למידע מתוך פנקס הבוחרים יינתנו רק למי שעבר הליך מיון מסודר ונמצא מתאים, לאחר ביצוען של הדרכות בנושא החובות החלות לפי החוק והתקנות.	מומלץ לדרוש מן המועמד תעודת מידע פלילי.
תקנות 8, 9 - הגבלת הגישה למידע רק למורשי הגישה החיוניים, בהתאם להגדרות תפקידם ובמידה הנדרשת לביצוע תפקידם בלבד.	מומלץ לוודא כי מוגדר מנגנון ניהול הרשאות היררכי קפדני על בסיס הצורך לדעת (Need To Know) והצגת מינימום המידע הדרוש.
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. כל שינוי בתפקידים או בהרשאות חייב להיות מתועד ביומן ההרשאות.	
על המפלגה לוודא כי בטרם מתן גישה למידע אישי, כל בעל הרשאה מתאים לקבלת גישה למידע בהתאם לתפקידו, ועבר הדרכה בנושא החובות על פי חוק הגנת הפרטיות ותקנותיו.	
יש לוודא כי בכל גישה למידע אישי מיושמת מדיניות סיסמאות מוקשחת. חובה לוודא שמי שניגש למידע במאגר הוא עובד מורשה, ולכן יש לאמת את זהותו לפחות באמצעות סיסמא חזקה.	מומלץ לעשות שימוש במנגנון אימות OTP\2FA\MFA.

דגשים למימוש הוראות התקנות	המלצות נוספות
אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.	
חובה להגדיר מנגנון ניטור ותיעוד לכלל הפעולות המבוצעות על ידי המשתמשים ללא אפשרות ביטולו.	
יש לשמור את התיעוד (לוגים) של כל פעולות הצפייה/ההורדה/עדכון המידע המצוי במאגר המידע.	
תקנה 11 – חובת דיווח מיידי לרשות להגנת הפרטיות על אירוע אבטחת-מידע חמור. לדוגמה, השבתת האתר עקב מתקפה זדונית; או דלף נתונים ממאגר המידע וחשיפת הנתונים באינטרנט. להן קישור לטופס דיווח: https://formspdf.justice.gov.il/PrivacyProtectionAuthority/ReportingSecurityIncident.aspx	
תקנה 12 - מניעת העתקה וחיבור של התקנים ניידים.	• מומלץ לקבוע מדיניות אבטחה המונעת חיבור התקן נייד ליציאת USB. • מומלץ להגביל אפשרות ייצוא נתונים/דוחות למינימום הנדרש (לרבות מניעת אפשרות צילום מסך).

דגשים למימוש הוראות התקנות	המלצות נוספות
תקנה 14 - אבטחת תקשורת ורשתות. יש לאבטח את התקשורת של משתמשי האפליקציה והאתר לשם הגנה על מערכות מאגר המידע. במקרה של משתמש שאינו עובד המפלגה, יש להקפיד על תקשורת מאובטחת ומוצפנת ועל הרשאת גישה קשיחה וממודרת. במקרה של עובד המתחבר באמצעות אפליקציה על-גבי הרשת הארגונית יש להקפיד על ההנחיות להלן.	• מומלץ להגדיר את הארכיטקטורה בהתאם לסיכוני אבטחת מידע. • מומלץ להגדיר את אבטחת שירות הענן על פי ה-Best Practice של הספק, כגון: AWS\Azure\Google. • 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. • מומלץ לבצע הדרכת מודעות לפעילים טרם מתן אישור לחיבור מרחוק.
חובה לוודא כי כל מערכת הפעלה וכל תוכנת אבטחה מעודכנת עם כל עדכון (Patch) בגרסתו האחרונה.	
יש להטמיע מנגנון אבטחה אנטי-וירוס (Next Generation) או פלטפורמת הגנה רב-שלבית (EDR) בכל השרתים ועמדות הקצה הקשורות לשירות.	
יש להטמיע מנגנון ניטור, תיעוד והתרעה (למערכות האבטחה).	
יש להגדיר מראש מדיניות סיסמאות מוקשחת. לעובד המפלגה חובה להגדיר סיסמאות מוקשחות ושונות לכל שרות, שאינן חוזרות על עצמן.	
יש לוודא כי תווך התעבורה מוצפן, להימנע ככלל משימוש ברשתות Wi-Fi פתוחות ולעבוד באמצעות רשת סלולרית.	• מומלץ שעובד המפלגה יתחבר באמצעות רשת ווירטואלית פרטית (VPN). • מומלץ להטמיע מערכת לזיהוי ומניעה (IPS\IDS).
אימות הגישה יעשה באמצעי פיזי הנתון לשליטת המשתמש או באימות כפול (MFA/2FA/OTP).	

דגשים למימוש הוראות התקנות	המלצות נוספות
גישה תוענק על בסיס מדיניות הרשאות קפדנית והצורך לדעת בלבד (Need To Know).	לעובד המפלגה בעת ההתחברות מומלץ לחסום את אפשרות הגלישה במכשיר שלא דרך רשת הארגון.
יש לוודא הצגת גילוי נאות טרם פתיחת היישום בדבר האחריות האישית וחובת שמירת הסודיות של המשתמש.	
לעובד המפלגה יינתן אישור גישה מרחוק רק ממכשיר קבוע, מוכר ומאובטח. חובה לוודא שכלל המכשירים המשמשים להתחברות מרחוק עברו בדיקה מקדמית אשר כוללת וידוא גרסאות מעודכנות של מערכות ההפעלה, וידוא כי המכשיר אינו פרוץ, התקנת אנטי-וירוס, נעילת מכשיר וכו'.	
הגישה מרחוק תנוטר, תתועד ותופעל תחת מגבלת זמן (התנתקות אוטומטית בחלוף פרק זמן מוגדר ועבודה בשעות הפעילות המוגדרות).	מומלץ להגדיר נעילה אוטומטית לאחר 30 שניות.
לעובד המפלגה, חובה לוודא כי מכשיר הקצה המתחבר לא עבר פריצה (JailBreak\Root).	
לעובד המפלגה חובה לוודא כי במכשיר מוגדרת נעילת אבטחה (ביומטרי\סיסמה\תבנית\קוד).	
יש לחסום גיאוגרפית אפשרות חיבור מחו"ל.	
לעובד המפלגה אסור להשאיר את מכשיר הקצה ללא השגחה.	
יש לדווח מידית למנהלי הקמפיין על כל חשש לחדירה, העתקה או דליפה של מידע או דבר אחר שאינו שגרתי.	
יש להגדיר בקרה לביעור המידע ועותקיו לצמיתות בסיום השימוש.	
תקנה 15 - עריכת בחינה מוקדמת של התאמת האפליקציות והספקים להוראות הדין, חתימה על הסכם התקשרות מסודר עימם, ופיקוח ובקרה בפועל על פעולותיהם[10].	מומלץ כי נותני השירות הרלוונטיים יהיו מוסמכים בתקן ISO 27001 ובתקן ISO 27032.

[10] תקנה 15 לתקנות אבטחת המידע והנחיית רשם מאגרי המידע 2/2011 בעניין שימוש בשירותי מיקור חוץ : לחוק המלא.

דגשים למימוש הוראות התקנות	המלצות נוספות
על המפלגות לוודא כי השירות פותח מתחילתו ועד סופו על פי מתודולוגיית פיתוח מאובטח, באמצעות חברה בעלת רקורד ומוניטין בפיתוח תוכנה.	
תנאי-סף להתקשרות בין המפלגה לנותן השירות, יהיה קבלתו של דו"ח ביקורת או סקר סיכונים בנושא אבטחת מידע מהמחזיק.	
תקנות 5 ו-16 - ביצוע ביקורות וסקרי סיכוני אבטחה פנימיים למערכות המפלגה. חובה לוודא כי השירות עבר מבדק חדירות אפליקטיבי ותשתיתי וליקויים שנמצאו בו (ככל ונמצאו) תוקנו.	