הנחיות הגנת הפרטיות לקראת הבחירות לרשויות המקומיות

להלן יפורטו ההוראות החלות על המתמודדים בבחירות לרשויות המקומיות ואחרים (להלן – **המתמודד/ת** או **המתמודדים**),[1] בכללם מועמדים לראש הרשות המקומית ורשימות מועמדים למועצת הרשות, בכל הנוגע לאיסוף, עיבוד ושימוש במידע על הבוחרים בבחירות לרשויות המקומיות.

שימו-לב: ההוראות הן חובות שבדין, הנושאות עונשים בגין הפרתן.

- אין לעשות שימוש אסור במידע מפנקס הבוחרים. כל שימוש אחר, שאינו לשם התמודדות בבחירות לרשות המקומית (להלן - הבחירות) - אסור. גישה למידע בפנקס הבוחרים מוגבלת רק לצורך ההתמודדות בבחירות. **כל שימוש אסור עלול להוות עבירה פלילית הנושאת עמה עונש של עד 5 שנות מאסר.**
- כל פנייה ממוקדת במסגרת דיוור ישיר, מטעם המתמודד/ת המבוססת על פרופיל הנמען, תכלול את זהות הגורם מטעמו נשלחה ההודעה, ותצוין בה זכותו של הנמען לבקש להימחק ממאגר המידע שעל בסיסו נעשתה הפנייה. **העונש על הפרת הוראה זו עלול להגיע כדי קנס או מאסר של שנה.**
- **חל איסור על שימוש במידע מכל מאגר מידע המנוהל ברשות המקומית, לצרכי התמודדות בבחירות או לכל מטרה אחרת החורגת מהמטרות לשמן הוקם מאגר המידע מלכתחילה.** כל שימוש שכזה עלול להוות עבירה פלילית הנושאת עמה עונש של עד 5 שנות מאסר.
- הגישה למידע במאגר צריכה להיות מוגבלת רק על בסיס הרשאת-גישה בהתאם לתפקידו של בעל ההרשאה, ובהתאם לצרכי התפקיד (need to know basis).
- יש לקבוע מראש מי יהיו מורשי הגישה למערכות המידע ולהדריכם בהתאם להוראות אלו.
- יש לערוך יומן לכל מורשי הגישה, שכולל: שם מלא של בעל ההרשאה, תפקידו, המערכות אליהן הוא רשאי לגשת, תאריך מתן הרשאה, תאריך סיום הרשאה. **כל שינוי בתפקידים ובהרשאות חייב להיות מתועד ביומן.**
- יש לתדרך את כלל העובדים (כולל עובדים זמניים, מתנדבים ופעילים) לשם הגברת המודעות לאבטחת המידע ולהגנת הפרטיות, לקיומן של מגבלות גישה למערכות המידע, ולחובת דיווח מיידי לרשימה בכל חשש לחריגה מהנחיות אלו.
- יש להדגיש בפני כל העובדים את חובתם לשמור על סודיות המידע הנחשף בפניהם, ולהחתימם על התחייבות לסודיות.

[1] ההנחיות שלהלן מיועדות לרשויות מקומיות, למועצות מקומיות, לגופים המספקים לרשויות המקומיות שירותים, לעובדי הרשויות המקומיות, למועמדים לראש הרשות המקומית, לרשימות למועצת הרשות, למתנדבים, ולפעילים בבחירות לרשויות המקומיות. מטרתן להבהיר ולחדד את החובות החלות עליהם מכוח חוק הגנת הפרטיות והתקנות, בכל הנוגע לשימוש במידע מכל מאגר מידע של הרשות המקומית. המידע המפורט להלן אינו מכיל את מלוא החובות הקבועות בדין, ואינו פוטר מהחובה להכיר ולקיים את מלוא הוראות הדין הרלוונטיות.

הפרת סודיות או גילוי המידע לגורם בלתי-מורשה הינן עבירות פליליות שדינן עד חמש שנות מאסר.

- בתום תקופת הבחירות יש לוודא כי קובץ פנקס הבוחרים, לרבות העתקיו המלאים, הושמד מכל אמצעי מדיה (לרבות כוננים קשיחים, אמצעי גיבוי וכל מדיה מגנטית או אופטית אחרת) ולהעביר על כך תצהיר חתום על ידי מורשה חתימה למפקח על הבחירות.
- על המתמודד/ת לוודא כי ברשותו/ה מסמך המאשר שגורם בעל הכשרה מתאימה ביצע ביקורת, המבטיחה את עמידתו/ה בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "תקנות אבטחת מידע" או "התקנות"), ומתעד את אופן ביצועה.

מה משמעות רמת האבטחה של המאגר?

על כל מתמודד/ת לקיים את כל הוראות התקנות הנוגעות למאגר מידע ברמת אבטחה **גבוהה או בינונית**, ובין היתר:

- **בהתקשרות עם ספק שירותים טכנולוגיים במסגרת 'מיקור חוץ' -**
  - יש לערוך <u>הסכם</u> שיכלול פירוט בנוגע למידע שהגורם החיצוני רשאי לעשות בו שימוש ומטרות השימוש המותרות בו לצורכי התקשרות המערכות של המתמודד/ת שהגורם החיצוני רשאי לגשת אליהן, סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות, משך ההתקשרות, אופן השבת המידע לידי המתמודד/ת בסיום ההתקשרות, מחיקתו על ידי הגורם החיצוני, דיווח על כך למתמודד/ת ועוד. על ההסכם לכלול התייחסות מפורשת למגבלות השימוש במידע מפנקס הבוחרים ולחובה לבער אותו או להחזירו עם תום מערכת הבחירות.
  - חובה עליכם להעביר לכל ספק שירותים טכנולוגיים את מסמך ההנחיות המצורף **<u>כנספח ג'</u>** למסמך זה.

לפני הבחירות, במהלכן ולאחריהן, חובה לדווח לרשות להגנת הפרטיות על כל חשד לאירוע אבטחת מידע חמור (כגון: אירוע כופרה או אירוע דלף מידע).

למידע נוסף - מוזמנים להיכנס לאתר הרשות בכתובת:

https://www.gov.il/he/departments/the_privacy_protection_authority/govil-landing-page

נספח א':

דרישות חוק הגנת הפרטיות לקראת הבחירות לרשויות המקומיות: מגבלות השימוש בפנקס הבוחרים ובמאגרי מידע ברשות המקומית ואחריות המתמודד/ת על אפליקציות וספקים חיצוניים

מבוא

1. בהליכי בחירות, בוודאי 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 לרשויות המקומיות, הרשות להגנת הפרטיות מזכירה למתמודדים בבחירות ולציבור הרחב את המגבלות החלות על שימוש במידע מפנקס הבוחרים ובסוגים אחרים של מידע שהמתמודדים אוספים במסגרת מסע הבחירות (הקמפיין), בהתאם להוראות חוק הרשויות המקומיות (בחירות), תשכ"ה-1965 (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 המתמודד/ת על הפרות ועבירות המבוצעות בידי קבלנים וספקים הפועלים מטעם המתמודד/ת או עבורם.
4. בדומה לתהליכים אחרים, גם עולם ניהול מסע בחירות לקראת מערכת בחירות הפך בשנים האחרונות לדיגיטלי, ומדי מערכת בחירות קמות חברות המתמחות ביצירת פלטפורמות לניהול הקשר עם הבוחרים.
5. בתוך כך, פועלות חברות אשר עוסקות במתן שירותים לרשימות 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 במתמודד/ת, התנדבות, סיוע למצביעים להגיע לקלפיות ועוד.
   5.5. אפשרות יצוא נתונים לצרכי ניהול מסע בחירות, 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.

<u>רקע נורמטיבי</u>

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

6. אינפורמציה הנוגעת לאנשים יחידים, הנאספת ומנוהלת בידי המתמודדים במסגרת מסע הבחירות, בעצמם 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 אבטחת מידע.
7. על ניהול מאגר מידע חלות הוראות פרק ב' לחוק הגנת הפרטיות ותקנות אבטחת מידע. המתמודדים הם "**בעל המאגר**" כמשמעותו בחוק, וככאלו הם הנושאים 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 שהמתמודדים וספקיהם מנהלים ומעבדים, וזאת <u>בנוסף</u> לחוק הבחירות ובמקביל להוראותיו.**[2]

<u>הוראות החוק הרלבנטיות</u>

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 85(ב) לחוק הבחירות, הקובע כי העושה שימוש במידע פנקס או המוסר מידע ממידע פנקס כהגדרתו בסעיף 16 שלא לצורכי התמודדות בבחירות או לצורכי קשר עם ציבור הבוחרים, דינו - מאסר שנתיים או קנס.
11. בנסיבות מסוימות הפרת עקרון צמידות המטרה 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.[3]
12. **בתוך כך, חל איסור על שימוש במידע מכל מאגר מידע המנוהל ברשות המקומית, לצרכי התמודדות בבחירות או לכל מטרה אחרת החורגת מהמטרות לשמן הוקם מאגר המידע מלכתחילה.** הפרתו היא עבירה פלילית לפי סעיף 2 לחוק הגנת הפרטיות, שעונשה עד 5 שנות מאסר.
13. לפי סעיף 17 לחוק הגנת הפרטיות, מוטלת על המועמדים, כבעלי המאגר, האחריות לאבטחת המידע המוחזק אצלם. תקנות אבטחת מידע מפרטות את עקרונות האבטחה הקשורים בניהול ובשימוש במידע השמור במאגרי מידע, דוגמת פנקס הבוחרים.
14. 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.

[2] תקנה 25 לתקנות אבטחת מידע קובעת במפורש כי התקנות "יחולו **<u>נוסף</u>** על הוראות בעניין אבטחת מידע בחיקוקים אחרים, זולת אם יש סתירה ביניהן".
[3] סעיפים 5 ו-31א לחוק הגנת הפרטיות.

15. על מאגרי מידע ברמת האבטחה הבינונית והגבוהה חלה חובת דיווח לרשות להגנת הפרטיות במקרה של אירוע אבטחה חמור, כהגדרתו בתקנה 1 לתקנות אבטחת מידע.[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 הוראות החוק הכלליות. להלן יפורטו דגשים והמלצות של הרשות בנושא:

<u>פירוט דרישות החוק</u>

17. מבלי לגרוע מכלליות האמור, מוטלת על המתמודד/ת האחריות המשפטית הישירה:
    17.1. להימנע מלעשות במידע מפנקס הבוחרים שימוש שאינו קשור להתמודדות בבחירות וליצירת קשר עם הבוחר, לרבות הימנעות מהעברתו לצד שלישי לשימושים אחרים.[5]
    17.2. להימנע מאיסוף מידע אישי ומכל שימוש בו, אשר חורגים מן המטרות להן הסכים האדם (נושא המידע) בעת שמסר את המידע על אודותיו.
    17.3. ניתן לאסוף שמות של צדדים שלישיים כתומכים פוטנציאליים במתמודד/ת, לרבות באמצעות אפליקציה. אולם, כאשר המידע על התומך הפוטנציאלי מבוסס על מידע שהתקבל מהאדם עצמו (נושא המידע), נדרשת הסכמתו לכך שהמתמודד/ת י/תאסוף מידע אודותיו, בין אם בדרך של הסכמה מפורשת כי המידע יועבר למתמודד/ת, לאחר שהוסברו לו המטרות והשימושים שייעשו במידע,[6] ובין אם בדרך אחרת ממנה ניתן להסיק בבירור על הסכמה משתמעת למסירת המידע, כגון במקרה בו אדם הביע באופן פומבי תמיכה מובהקת ומפורשת ברשימה מסוימת בפרופיל הפתוח שלו ברשת חברתית.
    17.4. ככל שמתמודדים מעוניינים לבצע איסוף מידע אודות תומכים פוטנציאליים באמצעות אפליקציה, עליהם להבהיר לכלל המשתמשים באפליקציה כי חלה חובה לקבל את הסכמתו של כל תומך פוטנציאלי לאיסוף המידע אודותיו ולשימושים במידע זה (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.
    17.5. להימנע מלעשות שימוש במידע אשר הגיע מפנקס הבוחרים שאינו הפנקס העדכני אשר קיבלו המתמודדת/ת מהמפקח על הבחירות לצורך בחירות אלה. **אין לעשות שימוש בפנקסי עבר, פנקסים מהבחירות הארציות וכדומה.**

[4] תקנה 11(ד)(1) לתקנות אבטחת מידע.
[5] סעיפים 2(9) ו-8(ב) לחוק הגנת הפרטיות.
[6] סעיף 11 לחוק הגנת הפרטיות.

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

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

17.6.2. 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.

17.6.3. יש לוודא שמי שניגש למידע במאגר הוא עובד מורשה, ולשם כך יש לאמת את זהותו לפחות באמצעות סיסמא חזקה.

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

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

17.6.6. תקנה 6 - יש לוודא את האבטחה הפיזית של מערכות המידע המכילות את המאגר.

17.6.7. תקנה 7 - דווקא בשל העומס הרב שמאפיין את תקופת הבחירות והשימוש בעובדים זמניים ובמתנדבים, על המתמודד/ת 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.

17.6.8. תקנה 11 - חלה חובת דיווח מיידי לרשות להגנת הפרטיות על אירועי אבטחה חמורים.[7]

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

17.6.10. תקנה 14 - אבטחת תקשורת ורשתות.

17.6.11. תקנה 15 - עריכת בחינה מוקדמת של התאמת האפליקציות והספקים להוראות הדין, חתימה על הסכם התקשרות מסודר עימם, ופיקוח ובקרה בפועל על פעולותיהם.[8] דרישה מקדמית לכל התקשרות בין המתמודד/ת לבין נותן השירות, תהיה קבלתו של דו"ח ביקורת או סקר סיכונים בנושא אבטחת מידע מהמחזיק.

17.6.12. תקנות 5 ו-16 - ביצוע ביקורות וסקרי סיכוני אבטחה פנימיים למערכות המתמודד/ת.

17.7. 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.[9] להרחבה ראו הנחיית רשם מאגרי מידע

---

[7] לדוגמאות של אירועי אבטחה חמורים ראו: https://www.gov.il/he/Departments/General/data_security_report_examples

[8] תקנה 15 לתקנות אבטחת המידע והנחיית רשם מאגרי המידע 2/2011 בעניין שימוש בשירותי מיקור חוץ: https://www.gov.il/he/departments/policies/outsourcing.

[9] סעיף 2א1 לחוק הבחירות (דרכי תעמולה), התשי"ט-1959, 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.

מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר".[10]

<u>שימוש במידע מפנקס הבוחרים</u>

בתום הבחירות יש לבער את כל עותקי פנקס הבוחרים שנמצאים אצל המתמודדים, ולוודא ביעור עותקי הפנקס אצל כל הספקים של המתמודדים, הפועלים במיקור חוץ.

18. סעיף 11(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.
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 (להלן: "**מידע פנקס**").
20. לקראת הבחירות, מוסר משרד הפנים למתמודד/ת, מידע פנקס באמצעי אלקטרוני או מגנטי, בהתאם להוראות סעיף 16 לחוק הבחירות. שר הפנים רשאי להורות, כי באמצעי האלקטרוני או המגנטי ייכלל אמצעי הגנה, לרבות הוספת מידע לזיהוי הקובץ ("סימן מים").
21. סעיף 16(ה) לחוק הבחירות קובע, כי שר הפנים יודיע לרשות להגנת הפרטיות לאילו מתמודדים נמסר הפנקס.
22. עם תום תקופת הבחירות, על המתמודד/ת להחזיר את מידע הפנקס ליחידת הפיקוח הארצי על הבחירות או לבער אותו.

(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.

(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".

[10] הנחיית רשם מאגרי מידע מספר 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר", זמינה בקישור: https://www.gov.il/he/departments/policies/direct_mail_2.

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

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

24. **הרשות מבהירה כי האחריות לקיום הוראות חוק הגנת הפרטיות וחוק הבחירות מוטלת בראש ובראשונה על המתמודדים עצמם. המתמודדים הם "בעלי המאגר" אשר עלולים לשאת באחריות פלילית או אזרחית, <u>גם להפרות שיבוצעו באפליקציה או בידי ספק שירות חיצוני עבור</u> המתמודדים <u>או מטעמם.</u>**

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

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

26. 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.

נספח ב':

דרישות חוק הגנת הפרטיות לקראת הבחירות לרשויות המקומיות: מגבלות השימוש בפנקס הבוחרים ובמאגרי מידע אחרים ואחריות המתמודדים על אפליקציות וספקים חיצוניים

טבלת דגשים בהיבטי אבטחת מידע

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 המתמודדים 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.	
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 המתמודדים 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).
תקנה 14 - אבטחת תקשורת ורשתות. יש לאבטח את התקשורת של משתמשי האפליקציה והאתר לשם הגנה על מערכות מאגר המידע. במקרה של משתמש שאינו מועסק בידי המתמודד/ת כעובד, 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.

דגשים למימוש הוראות התקנות	המלצות נוספות
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. למועסק בידי המתמודד/ת 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 שהמועסק בידי המתמודד/ת 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).	
גישה תוענק על בסיס מדיניות הרשאות קפדנית והצורך לדעת בלבד (Need To Know).	למועסק בידי המתמודד/ת 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.	
למועסק בידי המתמודד/ת 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.
למועסק בידי המתמודד/ת, חובה לוודא כי מכשיר הקצה המתחבר לא עבר פריצה (JailBreak\Root).	

דגשים למימוש הוראות התקנות	המלצות נוספות
למועסק בידי המתמודד/ת חובה לוודא כי במכשיר מוגדרת נעילת אבטחה (ביומטרי\סיסמה\תבנית\קוד).	
יש לחסום גיאוגרפית אפשרות חיבור מחו"ל.	
למועסק בידי המתמודד/ת 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.[11]	מומלץ כי נותני השירות הרלוונטיים יהיו מוסמכים בתקן ISO 27001 ובתקן ISO 27032.
על המתמודדים לוודא כי השירות פותח מתחילתו ועד סופו על פי מתודולוגיית פיתוח מאובטח, באמצעות חברה בעלת רקורד ומוניטין בפיתוח תוכנה.	
תנאי-סף להתקשרות בין המתמודד/ת לבין נותן 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 המחשב של המתמודד/ת. חובה לוודא כי השירות עבר מבדק חדירות אפליקטיבי ותשתיתי וליקויים שנמצאו בו (ככל ונמצאו) תוקנו.	

[11] תקנה 15 לתקנות אבטחת המידע והנחיית רשם מאגרי המידע 2/2011 בעניין שימוש בשירותי מיקור חוץ: https://www.gov.il/he/departments/policies/outsourcing.

נספח ג':

הנחיות לספק או לחברה המספקים שירותים טכנולוגיים למתמודדים

להלן יפורטו ההוראות החלות על מחזיק במאגר מידע הכולל **מידע** על בוחרים: **זכות הבחירה, כתובתם, מקום הצבעתם וכן מידע רגיש נוסף (מידע רפואי, דעות פוליטיות וכו').**

שימו לב: ההוראות הן חובות שבדין, הנושאות עונשים בגין הפרתן.

1. **מידע שמתקבל ממתמודד/ת ינוהל בנפרד מכל מידע של כל לקוח אחר**. ההפרדה תתבצע ברמה הפיזית או לכל הפחות ברמה הלוגית במסגרת סגמנטציה הכוללת שימוש בחומת אש, כלי ניטור ובקרת גישה (לרבות מנגנון אימות דו-שלבי). יש לוודא שכל אמצעי טכנולוגי הרלוונטי לביצוע ההפרדה, מוגדר ומוקשח לפי הפרקטיקה המקובלת. יש לנהל רשימת מצאי של כל האמצעים הנ"ל תוך פירוט סוג וגרסה.
2. הגישה למידע של מתמודד/ת צריכה להיות מוגבלת רק לצורך ביצוע השרות שלשמו נשכרו שירותכם.
3. יש לקבוע מראש מי יהיו מורשי הגישה למערכות המידע ולהדריכם בהתאם להוראות אלו.
4. יש לערוך יומן מורשי גישה הכולל - שם מלא, תפקיד, המערכות אליהן רשאי לגשת, תאריך מתן הרשאה, תאריך סיום הרשאה. **כל שינוי בתפקידים והרשאות חייב להיות מתועד ביומן.**
5. יש לתדרך את כלל העובדים (כולל עובדים זמניים ומתנדבים) למודעות לאבטחת המידע והגנת הפרטיות, לקיומן של מגבלות גישה למערכות המידע וחובת דיווח מיידי למתמודד/ת בכל חשש לחריגה מהנחיות אלו.
6. יש להדגיש בפני כל העובדים את חובתם לשמור על סודיות המידע, ולהחתים אותם על התחייבות בעניין זה.

בתום תקופת הבחירות או ההתקשרות יש לוודא כי כל המידע שהתקבל מהמתמודד/ת הושמד מכל אמצעי המדיה (לרבות כוננים קשיחים, אמצעי גיבוי וכל מדיה מגנטית או אופטית אחרת) ולהעביר על כך תצהיר חתום על ידי מורשה חתימה למתמודד/ת.

שימו לב: הפרת חובת הסודיות, או שימוש במידע שלא למטרת ההתמודדות במערכת הבחירות עלולים להוות עבירות פליליות שדינן עד חמש שנות מאסר.

7. אם אתם מעוניינים להעניק שירות טכנולוגי בשיתוף פעולה עם חברה נוספת אחרת, עליכם לבקש את אישור המתמודד/ת לכך, בכתב ומראש. יש לציין את פרטי הקשר של קבלן המשנה, מהות תפקידו, פירוט מערכות המידע וההרשאות להן הוא זקוק, ותצהיר/אסמכתא מגורם בעל הרשאה מתאימה בדבר ביקורת על עמידה בתקנות אבטחת מידע, לרבות מסמך בכתב המתעד את אופן ביצועה של הביקורת. יודגש כי גם קבלן המשנה כפוף להנחיות אלה.
8. **עליכם לדווח למתמודד/ת על כל מקרה של חשד לאירוע אבטחת מידע** (כגון: אירוע כופרה או אירוע דלף).
9. עליכם לוודא כי ברשותכם מסמך המאשר שבוצעה בידי גורם בעל הכשרה מתאימה ביקורת המבטיחה את עמידתכם בתקנות אבטחת מידע, ומתעד את אופן ביצועה.

נספח ד':

הנחיות להדרכת עובדים ומתנדבים בתקופת בחירות

1. יש לוודא שהגדרת התפקיד הולמת לממלא התפקיד וכי הוא מקבל גישה והרשאות רק למידע הנחוץ לו לצורך ביצוע תפקידו הספציפי.
2. טרם מתן אישור הגישה למערכות המידע הרלוונטיות, יש להדריך את העובד (לרבות מתנדב) בנושא עקרונות הגנת המידע והפרטיות, ובמסגרת זו לוודא מודעות לסיכונים ולתרחישים שבהם מידע עלול להיחשף לגורם בלתי מורשה. **העברת מידע לגורם בלתי מורשה, או חשיפה של מידע שלא למטרת התמודדות בבחירות, עלולה להוות עבירה פלילית שדינה עד חמש שנות מאסר.**
3. יש לוודא כי העובד מבין את האיסור הגורף על העברת סיסמאות או פרטי גישה למערכות המידע לאחר. עובד לא יוכל לאפשר גישה למערכות מידע. **הפרת חובת סודיות זו עלולה להגיע כדי עבירות פליליות שדינן עד חמש שנות מאסר.**
4. חובה על עובד לדווח מיידית לממונה עליו על כל חריגה שלו או של אחרים מהוראות אלה.
5. האחריות על מידע שהעובד נושא על גבי כל התקן או פורמט (מחשב נישא, דיסק און קי, טאבלט, ניירת וכיוצא באלה) הינה של העובד.
6. יש לוודא כי העובד השיב או השמיד כל מידע אישי שהועבר אליו בכל צורה - דיגיטלית או פיזית. על העובד לחתום על הצהרה בעניין.
7. על כל עובד לחתום על נספח העסקה הכולל לכל הפחות הוראות אלה, מבלי לגרוע מיתר חובותיו לפי כל דין.