הנחיות הרשות להגנת הפרטיות
למפלגות לקראת הבחירות לכנסת ה-26

ppa@justice.gov.il | 073-3928529 | *3103
שד' וולפסון 2, קריית הממשלה, ירושלים, ת"ד 49029, מיקוד 9149001
www.go.gov.il/ppa

תוכן עניינים

הנחיות למפלגות לקראת הבחירות לכנסת ה-26:
דרישות חוק הגנת הפרטיות, מגבלות השימוש בפנקס הבוחרים 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-26, 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 האישי, 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 זה מכבר 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 הכרוכים בעיבוד מידע אישי.

שימוש במידע מפנקס הבוחרים

6. 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.

7. 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**").

8. 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").

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

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

<u>רקע נורמטיבי</u>

<u>הוראות החוק הרלוונטיות</u>

11. בחוק הגנת הפרטיות "**מידע אישי**" מוגדר **ככל פריט אינפורמציה מכל סוג הנוגע לאדם הניתן לזיהוי**.[1]

12. אוסף פרטי מידע אישי הנאספים, מוחזקים או מעובדים בדרך אחרת בידי מפלגות או למענן במסגרת קמפיין הבחירות, בעצמן או באמצעות נותני שירות או אפליקציות חיצוניות, הוא "**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 המידע**").

13. על ניהול מאגר מידע חלות הוראות פרקים ב', ו-ד' עד ה' לחוק הגנת הפרטיות ותקנות אבטחת מידע. זאת בנוסף להוראות פרק א' לחוק האוסרות על פגיעה בפרטיותו של אדם, גם שלא במסגרת ניהול מאגר מידע. המפלגות הן "**בעל שליטה במאגר**" כהגדרתו בחוק, וככאלו הן הנושאות באחריות העיקרית לקיום הוראות החוק והתקנות שמכוחו.

14. נותן שירות חיצוני המעבד מידע אישי עבור המפלגות (לרבות ספק אפליקציית בחירות) הוא "**מחזיק**" כהגדרתו בחוק הגנת הפרטיות, הכפוף גם הוא למרבית הוראות החוק והתקנות שמכוחו.

[1] "מידע אישי" שהחוק חל עליו, מוגדר בסעיף 3 לחוק כדלקמן: "נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי; לעניין הגדרה זו "אדם הניתן לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי".

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

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

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

17. **<u>שימוש במידע:</u>** חוק הגנת הפרטיות קובע בסעיף 2(9) את עקרון צמידות המטרה, דהיינו שהשימוש בידיעה על ענייניו הפרטיים של אדם ייעשה רק למטרה שלשמה נמסר. כמו כן, סעיף 8(ב) לחוק קובע כי "לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין". עקרון צמידות המטרה קיבל ביטוי אף בסעיף 39(ג) לחוק הבחירות, הקובע במפורש כי אסור למפלגה או לסיעה לעשות במידע פנקס שימוש אחר, שאינו קשור להתמודדות בבחירות ולקשר עם הבוחר, לרבות העברתו לצד שלישי לשימושים אחרים.

18. שימוש במידע מתוך פנקס הבוחרים, כגון רשימת בעלי זכות הבחירה, למטרות אחרות מאלה שפורטו בסעיף 39(ג) לחוק הבחירות, מהווה עבירה שדינה שנתיים מאסר, לפי סעיף 118א לחוק הבחירות. שימוש שכזה מפר גם את סעיף 8(ד)(1) לחוק הגנת הפרטיות אשר אוסר על בעל שליטה במאגר מידע להחזיק או להשתמש במידע אישי אשר נצבר או נאסף **בניגוד להוראות "כל דין אחר המסדיר עיבוד מידע"**. בנסיבות מסוימות הדבר יהווה גם עבירה של פגיעה בפרטיות לפי סעיף 2 לחוק הגנת הפרטיות, שדינה חמש שנות מאסר.[3]

19. כמו כן, נזכיר כי סעיף 16 לחוק הגנת הפרטיות קובע שגילוי מידע אישי 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.

20. **<u>אבטחת המידע:</u>** לפי סעיף 17 לחוק הגנת הפרטיות, מוטלת על המפלגות כבעלות השליטה במאגר האחריות לאבטחת המידע המוחזק אצלן. תקנות אבטחת המידע מפרטות את עקרונות האבטחה הקשורים בניהול ובשימוש במידע האישי השמור במאגרי מידע, דוגמת מידע מפנקס הבוחרים.

21. 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 מידע הכולל 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] סעיף 5 לחוק הגנת הפרטיות.

22. על מאגרי מידע ברמת האבטחה הבינונית והגבוהה חלה חובת דיווח לרשות להגנת הפרטיות במקרה של אירוע אבטחה חמור, כהגדרתו בתקנה 1 לתקנות אבטחת המידע.[4]

23. **<u>בינה מלאכותית:</u>** להסיר ספק, **כל הוראות חוק הגנת הפרטיות חלות** גם על איסוף ועיבוד של מידע אישי באמצעות מערכות בינה מלאכותית על ידי מפלגות או עבורן במסגרת מערכת הבחירות, כולל מידע אישי שנוצר בדרך של היסק או הערכה.[5]

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

עד כאן הוראות החוק הכלליות. להלן יפורטו דגשים והמלצות של הרשות:

<u>פירוט דרישות החוק</u>

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

24.1. **<u>איסוף ושימוש במידע:</u>** להימנע מלעשות במידע מפנקס הבוחרים שימוש שאינו קשור להתמודדות בבחירות לכנסת וליצירת קשר עם הבוחר, לרבות הימנעות מהעברתו לצד שלישי לשימושים אחרים.[6]

24.2. להימנע מאיסוף ומכל שימוש במידע אישי מכל סוג, אשר חורגים מן המטרות להן הסכים האדם (נושא המידע) בעת שמסר את המידע על אודותיו.

24.3. ניתן לאסוף שמות של תומכים פוטנציאליים במפלגה, לרבות באמצעות אפליקציה. אולם, כאשר המידע על התומך הפוטנציאלי מבוסס על מידע 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,[7] 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.[8]

כמו כן, ככל שמפלגה מעוניינת לבצע איסוף מידע אישי אודות תומכים פוטנציאליים, לרבות באמצעות אפליקציה, המפלגה **היא שנושאת באחריות** למתן הודעה כדין לפי סעיף 11 לחוק בכל פניה המבוצעת מטעמה לאדם לשם איסוף מידע אישי. עליה להבהיר

---

[4] תקנה 11(ד)(1) לתקנות אבטחת מידע.

[5] להרחבה ראו הנחיה בנושא תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית, שפרסמה הרשות להגנת הפרטיות (2025). ההנחיה פורסמה בשלב ראשון כטיוטה להערות הציבור, והיא זמינה כאן.

[6] סעיף 39(ג) לחוק הבחירות. ראו גם סעיפים 2(9), 8(ב) ו-8(ד)(1) לחוק הגנת הפרטיות.

[7] כנדרש בסעיף 11 לחוק הגנת הפרטיות. יצוין כי בתיקון 13 לחוק הגנת הפרטיות, שנכנס לתוקף ביום 14.8.25, נקבעו מספר **פרטים נוספים אותם יש לכלול בהודעה לפי סעיף 11**, לרבות תוצאת אי ההסכמה למסירת המידע וזהות בעל השליטה במאגר שאליו נאסף המידע. במסגרת אותו תיקון, נקבעה בחוק **עבירה חדשה** בסעיף 23נו, לפיו הפונה לאדם לקבלת מידע אישי לשם עיבודו במאגר מידע ומוסר לו פרטים לא נכונים, בניגוד להוראות סעיף 11 ובכוונה להטעותו, דינו – מאסר שלוש שנים.

[8] להרחבה בעניין אופן מתן הסכמה ראו גילוי דעת שפרסמה הרשות להגנת הפרטיות בנושא "הסכמה בדיני הגנת הפרטיות" (2026). גילוי הדעת זמין כאן.

לכלל הפעילים והמשתמשים באפליקציה מטעמה 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).

24.4. 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'.**

24.5. **<u>מינוי ממונה על הגנת פרטיות:</u>** למנות למפלגה ממונה על הגנת הפרטיות, לפי הוראות סעיף 17ב1(א)(4) לחוק הגנת הפרטיות, בכל מקרה שבו המפלגה אוספת ומעבדת מידע אישי בעל רגישות מיוחדת בהיקף ניכר, כגון מידע אישי על אודות דעותיו הפוליטיות של אדם.[9] **חובה זו תחול ביחס לרבות מן המפלגות המתמודדות בבחירות לכנסת, מאחר שאלו מעבדות מידע בעל רגישות מיוחדת בהיקף ניכר**.

24.6. כאשר המפלגה מחויבת למנות ממונה על הגנת הפרטיות, חובת המינוי תחול גם ביחס לכל ספק המעניק למפלגה שירותי מיקור חוץ שכוללים עיבוד מידע אישי, מאחר שהוא משמש כ"מחזיק" במאגרי המפלגה, לפי החוק. חובת המינוי עשויה לחול על הספק גם אם המפלגה אינה מחויבת בעצמה למנות ממונה על הגנת הפרטיות, זאת אם עיסוקו של המחזיק עצמו כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר, למשל אם הוא מספק שירותים למספר רב של מפלגות או גופים אחרים. הכל בהתאם להוראת סעיף 17ב1(א)(4) לחוק. ראוי כי המפלגה תוודא כי כל ספק המעניק לה שירותי מיקור חוץ הכוללים עיבוד מידע אישי בהיקף ניכר, מינה ממונה על הגנת הפרטיות.

24.7. **<u>אבטחת המידע:</u>** לקיים את כל הוראות תקנות אבטחת מידע הנוגעות למאגר ברמת אבטחה גבוהה או בינונית לפי התקנות, ובכלל זה ההוראות הבאות –

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

24.7.2. **יש לקבוע הרשאות גישה למאגר לכל עובד או מתנדב, 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.

24.7.3. יש לוודא שמי שניגש למידע במאגר הוא גורם מורשה, **ולכן יש לאמת את זהותו לפחות באמצעות סיסמא חזקה.**

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

[9] להרחבה על הנסיבות המחייבות מינוי ממונה על הגנת הפרטיות וחובות נוספות הנוגעות למינוי ממונה הגנה על הפרטיות ותפקידיו, ראו גילוי דעת בנושא מינוי ממונה על הגנת הפרטיות בארגון לפי דרישות תיקון 13, שפרסמה הרשות להגנת הפרטיות (2025). גילוי הדעת פורסם בשלב ראשון כטיוטה להערות הציבור, והוא זמין כאן.

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

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

24.7.7. 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.**

24.7.8. תקנה 11 – **חובת דיווח מיידי לרשות להגנת הפרטיות** על כל אירוע אבטחה חמור.[10]

24.7.9. תקנה 12 – מניעת העתקה וחיבור של התקנים ניידים.

24.7.10. תקנה 14 – אבטחת תקשורת ורשתות.

24.7.11. תקנה 15 – עריכת בחינה מוקדמת של התאמת האפליקציות והספקים להוראות הדין, **חתימה על הסכם התקשרות מסודר עימם**, ופיקוח ובקרה בפועל על פעולותיהם.[11] דרישה מקדמית לכל התקשרות בין המפלגה לבין נותן השירות, תהיה קבלתו של דו"ח ביקורת או סקר סיכונים בנושא אבטחת מידע מנותן השירות.

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

24.8. **<u>דיווח ישיר:</u>** קיום דרישות סימן ב' לפרק ב' בחוק הגנת הפרטיות בנושא דיווח ישיר. זאת בשים לב גם לסעיף 2א1 לחוק הבחירות (דרכי תעמולה), תשי"ט-1959 האוסר פרסום של תעמולת בחירות מבלי לנקוב בשם האדם האחראי להזמנתה. להרחבה ראו הנחיית הרשות להגנת הפרטיות מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיווח ישיר ושירותי דיווח ישיר".[12]

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

---

[10] לדוגמאות של אירוע אבטחה חמור המחייב דיווח מיידי לרשות, ראו: https://www.gov.il/he/Departments/General/data_security_report_examples

[11] תקנה 15 לתקנות אבטחת המידע. ראו גם הנחיית הרשות להגנת הפרטיות מס' 2/2011 "שימוש בשירותי מיקור חוץ לעיבוד מידע אישי". ההנחיה זמינה כאן.

[12] הנחיית הרשות להגנת הפרטיות מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיווח ישיר ושירותי דיווח ישיר", זמינה כאן.

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

25. 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 אף לפרק זמן קצר יותר.

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

27. **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 ובתקנות אבטחת מידע, הן ביחס לעמידתן בדרישות החוק בעצמן והן ביחס לספקים אליהם יועבר המידע, בכל הנוגע לטיפול בפנקס.**

28. הרשות מבקשת להזכיר כי בסעיף 23כו לחוק הגנת הפרטיות, אשר נכנס לתוקפו ביום 14.8.25 במסגרת תיקון מס' 13 לחוק, הוסמכה הרשות להטיל על בעלי שליטה ומחזיקים במאגרי מידע עיצומים כספיים בסכומים ניכרים, בגין הפרות של הוראות החוק ותקנות אבטחת מידע, לרבות הפרת ההוראות שפורטו במסמך זה לעיל.

<u>נספחים מעשיים – דגשים והמלצות</u>

29. מבלי לגרוע מכלל האמור במסמך זה ומן החובה לקיים את **מלוא** הוראות החוק ותקנות אבטחת מידע, הנספחים המעשיים שלהלן כוללים דגשים והמלצות מפורטות בנושאים הבאים:

29.1. **נספח א' – דגשים בעניין אבטחת מידע.** המלצות ודגשים (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;

29.2. **נספח ב' - מדריך עזר בעניין התקשרות של מפלגות עם ספקי מיקור חוץ לפי תקנה 15 לתקנות הגנת הפרטיות (אבטחת המידע);**

29.3. **נספח ג' - הנחיות לספקי שירותים טכנולוגיים למפלגות;**

29.4. **נספח ד' - הדרכת עובדים ומתנדבים בתקופת בחירות.**

נספח א' - דגשים והמלצות בעניין 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 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.	
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.
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://www.gov.il/he/service/report-of-data-breach	
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 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).	
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.[13]	מומלץ כי נותני השירות הרלוונטיים יהיו מוסמכים בתקן ISO 27001 ובתקן ISO 27032.
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.	

[13] בנוסף להוראות תקנה 15 לתקנות אבטחת המידע. ראו גם הנחיית הרשות להגנת הפרטיות מס' 2/2011 "שימוש בשירותי מיקור חוץ לעיבוד מידע אישי". ההנחיה זמינה כאן.

נספח ב' - מדריך עזר למפלגות בעניין התקשרות עם ספקי מיקור חוץ לפי תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע) [14]

1. כללי:

במסגרת פעילותן של מפלגות[15], ובפרט בתקופת בחירות, הן נדרשות לבצע מגוון פעולות תוך הסתייעות בנותני שירותים חיצוניים דרך מיקור חוץ (להלן: "**הספק**" **או** "**גורם חיצוני**"), להם ניתנת גישה למאגרי המידע של המפלגה הכוללים מידע אישי רב ורגיש על ציבור הבוחרים, לרבות מידע על דעותיו הפוליטיות של אדם, המוגדר בחוק הגנת הפרטיות, התשמ"א-1981 כ"**מידע בעל רגישות מיוחדת**".[16] השימוש בספקים טומן בחובו יתרונות רבים, ותורם לייעול תהליכי עבודה, בפרט כאשר עולה הצורך בנקיטת פעולות במסגרת זמנים תחומה וממוקדת, אך מנגד מגביר את סיכוני אבטחת המידע הרבים הטמונים, בין היתר, בסוגיות של גישת הספק למאגרי המידע של המפלגות, העברת המידע בין הספק למפלגות וסיום ההתקשרות בתום תקופת הבחירות.

ככלל, ספקים מתאפיינים בכך שאינם מהווים חלק בלתי נפרד מהמפלגה ואינם נמנים על עובדיה. זאת ועוד, ספקים נדרשים לתת שירות למספר ארגונים במקביל. מאפיינים אלו מעלים את רף הסיכונים בתחום הסייבר ואבטחת המידע. הסיכונים העיקריים נובעים מסוגיות הנוגעות למתן גישה לספקים למידע האישי המצוי במאגרי המידע של מפלגה, העברת מידע בין המפלגה לספק וסוגיות הכרוכות בסיום ההתקשרות ביניהם.

תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: "**התקנות**") – מטרתה להסדיר את אופן ההתקשרות בין ארגונים לבין גורמים חיצוניים (שאינם אדם יחיד), המספקים לארגונים שירותים הכרוכים במתן גישה למאגר המידע של הארגון והשימוש בו. הוראות התקנה רלוונטיות גם למפלגות, בעת שהן מתקשרות עם ספקים המקבלים גישה למאגרי המידע אשר בבעלותן ועושים בו שימוש במסגרת מתן השירות למפלגה.

מדריך זה מיועד באופן ספציפי למפלגות, ונועד לסייע להן בנוגע לפעולות הנדרשות מצדן לשם עמידה בהוראות תקנה 15 בנוגע להתקשרות עם ספק חיצוני, בפרט בתקופת בחירות הטומנת בחובה אתגרים ייחודיים.

---

[14] מדריך זה מתפרסם ככלי עזר ספציפי למפלגות. האמור בו אינו ממצה את דרישות תקנה 15 ואת חובות בעל שליטה במאגר מידע, ואינו פוטר את בעלי השליטה במאגרים מקיום כל הוראות חוק הגנת הפרטיות והתקנות מכוחו, בשים לב לנסיבות הספציפיות של כל מאגר מידע וכל שירות הניתן על ידי מפלגה.

[15] כהגדרתן בסעיף 1 לחוק המפלגות, תשנ"ב-1992.

[16] ראו סעיף קטן (7) בהגדרת "מידע בעל רגישות מיוחדת" בסעיף 3 לחוק הגנת הפרטיות. ראו גם הגדרת "מידע אישי" בסעיף 3 לחוק זה.

<u>הוראות תקנה 15 לתקנות מחילות חובות שונות כתנאי להתקשרות עם ספק חיצוני</u>:

א. יש לבדוק האם הסיכונים הכרוכים בהתקשרות עם ספק מאפשרים את ההתקשרות עמו.[17] על מנת לסייע למפלגה לבצע את הבדיקה, ניתן להיעזר בשאלון הבדיקה הממוקד המוצע **בנספח ב'1** ("שאלון עזר למפלגה לבדיקת היבטי אבטחת מידע של הספק"), ולהתאימו לטיב השירותים ולמהות המידע בו נעשה שימוש במסגרת ההתקשרות בין מפלגה לספק, תוך התחשבות בסיכונים הנובעים מהתקשרות זו. ניתן לדרוש מן הספק להשיב על השאלון בתצהיר. אם אחת או יותר מהתשובות לשאלות 1-10 לשאלון אינן חיוביות, או שהתשובות לשאלות 11-12 אינן שליליות – רצוי להעמיק את הבדיקה ובמידת הצורך לפנות להתייעצות עם הרשות, או להיעזר בשירותי יעוץ אבטחת מידע חיצוני ובלתי תלוי בספק.

ב. עם ניסוחם של נוהלי עבודה המסדירים את פעילות המפלגה, ועל מנת לעמוד בדרישות תקנה 15, על המפלגה לתת ביטוי לנושאים הקבועים בהוראות התקנה במסגרת נוהלי אבטחת המידע. כאשר ההתקשרות עם ספק נעשית לפרק זמן העולה על שנה, או שמדובר ב"ספק קבוע" הנותן את שירותיו למשך שנים ארוכות, על המפלגה לבצע בקרה ולפקח על אופן יישום הוראות ההסכם בינה לבין הספק. לשם כך, ניתן להיעזר בשאלון הבקרה התקופתית הממוקד לספקים קבועים **שבנספח ב'2** ("שאלון בקרה תקופתית לספקים קבועים"). יש להתאים שאלון זה לנסיבות הספציפיות של השירות הניתן ולמהות המידע בו נעשה שימוש במסגרת ההתקשרות, ולעשות שימוש באמצעי פיקוח נוספים ככל שעולה הצורך.[18]

ג. כאשר ההתקשרות עם הספק היא לתקופה קצרת מועד בתקופת הבחירות, על אמצעי הפיקוח והבקרה שמחויבת המפלגה לנקוט כלפי הספק לפי תקנה 15(א)(4) לכלול לכל הפחות קבלת התחייבות של הספק לדווח למפלגה באופן מיידי על כל חשש לאירוע אבטחת מידע בו מעורב הספק (גם במתן שירותים לגורמים אחרים), על כל הליך פיקוח שפתחה הרשות להגנת הפרטיות כנגד הספק, וכן על כל חשש להפרת הוראה אחרת של ההסכם בינו לבין המפלגה. בכל מקרה בו בעקבות התשובות לשאלון או לדיווחים המידיים עולה אצל המפלגה חשש להפרה של הוראות החוק והתקנות – עליה לפנות ולהיעזר בשירותי יעוץ אבטחת מידע חיצוני ובלתי תלוי בספק , או להיוועץ ברשות.

ד. יש לערוך הסכם כתוב ומחייב מבחינה משפטית בין המפלגה (בעלת מאגר המידע), לבין הספק, ולקבוע בו הנחיות מפורשות, בהלימה לסוגי השירותים הדרושים למפלגה ולטיב המידע בו נעשה שימוש במסגרת ההתקשרות. על כן, יש לאפיין את מהות השירותים הניתנים, את התהליכים הטכנולוגיים (מערכות המידע ונכסי המידע הרלוונטיים להתקשרות), את מורשי הגישה של הספק למערכות המידע הרלוונטיות ואופן מתן הגישה למידע, ולבסוף להסדיר את אופן שינוי או סיום ההתקשרות ואופן הטיפול במידע שהועבר לספק עם סיום ההתקשרות.

[17] ראו הוראות תקנה 15(א)(1) לתקנות.
[18] ראו הוראות תקנות 15(א)(2) ו-15(א)(3) לתקנות.

ה. בנוסף, לצורך בדיקת סיכוני אבטחת המידע הכרוכים בהתקשרות עם הספק, כנדרש בתקנה 15(א)(1), ניתן לעשות שימוש גם בשאלוני העזר המצויים **בנספח ב'3** ("שאלוני עזר ממוקדים לספקים") לצורך בדיקת היבטי אבטחת המידע של ספקים הנותנים שירותי מחשוב שונים למפלגות.

2. <u>פירוט תוכן ההסכם המתחייב עם הספק על פי הוראות תקנה 15(א)(2) לתקנות:</u>

סעיפי תקנה 15(א)(2):	ביצוע	הערות
(א) המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות;	יש לנסח סעיפים המגדירים במפורש את סוגי המידע (לדוגמא: מידע על מתפקדים; מידע מפנקס הבוחרים; מידע על עובדי המפלגה) שאליהם רשאי הספק לגשת ואת מטרות השימוש לכל סוג של מידע (לדוגמא: דיוור ישיר; הצבעה מקוונת; טיוב מידע וכיו"ב).	
(ב) מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן;	יש לפרט על אודות מערכות המחשוב של מאגרי המידע אליהן הספק רשאי לגשת ועל אודות מורשי הגישה <u>מטעם הספק</u> המקבלים הרשאות גישה.	ניתן להסתייע במסמך מיפוי מערכות המאגר ומסמך הגדרות המאגר ולוודא כי הם מעודכנים.
(ג) סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות;	יש לפרט באופן מפורש אילו פעולות רשאי הספק לבצע ביחס למידע (לדוגמא: צפייה, כתיבה מחדש, שינוי וכיו"ב).	
(ד) משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל השליטה מאגר המידע;	יש לציין במפורש את מועד סיום ההתקשרות בין הספק לבעל המאגר. בהקשר זה, ראוי להבחין בין ספקים עמם מתקשרים לפרק זמן ממושך על מנת לקבל שירותים באופן קבוע ("ספקים קבועים") לבין ספקים עמם מתקשרים לתקופת זמן קצובה כגון תקופת בחירות. בהתאם לכך, יש לתת ביטוי במסגרת הוראות ההסכם למשך הזמן בו ניתנים השירותים, אם באופן קבוע או זמני. כמו כן, יש לתאר את האופן בו הספק ישיב או ישמיד את המידע	

סעיפי תקנה 15(א)(2):	ביצוע	הערות
	שקיבל מבעל המאגר עם תום ההתקשרות (לדוגמא: מחיקת קבצים ממערכות, דוא"ל, גיבויים ועוד; השבת התקן נייד עליו אוחסן מידע של בעל המאגר והועבר לספק). יש לוודא כי בתום ההתקשרות הספק מעביר דיווח לבעל המאגר הכולל אישור סופי ומחייב על ביצוע ביעור/מחיקה/השמדה/השבה של המידע הרלוונטי נשוא ההתקשרות.	
(ה) אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל השליטה במאגר המידע, אם קבע;	במקרים רבים, הגורם החיצוני עמו מפלגה בוחרת להתקשר (למשל: ספק שירותי אחסון בענן, ספק שירותי שיווק דיגיטלי מבוסס מידע דמוגרפי) ייחשב כ"מחזיק".[19] משכך, על ההסכם לפרט את אופן עמידתו בכלל החובות הקבועות בתקנות, לרבות מתן הנחיות פרטניות ליישומן, שכן הוראות החוק והתקנות מטילות אחריות ישירה על אבטחת מידע גם על המחזיק, לרבות חובת הדיווח המיידית לרשות להגנת הפרטיות על קרות אירוע אבטחת מידע חמור.	מומלץ לבדוק טרם ההתקשרות אם יש צורך בהעברת מידע אישי לספק דרך קבע או מתן הרשאת גישה **לזמן מוגבל** למשך תקופת ההתקשרות. מומלץ להיעזר בנספח ב'1 לבחינת סיכוני אבטחת המידע ולבקש מהספק תוצאות סקר סיכונים כמשמעותו בהוראות תקנה 5(ג) לתקנות.
(ו) חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה	יש לדרוש במסגרת ההתקשרות כי הספק יחתים את עובדיו על הסכם המעגן את חובותיהם לשמירה על סודיות המידע ועמידה בהסכם שנקבע בין בעל המאגר לספק.	

[19] על פי הוראות סעיף 3 לחוק, "מחזיק" הוא גורם חיצוני לבעל השליטה במאגר המידע המעבד בעבורו מידע.

סעיפי תקנה 15(א)(2):	ביצוע	הערות
הקבועים בהסכם כאמור בפסקת משנה (ה)		
(ז) התיר בעל שליטה במאגר מידע לגורם החיצוני לתת את השירות באמצעות גורם נוסף – חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו;	אם הספק נותן שירות באמצעות מיקור חוץ, עליו לחתום על הסכם עם אותו ספק משנה במיקור חוץ, בו יינתן ביטוי לכל העניינים המפורטים לעיל.	שימוש בספק משנה במיקור חוץ על ידי גורם חיצוני מעלה את רמת הסיכון הנובעת מההתקשרות ויש להביא זאת בחשבון בעת ביצוע ההתקשרות.
(ח) חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל השליטה במאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחת מידע	יש לקבוע סעיף המגדיר במפורש את אופן הדיווח על ידי הספק לבעל המאגר על אופן ביצוע חובותיו ועמידתו בכלל הוראות ההסכם, ובפרט דיווח על אירועי אבטחת מידע.	יש לוודא כי הגורם החיצוני מתעד ומנהל מקרים בהם התרחש אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה או לאי זמינות המידע באופן הפוגע ביישום ההתקשרות.

3. <u>מידע נוסף:</u>

ניתן למצוא פרסומים נוספים הכוללים הסברים ודוגמאות לדרישות החוק והתקנות ביחס לשימוש בשירותי מיקור חוץ הכרוך בגישה למידע אישי, באתר הרשות להגנת הפרטיות:

3.1. עמוד מידע בנושא אבטחת מידע בהתקשרות עם ספקים חיצוניים.[20]

3.2. עמוד שאלות ותשובות בנושא מיקור חוץ.[21]

3.3. פרק בנושא מיקור חוץ מתוך "המדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע)".[22]

יובהר, כי הנספחים להלן משמשים ככלי עזר בלבד, ואינם תחליף לעמידה בהוראות החוק והתקנות. על כל מפלגה, כבעלת מאגר מידע, לוודא כי היא ממלאת אחר כל היבטי אבטחת המידע אל מול ספק מיקור החוץ, ולהיעזר בגורמים מקצועיים ככל שעולה הצורך.

[20] ראו עמוד המידע בנושא אבטחת מידע בהתקשרות עם ספקים חיצוניים, זמין בקישור: https://www.gov.il/he/Departments/General/data_security_outsourcing

[21] ראו עמוד שאלות ותשובות באתר הרשות בנושא מיקור חוץ, זמין בקישור: https://www.gov.il/he/departments/guides/data_security_fqa?chapterIndex=5

[22] ראו הפרק בנושא מיקור חוץ, בתוך המדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע), הזמין בקישור: https://www.gov.il/he/Departments/Guides/data_security_guide?chapterIndex=17

נספח ב'1
שאלון עזר למפלגה לבדיקת היבטי אבטחת מידע של הספק

מס'	השאלה
.1	האם לספק יש קובץ נוהלי אבטחת מידע מעודכן?
.2	האם הספק מחזיק בתו תקן תקף בנושא אבטחת מידע בנוסף לעמידתו בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017? (לדוגמא: תקן ISO 27001).
.3	האם הספק מחזיק במסמך מיפוי מערכות הכולל פירוט של המערכות, השרתים, רכיבי הרשת והאפליקציות המצויים בסביבת השירות הנתמכת על ידו, בהתאם להיקף ההרשאות והשירותים שניתנו לו על ידי המפלגה, ובהתאם לתקנה 5 לתקנות?
.4	האם קיימת חלוקת אחריות ברורה בכל הקשור לניהול אבטחת המידע וההגנה על מאגרי המידע והגישה לסביבת הענן בין הספק לבין המפלגה? אם כן – מהי?
.5	האם הספק שומר לוגים ומנגנוני תיעוד עבור הפלטפורמות בהן הוא עושה שימוש, לרבות תיעוד מערכות ההגנה ואמצעי אבטחת המידע בהן הוא עושה שימוש לתקופה מינימאלית של 6 חודשים?
.6	האם לספק יש נוהל טיפול באירועי סייבר ונוהל או תוכנית עבודה להתאוששות מאירוע סייבר?
.7	האם הספק שומר עותק גיבוי למידע של הלקוחות מחוץ לחצרי הארגון כך שהוא לא מחובר לרשת המחשוב? אם כן, האם קיים נוהל מסודר אופן ביצוע הגיבויים והאם המידע מגובה ונשמר באופן מוצפן?
.8	האם מערכות ההפעלה של שרתי ותחנות הקצה של הספק מעודכנות ומאובטחות על ידי מערכת EDR או XDR.
.9	האם הספק משתמש בזיהוי דו שלבי (2FA) לצורך גישה מרחוק למאגרי המידע של לקוחותיו, והאם הגישה מתבצעת באמצעות תווך מאובטח שבו תעבורה מוצפנת?
.10	האם הספק מבצע בדיקות על ידי גורם חיצוני בלתי תלוי בנושא ניהול סיכוני אבטחת מידע?
.11	האם הספק עושה שימוש באמצעי ובמערכות הגנה לאבטחת מערך המחשוב, התקשורת והחיבור לסביבות לקוחותיו?
.12	האם התקיים אצל הספק בשלוש השנים האחרונות אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה (אירוע אבטחת מידע כמשמעותו בתקנה 11(א) לתקנות) או אירוע סייבר שפגע בתפקוד או בהמשכיות הפעילות העסקית שלו? אם כן נא פרט.
.13	האם התנהל כנגד הספק הליך פיקוח או אכיפה של הרשות להגנת הפרטיות או תביעה אזרחית בנושאי פרטיות או אבטחת מידע ב-3 השנים האחרונות?

נספח ב'2
שאלון בקרה תקופתית לספקים קבועים

מומלץ להעביר לספקים הקבועים מדי שנה ממועד ביצוע ההתקשרות את השאלון שלהלן, ובנוסף לדרוש דיווחים מיידים אם חל שינוי במצב העובדתי שעליו דווח בעת ההתקשרות:

מס'	השאלה
.1	האם בוצעו שינויים משמעותיים בתשתיות המחשוב או באמצעי ההגנה ואבטחת המידע של הספק? האם אלו נבדקו על ידי גורם חיצוני בלתי תלוי?
.2	האם הספק מחזיק בתו תקן תקף בנושא אבטחת מידע או הגנת הפרטיות בנוסף לעמידתו בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017? (לדוגמא: תקן ISO 27001, ISO 27701)
.3	האם הותלה או בוטל תו תקן כלשהו של הספק בשנה האחרונה?
.4	האם הספק קיבל תו תקן נוסף על עמידה בהוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 או האריך את תוקפו של תו תקן קיים?
.5	האם הספק חווה אירועי אבטחת מידע או אירוע סייבר, ובפרט כאלו המחייבים דיווח לרשות להגנת הפרטיות?
.6	האם נפתח הליך פיקוח או אכיפה מטעם הרשות להגנת הפרטיות או מתנהל הליך משפטי בנושאי פרטיות או אבטחת מידע כנגד הספק?
.7	האם הומצאה לספק הודעה על כוונת חיוב בעיצום כספי, התראה מינהלית, או הוראה להפסקת הפרה (פרק ד'3 לחוק הגנת הפרטיות)?
.9	האם חלה על הספק חובה למנות ממונה על הגנת הפרטיות (סעיף 17ב1 לחוק) וככל שחלה חובה, האם אכן מונה?
.10	האם במסגרת ההתקשרות הספק התקשר עם גורמים חיצוניים נוספים על מנת לספק את השירותים, ובהסכם עם הגורמים החיצוניים הנוספים נכללו כל הנושאים הנדרשים בהתאם להוראות תקנה 15 ועל פי ההתקשרות בין הספק לבעל המאגר?
.11	האם הספק עושה שימוש ברכיבי קוד פתוח במערכות המעבדות את מידע המאגר? ככל שכן, האם ניתן מענה הולם לסיכוני אבטחת מידע שכרוכים בשימוש בקוד הפתוח?[23]
.12	האם הספק עושה שימוש במערכות בינה מלאכותית (AI) בעיבוד מידע מהמאגר? ככל שכן, האם ניתן מענה הולם לסיכוני אבטחת המידע שכרוכים בכך?[24]

[23] למידע נוסף, ניתן לעיין במסמך הרשות בנושא "עקרונות לניהול סיכוני אבטחת מידע בשימוש בקוד פתוח" (2024). זמין כאן.

[24] ראו בעניין זה הנחיית הרשות להגנת הפרטיות בעניין "תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית", שפורסמה בשלב ראשון כטיוטה להערות הציבור. טיוטת ההנחיה זמינה כאן.

נספח ב'3
שאלוני עזר ממוקדים לספקים

מומלץ לעשות שימוש בשאלוני העזר להלן, ביחס לסוגי השירותים השונים הניתנים על ידי ספקים, על מנת לבדוק את היבטי אבטחת המידע ולהביא את העניינים המפורטים בהם לביטוי במסגרת הסכם ההתקשרות עם הספק.

ספק שירותי תמיכה טכנית

מס'	השאלה
.1	האם הספק מתקשר לסביבת המחשוב של המפלגה באופן מאובטח על ידי שימוש ב-VPN?
.2	האם החיבור בין הספק למפלגה לצורך מתן שירותי תמיכה באופן נקודתי מתבצע ביוזמת המפלגה והחיבור מנותק עם סיום מתן התמיכה?
.3	האם חומת האש (Firewall) של המפלגה מתעדת באמצעות לוג את חיבורי ה-VPN אל שרתי ומחשבי המפלגה והלוג נשמר לתקופה של 6 חודשים באחסון מקומי ומאובטח?[25] באופן דומה, האם מתבצע תיעוד מקביל אצל הספק?
.4	האם ניתן שם משתמש ייחודי לכל משתמש המספק שירותי תמיכה למפלגה? והאם מבוצע ניהול הרשאות בהתאם לתקנה 8 לתקנות?
.5	האם הזדהות הספק במסגרת ההתחברות אל סביבת המחשוב של המפלגה לצורך מתן שירותי תמיכה נעשית באמצעות מנגנון זיהוי רב שלבי (MFA) השולח סיסמה חד פעמית לטלפון נייד או לאפליקציית אימות?
.7	האם נחתם הסכם לשמירה על סודיות המידע בין המפלגה לבין הספק, והאם הוחתמו על כך גם בעלי ההרשאות אצל הספק? (תקנה 15(א)(2)(ו) לתקנות).
.8	האם במסגרת ההתקשרות הספק התקשר עם גורמים חיצוניים נוספים על מנת לספק את השירותים, ובהסכם עם הגורמים החיצוניים הנוספים נכללו כל הנושאים הנדרשים בהתאם להוראות תקנה 15 ועל פי ההתקשרות בין הספק לבעל המאגר?

ספק שירותי מחשוב ועיבוד מידע

מס'	השאלה
.1	האם מאגר המידע אשר מועבר לספק במסגרת ההסכם יוצפן באתר הספק ובמערכות המחשוב שלו?
.2	האם תוצרי העיבוד מועברים למפלגה בתווך מאובטח ומוצפן?

[25] ראו גם מדריך פעולה ליישום תקנה 10(ד) לתקנות הגנת הפרטיות (אבטחת מידע) לשמירת קבצי תיעוד ולוגים, שפרסמה הרשות להגנת הפרטיות (2024). המדריך זמין כאן.

.3	האם בתום עיבוד המידע הוא נמחק ממערכות המחשוב של הספק, לרבות ממערכות הגיבוי של הספק, והאם הספק מספק אישור בכתב על השמדת המידע (תקנה 15(א)(2)(ד) לתקנות)?
.4	האם נחתם הסכם לשמירה על סודיות המידע ועל אי שימוש בו שלא למטרות עיבוד המידע?

ספק שירותי מחשוב ואחסון בענן

מס'	השאלה
.1	האם הספק עושה שימוש בהמלצות השימוש המקובלות (best practices) העדכניות המפורסמות על ידי ספק שירותי הענן, בהגנה על מאגרי המידע המאוחסנים בענן בהתאם לרמת האבטחה של כל אחד ממאגרי המידע?
.2	מהי חלוקת האחריות בכל הקשור לניהול אבטחת המידע וההגנה על מאגרי המידע והגישה לסביבת הענן בין הספק לבין המפלגה (Shared Responsibility Model)?
.3	האם המידע מועבר לענן כשהוא מוצפן ובאמצעות תווך מאובטח ומוצפן? והאם מפתחות ההצפנה נשמרים בסביבה מוגנת ונפרדת מהמידע?
.4	האם הוגדרו תהליכים להחזרה/מחיקה של המידע בסיום ההתקשרות, ומתן אישור בכתב על השמדתו, לרבות מעותקי הגיבוי בענן?
.5	האם הוגדרו בקרות גישה זהותיות (IAM) הכוללות הזדהות רב-שלבית (MFA) למורשי הגישה, ועיקרון ההרשאה המינימלית?

ספק שירותי דיוור ישיר

מס'	השאלה
.1	האם מאגר המידע של המפלגה אשר יועבר לספק יוצפן באתר הספק?
.2	האם בתום מתן השירות המידע נמחק מסביבת המחשוב של הספק, לרבות ממערכות גיבוי של הספק?
.3	האם קיים הסכם לשמירה על סודיות המידע ועל אי שימוש בו שלא למטרת מתן שירותי דיוור ישיר?
.4	האם הספק פועל בהתאם להנחיית הרשות להגנת הפרטיות מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר"?
.5	האם הספק שומר רישום של מקורות המידע שמהם נאסף המידע, כנדרש בסעיף 17ה לחוק, ומספק את המידע על מקור הנתונים לדורש?
.6	האם קיים אצל הספק מנגנון לטיפול בבקשות של מקבלי פנייה להימחק מן המאגר, בהתאם להוראות סעיף 17ו לחוק, והאם בקשות ההסרה מועברות למפלגה בצירוף המידע הנדרש לצורך הסרת האדם מן המאגר שממנו נשלחה הפנייה?

נספח ג' - הנחיות לספקי שירותים טכנולוגיים למפלגות

להלן יפורטו ההוראות החלות על מחזיק במאגר מידע הכולל **מידע אישי** על בוחרים: **זכות הבחירה, כתובתם, מקום הצבעתם ובמיוחד מידע בעל רגישות מיוחדת נוסף (מידע רפואי, דעות פוליטיות וכו').**

שימו לב, ההוראות הינן חובות שבדין הנושאות סנקציות בגין הפרתן !!!

1. **מידע שמתקבל ממפלגה ינוהל בנפרד מכל מידע של לקוח/מפלגה אחרת**. 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 מפלגה צריכה להיות מוגבלת רק לצורך ביצוע השירות שלשמו נשכרו שירותיכם.
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 למפלגה בכל חשש לחריגה מהנחיות אלו.
6. יש להדגיש בפני כל העובדים את חובתם לשמור על סודיות המידע, ולהחתים אותם על התחייבות בעניין זה.
7. **שימו לב, הפרת חובת הסודיות, או שימוש במידע שלא למטרת ההתמודדות במערכת הבחירות עלולים להוות עבירות פליליות שדינן עד חמש שנות מאסר.**
8. בתום תקופת הבחירות או ההתקשרות יש לוודא כי כל המידע שהתקבל מהמפלגה הושמד מכל אמצעי המדיה (לרבות כוננים קשיחים, אמצעי גיבוי וכל מדיה מגנטית או אופטית אחרת) ולהעביר על כך תצהיר חתום על ידי מורשה חתימה למפלגה.
9. אם אתם מעוניינים להעניק שירות טכנולוגי בשיתוף פעולה עם חברה נוספת אחרת, עליכם לבקש את אישור המפלגה 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 הגנת הפרטיות (אבטחת מידע), לרבות מסמך בכתב המתעד את אופן ביצועה של הביקורת. ויודגש, גם קבלן המשנה כפוף להנחיות אלה.
10. **עליכם לדווח למפלגה על כל מקרה של חשש לאירוע אבטחת מידע** (כגון: אירוע כופרה או אירוע דלף).

11. עליכם לוודא כי ברשותכם מסמך המאשר שבוצעה בידי גורם בעל הכשרה מתאימה ביקורת המבטיחה את עמידתכם בתקנות הגנת הפרטיות (אבטחת מידע), ומתעד את אופן ביצועה.
12. שימו לב! המשך שמירת מידע אישי שהתקבל ממפלגה תוך חריגה מהרשאת המפלגה, מהווה עבירה פלילית שדינה שלוש שנות מאסר והפרה חמורה שביצועה עלול לגרור גם הטלת עיצום כספי בסכום ניכר.

נספח ד' - הדרכת 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 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 המפלגה בבחירות, עלולה להוות עבירה פלילית שדינה עד חמש שנות מאסר.**
3. יש לוודא כי העובד מבין את האיסור הגורף על העברה לאחר של סיסמאות או פרטי גישה למערכות המידע. עובד אינו רשאי 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 וכיוצ"ב) הינה של העובד.
6. יש לוודא כי העובד השיב/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 הוראות אלה לפחות, מבלי לגרוע מיתר חובותיו לפי כל דין.