יום שלישי 11 פברואר 2020
ט״ז שבט תש״פ

<u>אחריות המפלגות לקיום הוראות חוק הגנת הפרטיות בשימוש באפליקציות ובספקים חיצוניים לצורך ניהול מערכת בחירות</u>

1. כמו תהליכים אחרים, גם עולם ניהול הקמפיינים לקראת מערכת הבחירות הפך בשנים האחרונות לדיגיטלי, ולצד כל מערכת בחירות קמות חברות המתמחות באספקת פלטפורמות לניהול הקשר עם הבוחרים.
2. 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 שבשנה האחרונה, לאור רצף מערכות הבחירות בישראל, אנו עדים לגידול משמעותי בפעילות בתחום, וכניסתן של חברות אלה לעולם האפליקציות לטלפונים הניידים.
3. אפליקציות אלו מציעות שירותים ושימושים שונים, ובין היתר:
   3.1. הנגשת פנקס הבוחרים למערכת ניהול ידע נוחה לשימוש.
   3.2. הוספת שדות מידע ממקורות שונים לשם ״טיוב״ המידע אודות בוחרים, כגון גילאים, שפות, מגדר וכו׳.
   3.3. הצלבת נתונים עם מאגרי מידע פתוחים ברשת כגון רשתות חברתיות ומאגרים שנרכשים מחברות אחרות.
   3.4. אפשרות יצירת קשר עם הבוחר לצרכי תמיכה במפלגה, התנדבות, סיוע למצביעים להגיע לקלפיות ועוד.

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

4. כל האינפורמציה הנאספת במהלך הפעלת אפליקציות הבחירות נחשבת למידע אישי המוגן בהוראות חוק הגנת הפרטיות, התשמ״א – 1981 (להלן: ״**חוק הגנת הפרטיות**״), וכפופה לחובות ולדרישות שמטיל החוק על ניהול ועיבוד של ״מאגר מידע״.
5. השימוש בנתונים שמקורם בפנקס הבוחרים, כפוף גם למגבלות המחמירות שמטיל חוק הבחירות לכנסת [נוסח משולב], התשכ״ט – 1969 (להלן: ״**חוק הבחירות**״).
6. **הרשות מתריעה כי האחריות לקיום הוראות חוק הגנת הפרטיות וחוק הבחירות מוטלת בראש וראשונה על המפלגות עצמן. המפלגות הן ״בעלי המאגר״ אשר לפי החוק, עלולות**

לשאת באחריות פלילית או אזרחית, לפי העניין, גם להפרות שיבוצעו באפליקציה או בידי ספק שירות חיצוני עבור המפלגות או מטעמן.

7. מידע מפורט על החובות והאיסורים המוטלים על המפלגות, כלול במסמך "**ריענון הוראות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה – 23: מגבלות השימוש במידע מפנקס הבוחרים ומגבלות השימוש במידע אישי**"[1], שפרסמה הרשות לאחרונה, ומפורט בהוראות החוק עצמן.

8. מבלי לגרוע מכלליות האמור, מוטלת על המפלגות ועל המתמודדים האחריות המשפטית הישירה:

8.1. **להימנע מלעשות במידע מפנקס הבוחרים שימוש שאינו קשור להתמודדות בבחירות** לכנסת ה- 23 וליצירת קשר עם הבוחר, לרבות הימנעות מהעברתו לצד שלישי לשימושים אחרים;[2]

8.2. **להימנע מלעשות במידע מכל סוג אחר שימוש שלא ניתנה לגביו הסכמה** של האדם הרלבנטי, **או שימוש החורג מההסבר שחובה לתת לאדם ממנו אוספים מידע,** בדבר מטרת השימוש ולמי ימסר;[3]

8.3. **להימנע מלעשות שימוש במידע אשר הגיע מפנקס בוחרים אשר אינו הפנקס העדכני אשר קיבלה המפלגה מהמפקחת על הבחירות לצורך בחירות אלה**. אין לעשות שימוש בפנקסי עבר (ואפילו לא מהבחירות הקודמות), מפנקסי בחירות לרשויות המקומיות וכדי.

8.4. לקיים את **כל הוראות תקנות הגנת הפרטיות (אבטחת מידע),** התשע"ז – 2017 הנוגעות למאגר ברמת אבטחה גבוהה או בינונית, לרבות –

8.4.1. תקנות 8-9 - **הגבלת הגישה למידע רק למורשי הגישה החיוניים ובהיקף הנדרש**:

8.4.1.1. יש לקבוע הרשאות גישה למאגר לכל עובד, רק במידה הנדרשת לו לצורך ביצוע תפקידו;

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

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

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

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

8.4.3. תקנה 7 – מיון והדרכת כוח אדם;

[1] https://www.gov.il/he/departments/publications/reports/elections_23
[2] סעיפים 2(9) ו – 8(ב) לחוק הגנת הפרטיות וסעיף 39(ג) לחוק הבחירות.
[3] סעיפים 1 ו – 11 לחוק הגנת הפרטיות

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

8.4.5. תקנה 12 - מניעת העתקה וחיבור של התקנים ניידים ;

8.4.6. תקנה 14 - אבטחת תקשורת ורשתות ;

8.4.7. תקנות 5, 16 - ביצוע ביקורות וסקרי סיכוני אבטחה ;

8.5. להגיש **בקשה לרישום מאגר המידע** המנוהל באפליקציה או בידי ספק השירות בפנקס מאגרי המידע ברשות להגנת הפרטיות ;

8.6. **קיום דרישות חוק הגנת הפרטיות בנושא דיוור ישיר -** חוק הגנת הפרטיות קובע, כי כל פנייה בדיוור ישיר תכלול 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״[4], וכן ראו ״קוים מנחים לרכישת מידע לצרכי דיוור ישיר״ שפרסמה הרשות.[5]

8.7. **עריכת בחינה מוקדמת של התאמת האפליקציות והספקים לציות להוראות הדין, חתימה על הסכם התקשרות מסודר עימם, ופיקוח ובקרה בפועל על פעולותיהם.**[6]

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

[4] https://www.gov.il/he/Departments/Policies/direct_mail_2.

[5] https://www.gov.il/BlobFolder/generalpage/buying_data/he/BuyingData_for_DirectMareketing-Dos_and_Dont's.pdf

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