**ריענון הוראות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה – 22**

**מגבלות השימוש במידע מפנקס הבוחרים ומגבלות השימוש במידע אישי**

1. לקראת הבחירות לכנסת ה-22, הרשות להגנת הפרטיות מבקשת להזכיר את המגבלות החלות על שימוש במידע מפנקס הבוחרים ועל השימוש במידע אישי שאוספות המפלגות עצמן על חבריהן, בהתאם להוראות חוק הבחירות לכנסת [נוסח משולב], התשכ"ט-1969 (להלן: "**חוק הבחירות**") וחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**").

נבקש לחדד את חובות אבטחת המידע החלות על המתמודדים והמפלגות, המגבלות על רכישת מידע, וכן את הוראות חוק הגנת הפרטיות בנושא פניות אל ציבור הבוחרים שהן בגדר דיוור ישיר ושירותי דיוור ישיר.

**שימוש במידע מפנקס הבוחרים**

2. 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.
3. 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. מידע נוסף שניתן ללמוד מקובץ זה הוא העובדה שכל הרשומים בו הם מעל גיל 18, ובין החיים (להלן: "**מידע פנקס**").
4. 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.
5. סעיף 39(ה) לחוק הבחירות קובע, כי שר הפנים יודיע לרשם מאגרי מידע לאילו מפלגות או סיעות נמסר הפנקס.
6. עם תום תקופת הבחירות, על המפלגה או הסיעה להחזיר את מידע הפנקס ליחידת הפיקוח הארצי על הבחירות.
7. 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.

8. המידע הנמסר לרשימות הוא למעשה מאגר מידע, כהגדרתו בחוק הגנת הפרטיות. אי לכך, חלות עליו הוראות פרק ב' לחוק הגנת הפרטיות, שעניינו הגנה על הפרטיות במאגרי מידע, לרבות חובת רישום המאגר. ככלל, בעל המאגר כמי שנושא באחריות העיקרית לקיום הוראות החוק ולרישום המאגר – יהיה המפלגה או הסיעה[1].

9. 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 סיעה לעשות במידע שימוש אחר שאינו קשור להתמודדות בבחירות ולקשר עם הבוחר, לרבות העברתו לצד שלישי לשימושים אחרים.

10. שימוש במידע פנקס, כגון רשימת הבוחרים למטרות אחרות מאלה שפורטו בחוק, הוא 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[2].

**<u>אבטחת המידע</u>**

11. לפי סעיף 17 לחוק הגנת הפרטיות, מוטלת על המפלגות גם האחריות לאבטחת המידע המוחזק אצלן. בחודש מאי 2018 נכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**התקנות**"), אשר מפרטות את עקרונות אבטחת המידע הקשורים בניהול ובשימוש במידע השמור במאגרי מידע, דוגמת פנקס הבוחרים.
התקנות 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. כמו כן, על מאגרי מידע ברמה הבינונית והגבוהה חלה חובת דיווח לרשות להגנת הפרטיות (רשם מאגרי המידע) במקרה של אירוע אבטחה חמור, כפי שמוגדר בתקנה 1 לתקנות.
מידע נוסף בנושא ניתן למצוא באתר הרשות להגנת הפרטיות: https://www.gov.il/he/Departments/Topics/data_security_privacy_protection_authority.

12. כמו כן, אנו מבקשים להזכיר, 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>דיווח ישיר</u>**

---

[1] אולם יש לבחון כל מקרה לגופו.
[2] סעיפים 5 ו – 31א לחוק הגנת הפרטיות.

13. על הודעות הנשלחות לבוחרים מטעם מפלגות, רשימות או מתמודדים יחידים, המפולחות על בסיס מאפיין אישי, חלות הוראות חוק הגנת הפרטיות בנושא דיוור ישיר.
14. החוק 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.
15. גם הפרת הוראות החוק בעניין דיוור ישיר עשויה להגיע כדי עבירה פלילית. להרחבה ראו הנחיית רשם מאגרי מידע מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר"[3].
16. דיני הדיוור הישיר חלים על **כל** פניה לאדם המתבססת על אפיון אישי, וזאת בכל מדיה, טכנולוגיה או פורמאט[4], לרבות בהודעות SMS, ברשתות חברתיות ובאפליקציות מסרים מיידיים. בניגוד להוראות חוק התקשורת בנושא "דואר זבל", הוראות חוק הגנת הפרטיות בנושא דיוור ישיר חלות גם על תעמולה פוליטית ולמעשה על כל סוג של פניה מפולחת לאדם, בלי קשר לתוכנה ולמהותה.

**מגבלות על רכישת מידע מסוחרי מידע**

17. חוק הגנת הפרטיות קובע עקרון בסיסי, לפיו אסור לעשות שימוש במידע אישי על אדם או לפרסם אותו, אלא אם הסכים האדם לשימוש במידע וכן נתן הסכמתו למטרה לשמה ייעשה השימוש. סחר במידע ללא שניתנה הסכמה כאמור, אינו חוקי.
18. הרשות להגנת הפרטיות מדגישה, כי על כל מי ששוקל להתקשר עם גורם המציע לו מידע אישי על אנשים, לוודא שמקורות המידע אותו הוא מציע הינם חוקיים.
19. שימוש לא חוקי במידע חושף את מוכרי המידע ורוכשיו לפעולות אכיפה והטלת סנקציות על ידי הרשות להגנת הפרטיות, ולתביעות אזרחיות מצד אלו שפרטיותם נפגעה. הרשות להגנת הפרטיות פירסמה כללי אצבע לבחינה טרם רכישת מידע[5] ואנו ממליצים לעיין בהם.

[3] https://www.gov.il/he/Departments/Policies/direct_mail_2.
[4] או ב "אמצעי אחר" – סעיף 17ג לחוק הגנת הפרטיות.
[5] https://www.gov.il/BlobFolder/generalpage/buying_data/he/BuyingData_for_DirectMareketing-Dos_and_Dont's.pdf