מחלקת אכיפה

הנחיות לספק או לחברה המספק/ת שירותים טכנולוגיים למפלגות

להלן יפורטו ההוראות החלות על מחזיק במאגר מידע הכולל **מידע אישי** על בוחרים: **זכות הבחירה, כתובתם, מקום הצבעתם וכן מידע רגיש 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 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 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.**

מחלקת אכיפה

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 עמידכם בתקנות הגנת הפרטיות (אבטחת מידע), ומתעד את אופן ביצועה.