הנחיית רשמת מאגרי מידע מס'

אחריות בעל מאגר מידע לקיום אמצעי אבטחה בעת מתן עיון במידע אישי באמצעות אתר אינטרנט או בהפצתו בדואר אלקטרוני

1. מטרה

1.1 מטרת ההנחיה להבהיר את עמדת רשמת מאגרי מידע ביחס לתחולת חובות אבטחת המידע לפי הוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן - **החוק**) לעניין עיון במידע באמצעות האינטרנט או הפצתו בדואר אלקטרוני.

2. רקע

2.1 בעלי מאגרים רבים מציעים ללקוחותיהם נושאי המידע לקבל דיווחים שונים הנדרשים לפי הדין או לפי הסכמי השירות באמצעות דואר אלקטרוני או באמצעות עיון באתר אינטרנט.

2.2 הנגשת השירות באמצעים טכנולוגיים, לרבות העברת וקבלת מידע, משרתת הן את האינטרסים של בעל המאגר והן את אלה של הלקוח המשתמש[1]. שימוש בדואר אלקטרוני או באינטרנט לקבלת מידע הינו בעל תועלות רבות לבעלי המאגרים ועשוי לסייע ללקוחות בתיוק ובאיחזור המידע. (ראו: ח"א 8010/02 המפקח על הבנקים נגד בנק הפועלים).

2.3 עם זאת, המידע המופץ באמצעים אלה הינו לעתים מסוגי המידע הרגישים ביותר שהחוק עוסק בהם, שכן מדובר במידע ממוסדות בריאות, חברות ביטוח וקופות גמל וכדומה.

2.4 סעיף 17 לחוק מטיל אחריות לאבטחת המידע על בעל מאגר מידע, מנהל מאגר מידע והמחזיק בו. אבטחת מידע מוגדרת בסעיף 7 לחוק כהגנה על שלמות המידע ומניעת חשיפתו, העתקתו או שימוש בו ללא רשות כדין. על הגורמים האחראיים לאבטחת המידע מוטלת החובה לנקוט בכל האמצעים הדרושים להשגת רמה נאותה של אבטחת מידע, לפי דרישות הדין.

2.5 כך, מול היתרונות הקיימים בהפצת מידע בדרך מקוונת עולה החובה להקפיד על הוראות סעיף 17 לחוק, שעניינן נקיטה באמצעים טכניים ונוהליים שימנעו עיון לא מורשה במידע.

[1] ח"א 8010/02 המפקח על הבנקים - בנק ישראל נ' בנק הפועלים, פסקה 2 לפס"ד.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

2.6 לעניין השימוש בדואר אלקטרוני לדיוור מידע אישי, יצוין כי ככלל, פרוטוקול SMTP התומך בדואר אלקטרוני אינו מספק רמת אבטחה גבוהה למידע אישי, וככלל הינו חשוף מאוד ליירוט ולשימוש לא מורשה[2]. באופן כללי ניתן לומר כי הפצת מידע בדואר אלקטרוני ללקוח מחלישה במידה משמעותית מאוד את מידת ההגנה שניתנת לאותו מידע, על ידי בעל המאגר.

2.7 בידי בעל המאגר מצויים הכוח והכלים לאבטח את השירות ולמנוע את מירב הסיכונים, וכן היכולת לפקח על פעילות המערכת. אי לכך עולה החשש מניצול פערי הכוחות והטלת אחריות בלתי הוגנת על הלקוח[3].

2.8 הטלת אחריות בלתי הוגנת על לקוח הינה בגדר תנאי מקפח אשר מגלם בתוכו הגנה יתירה על האינטרס של בעל המאגר[4].

2.9 בהתאם לכך הנחיה זו נועדה להבהיר את החובות החלות על בעל מאגר ועל מחזיק מטעמו, המספקים שירות של עיון או הפצה של מידע ללקוח.

2.10 יודגש עוד כי החובות החלות בתחום אבטחת המידע חלות ישירות על בעל המאגר והמחזיק, והוראות חוזיות או כתבי הסכמה לכאורה עליהם חותם לקוח אינם יכולים לפטור את בעל המאגר או המחזיק מחובותיהם בעניין זה. (וראו לעניין זה ח"א 8010/02 הנ"ל).

2.11 על בעל המאגר מוטלת החובה לספק פירוט ברור ומקיף ללקוח אודות מסגרת הסיכונים הכרוכה בשימוש במערכות טכנולוגיות עוד בטרם מתן הסכמתו לשימוש בה[5].

2.12 בהתאם לכך, על ארגון המבקש למקסם את התועלות של הפצת מידע בדרך אלקטרונית, לבחון את הסיכונים הנובעים מכך בהקשר של סוג המידע המופץ, ולנקוט אמצעים מתאימים למזעור סיכונים אלה.

2.13 על בעל המאגר לנקוט אמצעי זהירות סבירים בעת שימוש במערכות להעברת מידע לרבות ווידוא זהות הלקוח ומילוי אחרי הוראותיו[6].
אמצעים שיקדמו את האינטרסים של הצדדים מחד, ואשר לא יכבידו על מתן השירותים ע"י בעל המאגר מאידך[7].

---

[2] ניתן לומר שהוא דומה לפרוטוקול HTTP בכך שהוא לא מוצפן.
[3] ח"א 8010/02 המפקח על הבנקים - בנק ישראל נ' בנק הפועלים, פסקאות 24, 32 לפס"ד.
[4] ח"א 8010/02 המפקח על הבנקים - בנק ישראל נ' בנק הפועלים, פסקה 18 לפס"ד.
[5] ח"א 8010/02 המפקח על הבנקים - בנק ישראל נ' בנק הפועלים, פסקה 35 לפס"ד.
[6] ח"א 8010/02 המפקח על הבנקים - בנק ישראל נ' בנק הפועלים, פסקה 21 לפס"ד.
[7] ח"א 8010/02 המפקח על הבנקים - בנק ישראל נ' בנק הפועלים, פסקה 23 לפס"ד.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

2.14 מערכת אבטחת מידע יעילה תמשוך משתמשים פוטנציאליים שלא יירתעו משימוש ברשת האינטרנט. אבטחת נתונים בעת שימוש באינטרנט חייבת להבטיח שאך ורק אנשים מורשים ייחשפו לנתוני המידע, שהתקשורת תהיה בטוחה מחדירת וציתות גורם חיצוני, ושלא תתאפשר גישה לנתונים המועברים באופן בו צד שלישי יוכל לשנות את המידע האלקטרוני[8].

2.15 כאשר מדובר על גישה באמצעות אתר אינטרנט, באופן כללי, לעניין גישה מרחוק, יש לוודא כי תשויך זהות פיזית להרשאה כפי שהוגדרה במערכות המחשב של המאגר. קיימים מספר מנגנונים המאפשרים אימות זהות של משתמש: שם משתמש וסיסמה, אמצעי חומרה פיזי (כגון כרטיס חכם), וכדומה. יוזכר כי בעת מתן הרשאה לגישה מרחוק למידע במאגר מידע, יש לקיים את הוראות הנחית רשם מאגרי מידע 1-2010 בה נקבע כי אימות זהות של נושא מידע לצורך מתן גישה מרחוק למידע אודותיו או לצורך שחזור היכולת לגשת למידע, מחייב אימות הכולל נתון שידוע רק לנושא המידע ואינו נכלל בעותק מרשם האוכלוסין שנגנב והופץ.

2.16 כאשר מדובר על הפצה בדואר אלקטרוני יש לנקוט באמצעים משלימים משמעותיים יותר.

3. ההנחיה

3.1 עמדתה של רשמת מאגרי מידע היא שלאור תכלית החקיקה, הקשיים והסיכונים שתוארו לעיל, על בעל מאגרי מידע לפעול בהתאם לחלופות כדלקמן:

3.1.1 אין להפיץ דוחות אישיים הכוללים מידע בעל רגישות ממאגר מידע, כגון מידע רפואי או נפשי, מידע פיננסי ומידע הכולל נתוני מיקום או פירוט שיחות, באמצעות דואר אלקטרוני בלבד, ללא נקיטת אמצעי אבטחה נוספים כמפורט בהנחייה זו.

3.1.2 לאור הסיכונים הגלומים בהפצת מידע אישי רגיש באמצעות דואר אלקטרוני, או במתן גישה אליו באמצעות האינטרנט – יש לקבל תחילה את הסכמת הלקוח במתכונת של OPT IN.

3.1.3 על בעל מאגר או מחזיק המפיץ מידע בתקשורת מקוונת ללקוחותיו, להציג התמודדות נאותה עם הסיכונים הנובעים משיטת הפצת המידע, סוג המידע המופץ ורגישותו. לצורך כך על בעל מאגר לקיים דיון תקופתי בדרג מתאים בנושא זה, הסיכונים שאותרו ודרכי ההתמודדות עמם, לצורך מזעורם, ולתעד דיון זה.

[8] ח"א 8010/02 המפקח על הבנקים - בנק ישראל נ' בנק הפועלים, פסקה 15 לפס"ד.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

3.1.4 לעניין קיום הוראות הנחייה זו, בכפוף לסוגי מידע בעלי רגישות מיוחדת בהם יידרשו אמצעי אבטחה חמורים יותר, תראה הרשמת בעל מאגר המיישם את אחת השיטות המפורטות מטה, כמי שהציג התמודדות נאותה עם הסיכונים הנובעים מהפצת מידע אישי בתקשורת.

3.1.4.1 **חלופה א': הפצת המידע באמצעות אתר אינטרנט מאובטח של בעל המאגר**. על בעל מאגר מידע המבקש לשלוח מידע לנושא המידע, לעשות זאת באמצעות משלוח הודעה בדוא"ל המציינת כי קיים מידע חדש אודות נושא המידע. הגישה למידע תתאפשר באמצעות קישור לאתר בעל מאגר המידע. נושא המידע יוכל לעיין במידע באמצעות כניסה לאתר בעל מאגר המידע לאחר שהזדהה בהתאם לשיטת זיהוי מקובלת שנבחרה בשים לב לרמת הסיכון של השירות.

3.1.4.2 **חלופה ב': הצפנת המידע בעת המשלוח והתעבורה בהתאם לשיטה שמקיימת את הדרישות המצטברות הבאות:**

3.1.4.3 המידע מוצפן בשיטת הצפנה מקובלת[9].

3.1.4.4 גישה למידע נעשית באמצעות שימוש בקוד או סיסמא ייחודים הידועים ללקוח בלבד (ואינם נכללים בעותק מרשם האוכלוסין שנגנב והופץ).

3.1.4.5 הקוד או הסיסמא נמסרו ללקוח בדרך מאובטחת. (כגון בדואר, בהודעת סמס, בעת רישום פיזי לשירות וכדומה).

[9] פרוטוקול SMTP (MIME) הינו הרחבה של הפרוטוקול לצורך שליחת צרופות כגון קבצים ומדיה) אינו פרוטוקול מוצפן ולכן הורחב ל-S/MIME המאפשר בעצם לחתום צרופות מידע (אולם בגלל המגבלות הרבות לא נעשה בו שימוש רב) . להלן תיאור של סטנדרטים המשמשים להצפנה של תעבורת פרטוקולי דוא"ל שונים :
STARTTLS for IMAP and POP3 is defined in RFC 2595, for SMTP in RFC 3207

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

מידע לגבי ההנחיה

1. **מס' ההנחיה**:
2. **נושא ההנחיה**: אחריות בעלי מאגרי מידע על מסירה ושליחה מאובטחת של המידע אישי ללקוחות.
3. **תאריך פרסום**:
4. **בתוקף מתאריך**:
5. **חקיקה שאוזכרה**:
   א. חוק הגנת הפרטיות, התשמ"א-1981.
   ב. לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ב 2012.
6. **פסקי דין שאוזכרו**: אין.
7. **מאמרים שאוזכרו**: אין.
8. **הנחיות היועץ המשפטי לממשלה שאוזכרו**: אין.
9. **הנחיות רשם מאגרי המידע שאוזכרו**: הנחית רשם מאגרי מידע 2010-1.
10. **מילות מפתח**: מידע אישי, לקוחות, הפצה, מאגר מידע, אבטחת מידע.
11. **עדכונים**

גרסה	פרטים	תאריך

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il