

תיקון 13 לחוק הגנת הפרטיות

בא לציון גואל



ענר רבינוביץ'
מנכ"ל
PrivacyTeam



עו"ד אייל שגיא
שותף, ראש מחלקת משפט
וטכנולוגיה



AYR

עמר רייטר ז'אן שוכטוביץ ושות'

על מה נדבר?

סקירה כללית בלבד
רק של הדברים הבולטים או דוגמאות
מקריאה ראשונית
של חוק שעוד לא התפרסם סופית
יש דברים שתלויים בשר המשפטים
לא תחליף לייעוץ משפטי או בכלל

מה נשתנה?

הגדרות

תפקידים

חובת הרישום וחובת ההודעה

צמידות המטרה

הודעת פרטיות

סמכויות אכיפה

עיצומים כספיים

פיצויים ללא הוכחת נזק

תקופת התיישנות – רגילה (7 שנים במקום שנתיים)

כניסה לתוקף – שנה מיום הפרסום

מידע אישי, עיבוד

"מידע אישי" – נתון הנוגע לאדם מזוהה או לאדם 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).

"עיבוד, שימוש" – כל פעולה שמבוצעת על מידע אישי לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו או מתן גישה אליו. (לעניין חובות עיבוד – למעט אחסון באקראי ובתום לב)

"מידע רגיש במיוחד" – 12 קטגוריות

מידע רגיש במיוחד 1-7

מידע אישי שהוא / על:

1. צנעת חיי המשפחה של אדם, צנעת אישותו, נטייתו המינית

2. מצב בריאותו של אדם, ובכלל זה מידע רפואי

3. מידע גנטי

4. מזהה ביומטרי המשמש או מיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב

5. מוצאו של אדם

6. עברו הפלילי של אדם

7. דעותיו הפוליטיות או אמונותיו הדתיות של אדם או השקפת עולמו

מידע רגיש במיוחד – 8-12

8. הערכת אישיות מטעם גורם מקצועי שכדרך עיסוק מחווה דעתו על אישיותו של אדם או שנעשה באמצעי שמיועד לביצוע הערכה של מאפייני אישיות מהותיים, ובכלל זה קווי אופי, יכולת שכלית ויכולת תפקוד בעבודה או בלימודים
9. נתוני מיקום ונתוני תעבורה כהגדרתם בחוק סד"פ (סמכויות אכיפה – נתוני תקשורת) שנוצרו ע"י ספק מורשה (כהגדרתו בחוק האמור), לגבי אדם, ונתונים על אודות מיקומו של אדם שיש בהם כדי ללמד על מידע רגיש במיוחד (סוגים 1 עד 7 + 11)
10. נתוני שכר של אדם, פעילותו הפיננסית
11. מידע אישי שחלה עליו חובת סודיות שנקבעה בדין
12. מידע על חברות בארגון עובדים שהועבר לישראל מהאזור הכלכלי האירופי

בעשל"ט, מחזיק, מנהל

"בעל שליטה" במאגר מידע – מי שקובע, לבדו או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע

"מחזיק" – גורם חיצוני לבעל השליטה במאגר מידע המעבד מידע עבורו (ירד: "דרך קבע", ו"רשאי לעשות בו שימוש")

"מנהל מאגר" – בעל שליטה במאגר מידע (ולעניין גוף ציבורי – מנכ"ל הגוף שבבעלותו או בהחזקתו מאגר מידע או מי שהמנכ"ל הסמיכו לנהל את המאגר).

חובת רישום מאגר והודעה על מאגר

מאגר מידע חייב ברישום:

- דאטה ברוקרים (מטרה עיקרית של איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה), על יותר מ-10,000 בני אדם.
- בעל השליטה במאגר הוא גוף ציבורי (רחב...), אלא אם המאגר כולל מידע אישי על עובדי הגוף הציבורי בלבד.

מאגר מידע חייב בהודעה:

- מידע רגיש במיוחד על מעל ל-100,000 בני אדם
- הודעה בתוך 30 ימים על זהות בעל השליטה, מענו ודרכי ההתקשרות עימו, **על זהות ה-DPO** אם נדרש מינויו ודרכי ההתקשרות עימו, ומסירת העתק ממסמך הגדרות המאגר.

מאגר מידע שכבר לא חייב ברישום?

ניתן להודיע לרשות על כך שכבר לא חייב ברישום, והרשות תמחק את הרישום.

ביטול "מטרת הקמת המאגר"

הצמידות למטרת הקמת המאגר בוטלה, והוחלפה בצמידות למטרה שנקבעה לו כדין:
"לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין"

מי קובע את המטרה?
בעל(י) השליטה

מתי קובעים?
מתי שצריך מעת לעת

מה היא מטרה "כדין"?
שימו לב ל 2(9) ("ענייניו הפרטיים" + בהתחשב בסעיף 18), 11... מומלץ לערוך DPIA

מהו מאגר?
בעל(י) השליטה מחליטים – גמיש (בגבולות הסביר). האם לפצל?
יתרונות – הקמת מאגרים אד-הוק, הגבלת חשיפה (לפי כמות נושאי המידע).
חסרונות – חובת מינוי ממונה אבטחת מידע מעל חמישה מאגרים (גם לבעלי שליטה!); אדמיניסטרציה / תיעוד

הודעת פרטיות (סעיף 11)

- פניה לאדם לקבלת מידע אישי לשם עיבודו במאגר מידע תלווה בהודעה:**
- אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו **ומהי תוצאת אי-ההסכמה.**
 - המטרה אשר לשמה מבוקש המידע
 - **שמו של בעל השליטה ודרכי ההתקשרות עמו**
 - למי יימסר המידע ומטרות המסירה
 - **קיומן של זכות עיון וזכות לבקש תיקון**

וגם, למי שחלות עליו תקנות הגישור:

- יידוע גם במקרה של איסוף עקיף
- כתובת, סוג המידע שיועבר, קיומה של זכות לדרוש מחיקה של מידע עודף (וחלה גם חובה כזו...)
- ובמקרה של העברה לצד שלישי:
- הזאות ופרטי ההתקשרות של הצד השלישי או סוג הגורמים השלישיים שאליהם יועבר המידע

ממונה על הגנת הפרטיות

חובת מינוי ממונה על הגנת הפרטיות:

1. גוף ציבורי

2. דאטה ברוקר

3. חברה שעוסקת בעיבוד מידע רגיש במיוחד ב"קנה מידה גדול"

4. חברה שעוסקת בעיבוד מידע שמטרתו ניטור או מעקב באופן שיטתי ב"קנה מידה גדול"

תפקידו לפעול לקיום הוראות חוק הגנת הפרטיות וכן לקדם את השמירה על פרטיות ואבטחת המידע במאגרי המידע של הארגון

נדרש להיות בעל ידע מעמיק בדיני הגנת הפרטיות, הבנה הולמת בטכנולוגיה ואבטחת מידע וכן היכרות עם תחומי הפעילות של הגוף בו הוא ממלא תפקיד

יכול להיות גורם חיצוני לארגון

ממונה על אבטחת מידע

חובת מינוי ממונה על אבטחת מידע:

1. בעל שליטה או מחזיק של 5 מאגרי מידע החייבים ברישום או הודעה
2. גוף ציבורי
3. בנק, חברת ביטוח או חברה העוסקת בדירוג/הערכה של אשראי

נדרש להיות בעל "הכשרה מתאימה"
חובות ביצועיות תחת תקנות אבטחת מידע

סמכויות אכיפה / עיצומים מנהליים

פיקוח

בירור מנהלי

הוראה של ראש הרשות

צו הפסקה (דרך בימ"ש)

חובת פרסום הטלת עיצומים ע"י הרשות (שיימינג)

עבירות פליליות

עיצומים כספיים

”מחירון” (ולא טווח כמו בGDPR) – לפי גודל מאגר, לפי רגישות מאגר, לפי כמות נושאי מידע שנפגעו, כמעט ללא שק”ד לראש הרשות

תוספות על הפרה נמשכת, כפל על הפרה חוזרת

הפחתות שונות לבקשת המפר (70% מקסימום): 10% על מינוי ממונה הגנת פרטיות כשקיימת חובה; הפחתה ל 5% מהמחזור; עסקים קטנים; נסיבות אישיות; תשלום פיצוי בנזיקין

עיצומים על בעל שליטה ועל מחזיק

הפרה אחת / מסכת אחת = עיצום אחד

עיצומים על הפרת תקנות אבטחת מידע, הגישור, העיון – אבל לא תקנות יצוא מידע

ערעור על עיצום כספי – בימ”ש רגיל לפי גובה הסכום (שלום/מחוזי)

עיצומים על הפרת תקנות אבט"מ

תחולה וגובה עיצום ייקבעו בהתאם לרמת אבטחת המידע של המאגר וגודלו

מעל מיליון נושאי מידע במאגר שחלה עליו רמת האבטחה הגבוהה – כפל עיצום

בחלק מההפרות נדרשת התראה מנהלית בטרם הטלת העיצום
(מסמך הגדרות מאגר, יישום נוהל הרשאות גישה, הפרדה ומידור של מערכות)

בחוק יש תשתית להתראה מנהלית חלף הטלת עיצום – ממתין לשר המשפטים

דוגמאות לעיצומים

אי מסירת הודעה לרשות על מאגר החייב בהודעה, סירוב לבקשת עיון:
₪ 150,000

פנייה לאדם ללא הודעה כנדרש בסעיף 11 לחוק:
מכפלה של 50 ₪ במספר האנשים שאליהם נעשתה הפנייה (מידע רגיש: 100 ₪)

פנייה לאדם ללא הודעה כנדרש בסעיף 11 לחוק כשהפנייה נעשתה לקבוצה לא מסוימת
של אנשים:
מכפלה של 2 ₪ במספר נושאי המידע במאגר (מידע רגיש: 4 ₪)

אי קיום מנגנון למחיקת מידע עודף:
2 ₪ לאדם (4 ₪ לגבי מידע רגיש)

דוגמאות לעיצומים

עיבוד מידע אישי למטרה שאינה כדין:

מכפלה של 4 ש' במספר האנשים שמידע אישי אודותם נמצא במאגר (מידע רגיש במיוחד – 8 ש')

**עיבוד מידע אישי שלא בהתאם למטרה שנקבעה בנסיבות בהן ניתן היה לקבוע כדין מטרה =
אי הכנת/עדכון מסמך הגדרות מאגר:
במגה מאגר: 320,000 ש'**

אי ביצוע בדיקת מידע עודף:

במגה מאגר: 320,000 ש'

אי ביצוע סקר סיכונים / מבדקי חדירות:

במגה: 640,000 ש'

אי דיווח אודות אירוע אבטחה חמור:

במגה: 640,000 ש'

דוגמאות לעבירה פלילית

עיבוד מידע אישי ממאגר מידע בלא הרשאה מאת בעל השליטה:
מאסר שלוש שנים.

פנייה לאדם לקבלת מידע אישי לשם עיבודו במאגר, ומסירת פרטים לא נכונים בניגוד
להוראות סעיף 11, בכוונה להטעותו באשר למסירת המידע האישי:
מאסר שלוש שנים.

עיצומים על אי מינוי

DPO, על גופים ציבוריים (שימו לב להגדרה):

עיצום כספי

DPO, על גופים פרטיים:

אין עיצום, אבל... אם מונה DPO לפי החובה, מזכה בהנחה של 10% בעיצומים

במאגר שכפוף לרישום/הודעה, צריך לדווח גם על זהות ה-DPO ודרכי ההתקשרות עימו, אם נדרש מינוי (יש עיצום על הפרת חובת הדיווח...)

ממונה אבטחת מידע:

מכפלה של 2 ש' במספר נושאי המידע במאגר (מידע רגיש: 4 ש')
(שימו לב: חובת מינוי גם על בעלי שליטה עם יותר מחמישה מאגרים, והעיצום יחול על כל המאגרים במקרה כזה)

פיצויים לדוגמה

פיצויים שאינם תלויים בנזק, בסכום של עד 10,000 ש"ח:

- עיבוד במאגר שחב ברישום ולא נרשם, ובלבד שנושא מידע פנה לבעל השליטה בדרישה לרשום – וחלפו 90 ימים מיום פנייתו.
- פניה לקבלת מידע אישי לשם עיבודו במאגר מבלי למסור הודעת פרטיות כדין, ובלבד שנושא מידע פנה לבעל השליטה בדרישה להודיע – וחלפו 30 ימים מיום פנייתו.
- אי מתן עיון במידע אישי.
- הסכים לבקשה לתיקון/מחיקה של מידע אישי לא מדויק, אך לא ביצע את השינויים או לא הודיע עליהם לכל מי שקיבל ממנו את המידע.
- לא הודיע למבקש תיקון/ מחיקה על סירובו לעשות כן.
- גופים ציבוריים (הגדרה מורחבת): לא הודיע לראש הרשות על קבלה דרך קבע של מידע אישי

מה לעשות מחר?

לבחון מחדש את סוגי המידע שהארגון מעבד ועל כמה בני אדם לנוכח ההגדרות החדשות
למה למהר? החוק חל על כל מידע אישי, ורובו יוגדר רגיש. זה משליך על הכל, כולל הערכות טכנית בעיקר באבטחת מידע ובטיפול במידע עודף. המיפוי הוא הבסיס לעמידה בחוק.

לבדוק אם צריך יהיה למנות DPO ולהחליט אם למנות
למה למהר? כי ה DPO צריך להכין את הארגון לחוק החדש תוך שנה, ולא החל מעוד שנה. אפשר לשכור שירות, אבל אם לא, צריך לעמוד בתנאי הכשירות.

לסיים לטפל במידע עודף / מחיקת מידע (גם לגבי דיוור ישיר)
למה למהר? הטיפול מסובך משפטית (מתי מידע נחשב עודף?) ודורש פיתוח טכני ארוך (בעיקר במערכות מסובכות וותיקות). לא לשכוח את 1.1.25 למי שחל.

עדכון מדיניות פרטיות, פרסום פרטי קשר
למה למהר? הכנת הקרקע לשינוי מטרות גמיש (ולמאגרים משותפים, היערכות לטיפול בפניות (עיצומים ופיצויים תלויים במקרים רבים בפניה מוקדמת – שלא ילכו פניות לאיבוד). שינוי מטרה תלוי ביידוע – זה צריך להיעשות מראש.

לערוך רשימת מסמכים, בדיקות, רישומים שיידרשו
למה למהר? יש הרבה עבודה, ונדרשת עמידה מהיום הראשון של תוקף החוק (והכי קל לבדוק ציוד)

לבחון את ביטוחי הסייבר / אחריות מקצועית
למה למהר? מו"מ לוקח זמן, התנאים עלולים להחמיר

שאלות?



ענר רבינוביץ'
aner@privacyteam.com



אייל שגיא
eyals@ayr.co.il