אחריות
מנהלי מאגרים

Integrity
Consulting & Risk Management

רקע – חוק הגנת הפרטיות

- חוק הגנת הפרטיות התשמ"א 1981 ותקנות ההגנה על מאגרי מידע מחייבים שמירה קפדנית וחסיונם של הנתונים הפרטיים של אזרחי המדינה.
- החוק נועד להגן על הפרטיות של בני אדם אשר נתוניהם האישיים מצויים במאגרי המידע השונים.
- המועצה/רשות מנהלת מאגרי מידע המכילים מידע מוגן עפ"י הגדרתו בחוק זה, ועל כן חייבת לנקוט בשורה של צעדי הגנה ואבטחה המתחייבים מהחוק ומהתקנות.

הפרת חוק הגנת הפרטיות- בעבר

הטלת קנס מינהלי על עיריית רמת גן וקבוצת קידום

הרשות למשפט טכנולוגיה ומידע (רמו"ט) הטילה קנס מנהלי על עירית רמת-גן וקבוצת קידום בע"מ בגין שימוש שלא כדין במידע אישי על אודות תלמידים תוך פגיעה בפרטיותם

הרשות למשפט טכנולוגיה ומידע (רמו"ט) הטילה קנס מינהלי על עירית רמת-גן וקבוצת קידום בגין הפרות של חוק הגנת הפרטיות במסגרת פנייה בדיוור ישיר לתלמידי תיכון בעיר רמת-גן.

קנס בסך 5,000 ₪ הוטל על עירית רמת-גן בגין שימוש במידע אישי של תלמידים בניגוד למטרת מאגר המידע של העירייה שבו כלולים פרטיהם, ובניגוד למטרה לשמה נמסר לעירייה המידע.

קנס בסך 1,000 ₪ הוטל על קבוצת קידום, ששלחה דיוור ישיר מטעמה לתלמידי העיר רמת-גן, מבלי שצוין בו כל הנדרש בחוק.

הפרת חוק הגנת הפרטיות- בהווה

מצלמות בסמוך לתאי ההלבשה, ללא שילוט מתאים ברשת איתי ברנדס: הרשות להגנת הפרטיות הטילה קנס מינהלי של 35 אלף שקל על חברת איתי ברנדס (Itay Brands LTD) בשל הצבת מצלמות ברחבי חנויותיה בקניונים שבעת הכוכבים ורמת אביב, לרבות בסמוך לתאי הלבשה - ללא שילוט ובכך ללא יידוע הלקוחות.

ברשות להגנת הפרטיות מסרו כי הרשת יצאה בזול משום ש"לאחר כניסתו של תיקון 13 לחוק הגנת הפרטיות לתוקף בחודש אוגוסט הקרוב, העיצום הכספי שיחול בגין הפרות אלה יעמוד על מאות אלפי שקלים".

מהו מידע אישי ומהו מידע רגיש?

- **מידע אישי**: "נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי; לעניין הגדרה זו, "אדם הניתן לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות".
- **מידע בעל רגישות מיוחדת**: "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו מוצאו של אדם, עבר פלילי, מידע גנטי, ביומטרי, הערכת אישיות, נתוני מיקום ותעבורה וכן פעילות פיננסית.".

מהו מאגר מידע?

- **מאגר מידע: אוסף פרטי מידע אישי המעובד באמצעי דיגיטלי**, למעט:
  - ❖ " אוסף לשימוש אישי שאינו למטרות עסק";
  - ❖ " אוסף הכולל רק שם, מען ודרכי התקשרות, לגבי 100,000 בני אדם או פחות, שאינו מלמד כשלעצמו על מידע אישי נוסף לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף אחר הכולל פרטי מידע אחרים לגבי אותם בני אדם;

התנאים לרישום מאגר מידע

- **מאגר מידע יירשם ככזה כאשר המידע בו עונה על <u>אחד מהתנאים</u> הבאים:**

מטרתו העיקרית היא איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, ויש במאגר מידע אישי על יותר מ־10,000 בני אדם

מאגר המידע הוא של **גוף ציבורי(רשויות ציבוריות ועיריות).**

מאגר המידע משמש לשירותי דיוור ישיר ויש במאגר מידע אישי על יותר מ־10,000 בני אדם.

"בעל שליטה במאגר מידע לא יעבד מידע אישי במאגר מידע חייב ברישום ולא ירשה לאחר לעבד בעבורו מידע כאמור, אלא אם כן מאגר המידע נרשם במרשם". (מרשם=פנקס המאגרים)

תפקידי מנהל מאגר

מנהל מאגר

- על פי הרשות להגנת הפרטיות מאגרי המידע ינוהלו בשני רבדים וסוגי דרישות:
  - ❖ דרישות ניהוליות.
  - ❖ דרישות טכנולוגיות.
- ההנחה היא כי מנהל המאגר אינו איש מחשוב, ועל כן עליו להיעזר באיש מחשוב / איש אבטחת מידע (המוגדר כממונה אבטחה על המאגרים לפי סעיף 17 ב') לצורך ווידוא יישום הדרישות הטכנולוגיות.

חובת היידוע

נושא חובת היידוע: חובת היידוע נגזרת מסעיף 11 לחוק הגנת הפרטיות ועל פיה קיימת חובה להודיע לאדם האם חלה כלפיו חובה חוקית למסור את המידע, לציין מה מטרות השימוש במידע ולאילו צדדים שלישיים המידע יועבר. כמו כן, בהודעה יש להוסיף את פרטי בעל השליטה, דרכי ההתקשרות עמו, השלכות אי מסירת המידע וזכויותיו של מוסר המידע לפי חוק (למשל לעיין במידע, לתקן אותו וכו').

המשמעות בפועל: יש למפות את כל הממשקים בהם אנו אוספים נתונים אישיים ובאותה נקודת חיכוך – ליישם את חובת היידוע (דוגמה קלאסית: מדיניות פרטיות באתר האינטרנט)

טיפול במאגרים

רישום מאגר חדש

- לצורך הגשת בקשה יש למלא טופס בקשת רישום המופיע באתר הרשות להגנת הפרטיות ובו למלא את כל חלקי הטופס, הכולל את הנושאים הבאים:
  - ❖ חלק א' - פרטי בעל המאגר.
  - ❖ חלק ב' – פרטי המאגר (מטרות, תשתית, מס' משתמשים וכדו').
  - ❖ חלק ג' – בעלי תפקידים במאגר.
  - ❖ חלק ד' – מקורות מידע של מאגר.
  - ❖ חלק ה' – העברות מידע של מאגר.
  - ❖ חלק ו' – מחזיקים במאגר.

- יש לצרף לטופס הרישום גם כתב מינוי מנהל מאגר חתום ע"י הגורמים הרלוונטיים וכן טופס מורשה חתימה בתאגיד.
- בתום מילוי הטפסים יש לשלוח אותם לרשות להגנת הפרטיות לצורך אישור בקשת רישום המאגר.
- משך זמן הטיפול בבקשת רישום הוא עד 90 ימי עבודה. (בפועל זה קצר יותר משמעותית)

עדכון מאגר

- במידה וחל שינוי בפרטי מאגר מידע רשום יש לעדכן את פרטי הרישום של מאגר המידע בפנקס מאגרי המידע באמצעות טופס עדכון מאגר המופיע באתר הרשות.
- סוגי עדכונים:

❖ עדכון פרטי מנהל המאגר (יש לצרף כתב מינוי מעודכן).

❖ עדכון שם בעל המאגר (יש לצרף תעודת שינוי שם של בעל המאגר)

❖ עדכון מטרת המאגר/סוג המידע/שירותי דיוור ישיר (יש לצרף הסבר בנוגע לסיבת ואופן השינוי)

❖ שינוי בעלים או מחזיקים (יש לצרף תצהיר על ביעור המאגר על ידי הבעלים המעביר ועותק מההסכם). הוספת מחזיק במאגר .

❖ הוספת מחזיק במאגר.

מחיקת מאגר

- **נסיבות שבהן בעל מאגר מידע רשאי לבקש מחיקת רישום מאגר ללא ביעור:**

❖ מאגר המידע לא הוקם מעולם.
❖ מאגר המידע אינו קיים (אצל בעל המאגר ו/או אצל צד ג' כלשהו).
❖ כפילות רישום של מאגר מידע (רישום בטעות).
❖ איחוד / מיזוג של מאגרי מידע.
❖ מאגר המידע אינו חייב ברישום.

- **אופן המחיקה:**

❖ מילוי תצהיר מחיקה הקיים באתר הרשות להגנת הפרטיות.
❖ צירוף מסמך מורשה חתימה בתאגיד
❖ הגשת המקור לרשם.

ביעור מאגר

- **נסיבות שבהן בעל מאגר מידע רשאי לבקש מחיקת רישום מאגר עם ביעור:**

❖ מאגר המידע נמסר/נמכר/הועבר לגורם אחר.
❖ בעל המאגר הפסיק את פעילותו העסקית הקשורה למאגר.
❖ סיבה אחרת המצדיקה טענת מחיקה – ילווה במסמך משפטי המצדיק המחיקה.

- **אופן המחיקה:**

❖ מחיקה באופן בלתי ניתן לשחזור של כל עותק מלא או חלקי של המאגר.
❖ השמדה של כל פלט מחשב או נגזרות של מידע ממנו.
❖ וידוא כי פעולות אלה בוצעו גם למי שניתן לו הרשאות גישה וכן ע"י כל מחזיק במאגר.
❖ מילוי תצהיר המופיע באתר רמו"ט.
❖ חתימה ידנית על התצהיר בפני עו"ד או רשם בית משפט.
❖ הגשת המקור לרשם.

מסמך הגדרות מאגר

מסמך הגדרות מאגר הוא מסמך שמפרט את המאפיינים והפעולות הקשורים למאגר מידע
מטרתו היא לתעד באופן מסודר את אופן ניהול המאגר
המסמך כולל לרוב את הפרטים הבאים:

- שם המאגר ומספרו ברישום
- מטרות השימוש במידע
- סוגי המידע שנשמרים במאגר (כולל מידע רגיש אם קיים)
- מקור המידע (למשל: מהנבדק, מספקים, ממאגר אחר)
- גורמים חיצוניים שיש להם גישה למידע (כמו ספקים)
- פרטי מנהל המאגר והממונה על אבטחת המידע

המסמך משמש גם לביקורות פנימיות ולפיקוח של הרשות להגנת הפרטיות.

בקרת מידע עודף

- יש לוודא כי במאגרי המידע לא נאסף או מעובד מידע שלא למטרה שהוגדרה במאגר. (לפחות אחת לשנה) לבחינת הצורך בהמשך שמירת המידע.
- יש למחוק מידע שהמטרה שלו הושגה או שאין עוד חובה משפטית או צורך עסקי להחזיק בו.החובה חלה גם על קבצים זמניים, טיוטות, קורות חיים ישנים ועוד.

- העיקרון המרכזי: פחות מידע = פחות סיכון לפרטיות במקרה של דליפה או שימוש לרעה.

.

בקרות טכנולוגיות

פעולות מחזוריות

פעולה	תדירות
החזקת מסמך הגדרות מאגר עדכני	אחת לשנה
ווידוא כי המידע הנשמר במאגר אינו רב מן הנדרש למטרות המאגר	אחת לשנה
עדכון ואישור נוהל אבטחת מידע	אחת לשנה
הדרכה לבעלי הרשאות במאגר בדבר חובותיהם	אחת לשנתיים
ביקורת (פנימית או חיצונית) כדי לוודא עמידה בהוראות התקנות	אחת לשנתיים
בקרת הרשאות גישה למאגרים	אחת לשנה
בקרת הרשאות למורשי הניהול של המערכת	אחת לשנה
יידוע בעלי ההרשאות בדבר מנגנון הבקרה למערכות המאגר	חלק מהסכם ההעסקה
ביצוע בחינת התאמת העובדים לרגישות תפקידם	שוטף
ביצוע ביקורת אבטחת מידע אצל ספקים המחזיקים /מעבדים מידע	אחת לשנה

בקרות טכנולוגיות

פעולות	
הגדרה ואכיפת מדיניות סיסמאות	הגבלה על חיבור USB ושמירה על ההתקנים הקיימים
החלפת סיסמאות אחת ל-90 יום	עדכוני אבטחת מידע למערכות ההפעלה בשרתי המאגר ובתחנות המשתמשים ברשת הארגון המתחברות למאגר
סיסמה מורכבת	עדכון אנטי וירוס בתחנות ושרתים
נעילה לאחר מספר ניסיונות שגויים	התקנת FW ו- IPS
ניתוק אוטומטי של משתמש לאחר פרק זמן שבו לא היה פעיל	הגבלת גישה למערכות שאינן ברשת לפי כתובת IP
הגדרת לוג המנהל את נושא כניסות למערכת והפעולות שבוצעו	ווידוא מול הספק שתווך התקשורת מוצפן
שמירת נתיב הבקרה למשך 24 חודשים	כתיבה ועדכון נוהל גיבויים
קבלת התראה על כל משתמש ניהול חדש המצורף להרשאות המערכת	שמירת גיבוי למשך 24 חודשים
אבטחת חדרי שרתים: כיבוי אש בגז, בקרת כניסה שומרת לוג, קירור, חיישני לחות והצפה, דלת ברזל	ביצוע שחזור מגיבוי

קביעת סדרי ניהול של מערכות המאגר

- יש לקבוע מי אחראי על ניהול ההרשאות – מומלץ לבחור אדם שמכיר היטב את התחום ואת העובדים.
- תפקידו של האחראי: לתת הרשאות גישה, להגדיר הרשאות לפי תפקיד, להסיר הרשאות במידת הצורך, ולהעביר הרשאות לעובד מחליף כשיש חופשה, חל"ד או חל"ת.
- יש להגדיר מי צריך לקבל עדכון כאשר עובד עוזב או מחליף תפקיד – כדי לוודא שההרשאות שלו מתעדכנות בהתאם. לעיתים יש לעדכן גם ספקים חיצוניים.
- חשוב להכין טפסים מסודרים לקליטת עובדים חדשים ולעזיבה – כולל הגדרת הרשאות מתאימות.
- כחלק מתהליך הקליטה או לפני עזיבת עובד, יש להחתים אותו מראש על טופס שמאשר לארגון גישה לתיבת הדוא"ל הארגונית שלו לצרכים תפעוליים.

קביעת הוראות תפעול שוטפות של מערכות המאגר

- ביצוע עדכונים שוטפים של המערכות והתוכנות המשמשות לגישה אל המידע במאגר המידע ולהגנה עליו, לרבות חומר המחשב הנדרש לפעולתן.
- עדכוני אבטחת מידע.
- מדיניות לגבי מדיה נתיקה (למשל דיסקאונקי)
- אופן קליטת קבצים ממקורות חיצוניים.
- אופן העברת קבצים למקורות חיצוניים.
- עדכוני גרסה והפרדת סביבות.
- הרשאות של גורמים חיצוניים – לעבודה/תמיכה.
- וידוא גיבויים.

ניהול רשימה של מורשי הגישה למערכות המידע

- הקצאת הרשאות נדרשות לעובד חדש בהתאם לטופס 'קבלת עובד'.
- ביטול ההרשאות של עובד שסיים את תפקידו בהתאם לטופס 'עזיבת עובד'.
- ניהול הרשאות גורמים חיצוניים.
- ניהול רישום מעודכן של תפקידים, הרשאות הגישה שנקבעו, ועובדים הממלאים תפקידים אלה והבקרות עליהם.
- סקירת הרשאות תקופתית: לוודא כי הגישה קיימת לגורמים מורשים בלבד

תפקיד	תיכונים	בי"ס יסודיים	גני ילדים	חינוך מיוחד
מנהל מחלקת חינוך	V	V	V	V
עובדת מחלקת גנים	----	----	V	---
עובדת אגף לחינוך מיוחד	----	----	----	V
מזכירת מחלקה	V צפיה	V צפיה	V צפיה	V צפיה

החתמת מורשי הגישה על סודיות וקיום ההוראות החלות על פעילות המאגר

החתמת עובדים על התחייבות לשמירת סודיות

החתמת ספקים על התחייבות לשמירת סודיות ואבטחת מידע

ביצוע הדרכה תקופתית אודות ההוראות החלות על פעילות המאגר

אבטחה

- נקיטת אמצעי אבטחה סבירים, בהתאם לרמת רגישות המידע שימנעו חדירה מכוונת או מקרית למערכת מעבר להרשאות הגישה
  - ❖ התקנת אנטי וירוס בשרתים ותחנות עבודה.
  - ❖ התקנת ואמצעי הגנה מתאימים המגנים מפני חדירה לא מורשית או השבתה ברמת התקשורת.
  - ❖ העברת מידע ממאגר המידע תיעשה תוך שימוש בשיטות הצפנה מקובלות.
  - ❖ אכיפת כל הנוגע לנושא סיסמאות – לא לשמור סיסמאות במקום גלוי, לא להעביר סיסמאות לעובדים אחרים (בכלל זה, מנהלים למזכירותיהן), החלפת סיסמא מידי 90 יום, הגדרת סיסמא מורכבת, מניעת מתן סיסמאות אחידות לעובדים וכדו'.

חובת ניטור ושמירת לוג

- על פי תקנה 10(ג) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז–2017,
- יש לשמור את הלוגים (רשומות הרישום) למשך שנתיים לפחות ממועד רישומם.

- כלומר, כל פעולה המתועדת ביומן הפעולות (כגון גישה, שינוי או מחיקה של מידע) צריכה להיות זמינה לצפייה או שחזור לתקופה של 24 חודשים לפחות.

- זוהי דרישה מחייבת עבור מאגרי מידע ברמת אבטחה בינונית או גבוהה.
- מאגר מידע של גוף ציבורי יהיה ברמה בינונית לכל הפחות

שמירת מידע

- שמירת מידע במדיה נתיקה כמו דיסקאונקי תתבצע ע"י מורשים לכך ע"י הגורם הרלוונטי במועצה/רשות, כאשר המידע יימחק עם הסיום בשימוש בו.
- תיקיות "המסמכים שלי" של המשתמשים ימופו לכונן רשת
- על המשתמשים להימנע מאחסון מידע על גבי הכוננים המקומיים (C:,D:) מידע השמור מקומית על גבי מחשבים אישיים אינו מגובה, ומאובטח פחות מאשר כונני הרשת.
- ניתן לשמור מידע פרטי על כונן : D שאינו מגובה.

מצלמות אבטחה

- הנחית רשם מאגרי מידע מס' 2012/4 בנושא 'במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן', מבהירה את תחולתם של דיני הפרטיות והגנת המידע על השימוש במצלמות המעקב, ומציגה את עקרונות השימוש במצלמות לאור דיני הפרטיות, ומחילה על מאגרי הצילומים, בתנאים מסוימים חובת רישום ואבטחה כמאגר מידע לכל דבר וענין.

- "בטרם קבלת ההחלטה על עצם השימוש במצלמה יש לערוך בדיקה מקיפה של השלכות השימוש במצלמה על זכויות הציבור, ובמיוחד על הזכות לפרטיות; ככל שתחום הכיסוי רחב יותר והיקף האנשים המושפעים צפוי להיות גדול יותר כך צריכה להיות הבדיקה המכינה עמוקה ומקיפה".

במסגרת הבדיקה יש להתייחס בין השאר לנושאים הבאים:

- התכלית אותה מבקשים להשיג באמצעות מצלמות המעקב.
- מידתיות השימוש במצלמות מעקב לשם השגת המטרה הרצויה.
- הצבת המצלמות באופן הגון שאינו פוגע בפרטיות
- חובת שילוט במרחבים רלוונטיים