

מאגרי המידע ופרטיות –

חידושים בתחום האכיפה

עו"ד דן חי

דן חי ושות', עורכי דין

דרך אבא הלל סילבר 12, רמת גן 52506

טל: 03-6005777; פקס: 03-6005888

www.danhay.co.il

www.hay-law.com

פריסת מצלמות במתקני החברה



פריסת מצלמות – הדרישות:

קבלת ההחלטה להצבת מצלמה, הכוללת:

- הגדרת מטרת הצבת המצלמות באופן ברור ומפורש;
- בחינת חיוניות ההצבה (האם זהו האמצעי המתאים להשגת המטרה; האם אין אמצעי חלופי; האם אכן צומחת תועלת מהתקנת המצלמה);



ההתקנה בפועל



- בחינת מיקום המצלמה וזווית הצילום שלה.
- כמות מצלמות קטנה ככל האפשר.
- מועדי הצילום.
- איכות הצילום.
- אין לשלב הקלטת קול.
- קבלת הסכמה מכללא לצילום – שילוט.

שילוט



לתשומת ליבכם!

במתקן זה מותקנות מצלמות במעגל סגור לצרכי אבטחה.

לשאלות ופרטים נוספים _____ טלפון, _____ מייל

לוגו החברה

אגף הביטחון

תוצאות פעולת מיקום המצלמות בשטח

- אבטחת החומר המצולם (הגנה פיזית ולוגית).
- סיווג מורשי גישה לחומר והיקף הגישה.
- קביעת משך שמירת החומר.
- קביעת תקנון שימוש בחומר המצולם.

סכנה נוספת בצילום – יצירת מאגר מידע

דרך היצירה: יכולת הצלבה בין הצילום לזהות המצולם.

• אפשרויות:

1. מצלמה מזהה פנים.
2. הצלבה בין מידע במאגרים שונים.
3. זיהוי אחר של אנשים.



פרטיות העובדים



פרטיות העובד - נקודות חשיפה:

- מעקב אחר מיקום במתקני החברה (מצלמות, כרטיסי קרבה).
- מעקב אחרי ביצועים (מצלמות, מעקב אחרי פעולות במחשב).
- נתוני תקשורת של עובדים (נתוני מיקום, פירוט שיחות, נתוני גלישה).
- עיון במיילים.
- מאגרי מידע של עובדים ומועמדים לעבודה - עיון העובד במידע.

ההגנה על העובד

פגיעה בפרטיות העובד אפשרית רק אם הסכים לכך.

מבחני ההסכמה של עובד לפגיעה:

• בעבר – קבלת מכשור מהמעביד = הסכמה מכללא.

• היום – דרישת הסכמה מדעת:

1. ההסכמה מרצון חופשי (לא כפייה).
2. אין להסתפק בהסכמה מכללא.
3. לטובת תכלית ראויה – מוצדקת לאור התפקיד.
4. מידתיות – בדיקה אם אין דרך אחרת להשגת המטרה.
5. צמידות למטרה.

תא הדואר-האלקטרוני של העובד כדוגמה

• תא מקצועי – ניתן להיכנס.

התנאי: אישור העובד מראש כי אסור לשלוח מיילים פרטיים ואפשרות חדירה.

• תא מעורב (מקצועי ופרטי) – אין כניסה.

אפשרויות: הסכמה מקומית או צו בית-דין.

• תא פרטי – אין כניסה.

האפשרות היחידה: צו בית-דין.





שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי העבודה:

- על מעסיק לקבוע מדיניות מפורשת ומפורטת לשימוש בטכנולוגיות מידע ולהודיע על כך לעובדים.
- יש להיוועץ עם ועדי ונציגי עובדים בנוגע למדיניות.
- הסכמת העובד למדיניות זו צריכה להינתן במפורש ולא מכללא.
- תוצרי הצילומים מהווים מאגר מידע – מאגר קיים או נפרד.
- שימוש במצלמות במקום העבודה צריך לעמוד בדרישות הסבירות, המידתיות, תום הלב והשקיפות.



שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי העבודה:

-המשך-

- הבחנה בין מצלמות באזורים ציבוריים לבין מצלמות במרחב פרטי במקום העבודה.
- שימוש במצלמות נסתרות הינו אסור, למעט מקרים חריגים במיוחד, וגם אז – רק בידיעת העובדים.
- לא ניתן לקבל הסכמה עקרונית מהעובד לצילומו, אלא יש לעדכן על מיקומה המדויק של כל מצלמה.
- אסור לצלם בחדרי שירותים או מקלחות, משרדו של העובד (גם אם הוא חולק אותו עם אחרים) או איזור מנוחה.



שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי העבודה - ביקורת:

1. הסכמת העובדים - אין מקום לדרוש ממעסיקים קבלת הסכמה מפורשת; די ביידוע באופן סביר תוך שקיפות מלאה.
2. במקרים המתאימים, אף יידוע לא ידרש אם יוסק כי המטרה 'מקדשת את האמצעים', כגון חקירת הטרדות, מניעת הונאות חמורות - אם גילוי הצילום עלול לפגוע במטרה זו.
3. שאלת מעורבות וועדי עובדים בקבלת ההחלטות בנושא אינה זה סבירה.



שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי העבודה - ביקורת:

-המשך-

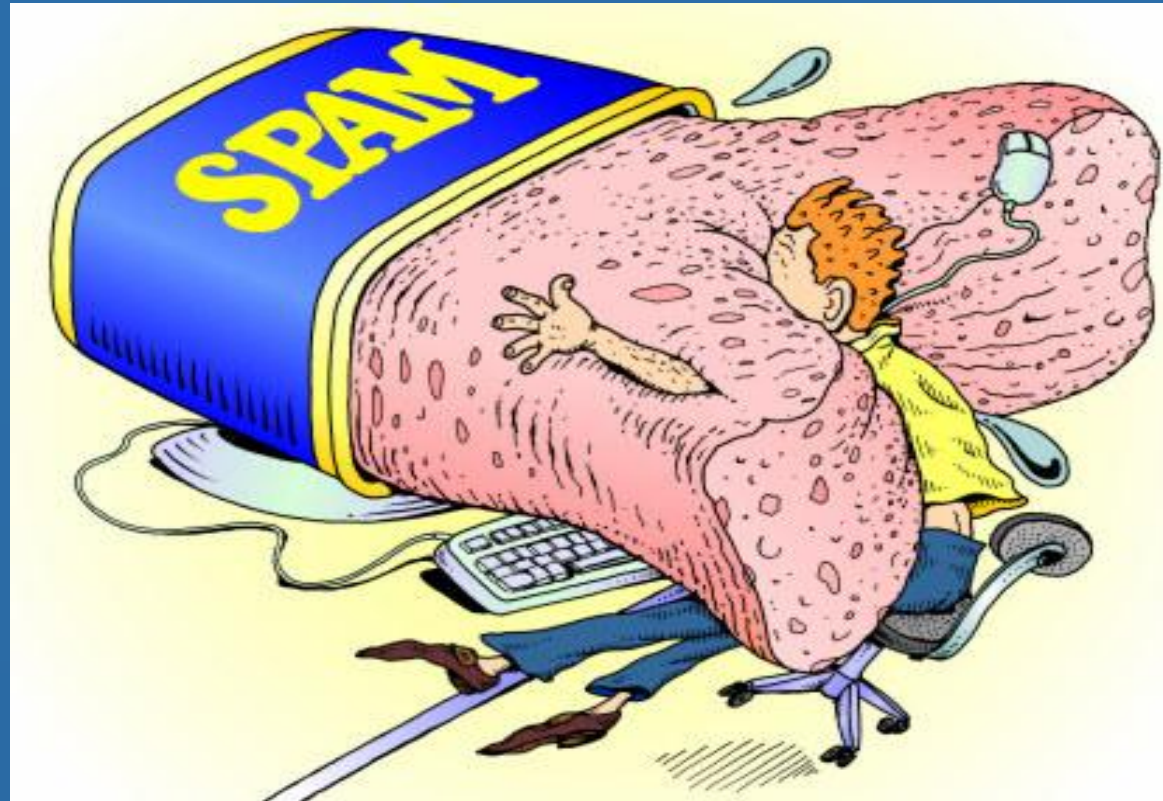
4. הרחבת הגדרות החוק 'מידע' ו- 'מאגר מידע' מעבר לנדרש בחוק. חוסר הבחנה בין אפשרות זיהוי בפועל לבין פוטנציאל תיאורטי בלבד.

5. הבחנה גורפת מדי בין מרחבים במקום העבודה (אזורים ציבוריים, בהם ישנם לקוחות, לעומת אזורי עבודה) – ההבחנה הנכונה צריכה להיות בהתאם לציפייה הסבירה לפרטיות

(כגון חדרי שירותים או מלתחות; ולא במחסנים או Open-Space, בהתחשב באינטרסים חיוניים של המעסיק).

6. איסור גורף מדי על צילום נסתר.

דיוור ישיר



דיוור ישיר

1. פניה אישית לאדם
2. בהסתמך על פרופיל (השתייכות לקבוצת אוכלוסין שנקבעה על-פי אפיון אחד או יותר)
3. בהתבסס על מאגר מידע

שני סוגים של "דיוור ישיר":

- דיוור עצמי לפרטים במאגר
- העברת הפרטים לצד ג' – שירותי דיוור ישיר

יש לרשום 'דיוור ישיר' או 'שירותי דיוור ישיר' במטרת מאגר המידע



• ניהול מאגר לשירותי דיוור ישיר-

1. יש לרשום את מקור המידע.
2. מועד קבלת המידע.
3. למי נמסר המידע.

כל פניה בדיוור ישיר תכיל באופן ברור ובולט:

1. ציון כי הפניה היא דיוור ישיר, בצירוף ציון מספר הרישום של המאגר המשמש לשירותי דיוור ישיר בפנקס מאגרי מידע;
2. הודעה על זכותו של מקבל הפניה להימחק מן המאגר בצירוף המען שאליו יש לפנות לצורך כך;
3. זהותו ומענו של בעל מאגר המידע שבו מצוי המידע שעל פיו בוצעה הפניה, והמקורות שמהם קיבל בעל המאגר מידע זה.

כל אדם זכאי לדרוש להימחק ממאגר מידע המשמש לדיוור ישיר

יש להודיע על המחיקה תוך 30 יום ממועד קבלת הבקשה.





פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר:

- הבחנה בין "דיוור ישיר", לבין "שירותי דיוור ישיר", ולבין דבר פרסומת ("ספאם").
- החרגה - פניה פרטנית של בעל מאגר לנמענים הרשומים בו שלא על פי פרופיל משותף – אינה דיוור ישיר.
- הבחנה בין פניה ללקוחות פעילים ללקוחות שאינם פעילים.
- דרך קבלת ההסכמות ממושאי המידע במסגרת חוזה אחיד – opt in.
- הזכות להימחק ממאגר מידע המשמש לדיוור ולמטרות נוספות – המחיקה רק מרשימת הדיוור.



טיוטת ההנחיה בנושא הדיור ישיר ושירותי דיור ישיר - ביקורת:

- ההוראות סותרות את הקביעה בחוק, לפיה מנגנון ההסכמה לדיור ישיר הינו מסוג של opt-out.
- דרך ניסוח ההוראות בנושא בחוזה אחיד – בעייתית.
- ההבחנה בין דיור ללקוחות פעילים לכאלו שאינם פעילים אינה נכונה.

תקנות אבטחת המידע החדשות



מסמכים הנדרשים על פי התקנות החדשות:

1. מסמך הגדרות הכולל פרוט של כל המידע המצוי במאגר המידע, השימושים שנעשים בו ופעולות אבטחת המידע לגביו.
2. נוהל אבטחת מידע.
3. מסמך מבנה מאגר המידע.
4. רשימת מצאי של מערכות המידע.
5. מסמך הרשאות גישה מסודר, מושכל ומעודכן.
6. תוכנית לבקרה שוטפת של עמידה בתקנות.
7. נוהל בדיקה שיגרתי של נתוני התיעוד של מנגנון הבקרה ועריכת דו"ח על הבעיות שהתגלו.
8. תיעוד אירועי אבטחה.

הוראות ביצוע בתקנות החדשות:

1. הקפדה על דרכי הזיהוי של מורשי הגישה (סיסמאות, עדכון וכד')
2. אבטחה פיזית וסביבתית – הוראות מפורטות, כגון בנושא בקרת כניסה.
3. חובה לעריכת הדרכות לעובדים לפני מתן גישה למידע.
4. הקפדה על זיהוי נכון של העובדים בעת הכניסה למידע.
5. הפעלת מנגנון של תיעוד ובקרה שישמר לפחות 24 חודש.
6. גיבוי ושחזור – הוראות פרטניות לעניין זה.
7. יש להודיע לרמו"ט על אירוע אבטחה חמור.
8. יש להגביל או למנוע גישה להתקנים ניידים.
9. יש להקפיד על אבטחת התקשורת למאגרי המידע.

הוראות לפעולות תקופתיות:

1. עדכון אחת לשנה של מסמך ההגדרות ונוהל אבטחת המידע.
2. סקר סיכוני אבטחת מידע - לפחות אחת ל-18 חודשים.
3. יש לדון באירועי אבטחת מידע לפחות אחת לרבעון.
4. יש לערוך ביקורת תקופתית לפחות אחת ל-24 חודש.



כאשר המידע מצוי מחוץ לארגון -

פעילות במיקור חוץ:

- אי העברת מידע עודף
- הסכם מיקור חוץ מחייב עמידה בכל ההוראות
- הטמעת נהלי אבטחת מידע
- פיקוח וביקורת
- ניתוק מגע (בסיום התקשרות)



סיווג מאגרים לפי התקנות החדשות

מאגרי מידע יסווגו לפי שלושה סוגים:

1. מאגר שחלה עליו רמת אבטחה בסיסית.
2. מאגר שחלה עליו רמת אבטחה בינונית.
3. מאגר שחלה עליו רמת אבטחה גבוהה.

מאגר יסווג לפי מספר קריטריונים אשר מופיעים בתוספת לתקנות, הקריטריונים מתייחסים בעיקר לגודל, סוגי המידע שבמאגר, אופן השימוש במאגר.

סיווג מאגרים לפי התקנות החדשות

-המשך-

חובות בעל מאגר תלויות בסיווג המאגר:

1. במאגר שחלה עליו רמת אבטחה בסיסית- עמידה רגילה בדרישות התקנות.
2. במאגר שחלה עליו רמת אבטחה בינונית- דרישות נוספות בתקנות: נוהל אבטחה מחמיר, בקרה ותיעוד של כניסות ויציאות מהמאגר, קיום הדרכות, דרישות בנושא זיהוי ואימות, קיום דיון לאחר אירועי אבטחה, קיום ביקורות, שמירת נתוני אבטחה, הכנת נוהל גיבוי ושחזור.
3. במאגר שחלה עליו רמת אבטחה גבוהה- בנוסף לדרישות החלות על מאגר בינוני ישנן עוד מספר דרישות כגון ביצוע סקר סיכונים ומבחני חדירות למערכת האבטחה.

תודה!

עו"ד דן חי

דן חי ושות', משרד עורכי-דין

דרך אבא הלל סילבר 12, רמת גן

טלפון: 03-6005777 פקס. 03-6005888

dan@hay-law.com

WWW.HAY-LAW.COM

הישארו מצודקנים – הצטרפו לניוולטר באתר!