

## היבטי פרטיות במעקב אחר עובדים מרחוק עדכון לקוחות – מחלקת הייטק וטכנולוגיה - ינואר 2023

### לקוחות יקרים,

ביום 25.12.2022 פרסמה הרשות להגנת הפרטיות ("הרשות") טיוטת מסמך שכותרתו "היבטי פרטיות במעקב אחר עובדים מרחוק" ("המסמך"). מטרת המסמך היא להציג את עמדת הרשות ביחס לתופעה הגוברת בשנים האחרונות של מעסיקים אשר מנטרים את פעילותם של עובדיהם העובדים מביתם, להציב זרקור על הסיכונים האפשריים בניטור זה, להציג ולסקור את הרקע המשפטי הרלוונטי ואת הפרשנות בדיון בקשר לנושא זה.

ראינו לנכון לסקור בתמצית את עיקרי המסמך הן משום שהוא כבר במתכונתו הנוכחית (כטייטה להערות הציבור) מצביע על האופן בו הרשות רואה סוגיה המשפיע על שגרת החיים של עובדים רבים העובדים מהבית בשנים האחרונות, והן משום שניתן להעביר לרשות התייחסות למסמך עד ליום 22.1.2023 בשעה 12:00.

**אנו נשמח לעמוד לרשותכם לצורך הגשת התייחסות למסמך, וכן על מנת לסייע לארגונכם לעמוד בהוראות דיני הגנת הפרטיות ואבטחת המידע החלים עליו.**

**להלן נפרט את עיקרי המסמך.**

### רקע

רבים ממקומות העבודה היום מאפשרים לעובדיהם לעבוד שלא ממקום העבודה (עבודה מרחוק). אחת ההשלכות של תופעה זו היא האופן שבו מעסיקים יוכלו לנטר את עבודת עובדיהם במצב שבו הם אינם נמצאים במשרד ולרוב נמצאים בביתם. לרוב ניטור זה נעשה באמצעים טכנולוגיים מתקדמים שונים ("אמצעי המעקב") ובצידם סכנות מסוימות בתחומי אבטחת המידע ושלהם השפעה רבה על פרטיות העובדים המנוטרים.<sup>1</sup> במסגרת המסמך הרשות מבקשת להעמיד אמות מידה לאופן בו יש לדעתה לעשות שימוש באמצעי מעקב אלו.

1. סיכונים עיקריים שמונה הרשות במסמך הם (א) איסוף ושמירת מידע ללא הסכמה (לאור הדרישה להסכמות שיש לקבל מעובדים בנסיבות מסוימות); (ב) איסוף וחשיפה של מידע רגיש (במיוחד בניטור עבודת העובד מהבית); (ג) איסוף ושמירת מידע עודף (למשל בעת שנקלטים בני הבית של עובדים או פעילות שלהם באמצעות אמצעי הניטור); (ד) דלף וזליגת מידע (במיוחד כשעבודה מרחוק מתבססת על רשתות ציבוריות ואמצעים הנתונים לגישה מרחוק ובמיוחד שיתכן בטכנולוגיות מסוימות שנאסף מידע היכול לשמש לגניבת זהות); (ה) שימוש לרעה במידע (הרשות מעלה חשש שמעסיקים יעשו שימוש במידע שנאסף באמצעי הניטור למטרות זרות (למשל ידיעה אודות עובדת המצויה בשלבי הריון ראשוניים) עת הם נחשפים למידע מבתי עובדים. מידע שמעסיקים אינם חשופים אליו לרוב.

למעסיק פררוגטיבה ניהולית הנגזרת מזכות הקניין לנהל את עסקו ומכוחה הוא רשאי להחליט על שימוש באמצעים טכנולוגיים במקום העבודה, כדי להגן על אינטרסים לגיטימיים של עסקו, ובהקשר זה אבטחה ופיקוח על העובדים. לעיתים למעסיקים אף יש חובה לנטר את פעילות עובדיהם. למשל מכוח סעיף 25 לחוק שעות עבודה ומנוחה, התשי"א-1951 ("חוק שעות עבודה ומנוחה"), שקובע חובת ניהול פנקס שעות עבודה, סעיף 24 לחוק הגנת השכר, התשי"ח-1958 והתוספת לחוק הקובעים חובה לפרט בתלוש השכר פרטים לגבי ימי העבודה ושעות העבודה בפועל.

חוק הגנת הפרטיות, תשמ"א-1981 ("חוק הגנת הפרטיות") הוא דבר החקיקה העיקרי המסדיר את סוגית הפרטיות בישראל. סעיף 1 לחוק הגנת הפרטיות קובע כי לא יפגע אדם בפרטיות זולתו ללא הסכמתו. סעיף 2 לחוק הגנת הפרטיות מונה דוגמאות לפגיעה בפרטיות ששימוש באמצעי המעקב יכול להתאים לחלקן. כך למשל ביחס לאיסור בילוש או התחקות אחר אדם (סעיף 2(1) לחוק), האזנה האסורה לפי חוק (סעיף 2(2)), צילום של אדם ברשות יחיד (סעיף 2(3)), שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה (סעיפים 2(9) וכו').

לאחר איזון הזכויות והחובות לעיל קבעו בתי המשפט בארץ לפי המסמך כי במסגרת הפררוגטיבה הניהולית הנגזרת מזכויות הקניין של המעסיק, רשאי מעסיק לפקח על פעילות העובדים במטרה לוודא שלא יעשו שימוש בלתי מורשה או בלתי חוקי בכלי העבודה הווירטואלי המופקד בידם, ורשאי הוא לקבוע את טכנולוגיות המעקב על פעולות העובדים במקום העבודה.<sup>2</sup> כל זאת בכפוף לעקרונות תום לב, גילוי, שקיפות, לגיטימיות, מידתיות וצמידות למטרה. בהתאם לכך, הפסיקה מבחינה בין אמצעי פיקוח שונים במקום העבודה, הפוגעים במידה שונה בפרטיות העובד ובהתאם לכך ולנסיבותיו של כל מקרה, משתנה גם צורת ההסכמה הנדרשת מהעובד כדי שהמעסיק ישתמש באמצעים השונים באיזוניה למול זכויות המעסיק.

2. כך ביחס לניטור תיבות מייל בע"ע (ארצי) 90/08 טלי איסקוב ענבר נ' מדינת ישראל - הממונה על חוק עבודת נשים (פורסם בבנו, 8.2.2011) וביחס למעקב נוכחות באמצעים ביומטריים בעס"ק (ארצי) 14-04-7541 הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי - עיריית קלנסווה (פורסם בבנו, 15.7.2017) ועוד.

הרשות מחלקת את אמצעי המעקב לשלושה סוגים על פי רמת הפגיעה שלהם בעובדים:

1. **אמצעי מעקב שאינם פוגעים בפרטיות העובדים** – מדובר באמצעי מעקב שכלל אינם דורשים איסוף מידע כגון טכנולוגיות של חסימת גישה לאתרים מסוימים או הגבלת הורדת תוכנות למכשירים ניידים.

2. **אמצעי מעקב שפוגעים בפרטיות העובדים בצורה מועטה** – מדובר באמצעי מעקב האוספים מידע שאינו אישי בקשר להתנהלות העובד ובזאת אמצעים המנטרים את השימוש של העובד במערכות תפעוליות של הארגון וכך עשוי להיאסף מידע אישי מסוים על העובד.

3. **אמצעי מעקב שפוגעים בפרטיות העובדים בצורה גבוהה** – אמצעי מעקב היכולים לשמש למעשה גם למשטור העובד כיוון שמדובר באיסוף מידע רגיש ואישי. מדובר באמצעי מעקב של איסוף מידע ביומטרי, נתוני מיקום, ניטור רציף לרבות צילום מסך המחשב של העובד והאזנה למיקרופונים ואף ניטור תיבות הדוא"ל של העובד בין אם היא אישית, מקצועית או מעורבת.

הרשות מציינת בין היתר את הכלים הבאים כאמצעי מעקב שפגיעתם בפרטיות גבוהה:

א. כלי סריקה ופיקוח על האתרים שבהם גולש העובד (בשונה מחסימת גישה לאתרים מסוימים) ותוכן תיבת הדוא"ל שלו (בין אם מדובר בתיבה מקצועית, אישית או מעורבת).

ב. אמצעים לשליטה על מצלמות רשת ועל מיקרופונים כדי לצלם ולהאזין לסביבתו של העובד.

ג. אמצעים לניטור תנועות עכבר ואופן השימוש במקלדת (Keyloggers).

ד. אמצעים לצילום מסך המחשב (Screenshots).

ה. אמצעים למעקב אחר תנועות העיניים לבחינת התכנים שבהם הוא צורך במחשב.

ו. אמצעים לאיסוף נתוני מיקום של העובד המותקנים ברכבו של העובד או מכשיריו הדיגיטליים.

עמדת הרשות היא כי שימוש מעסיקים באמצעי מעקב שפגיעתם בפרטיות גבוהה במיוחד (כגון אלו אשר צוינו לעיל) מעלה חשש ממשי לחריגה מהוראות הדין.

### לגיטימיות, מדתיות וצמידות למטרה

כאמור לעיל, לפי המסמך מעסיק המבקש לעשות שימוש באמצעי מעקב יכול לעשות כן רק לשם מטרה מוגדרת ולגיטימית בעלת זיקה לאינטרסים הלגיטימיים של מקום העבודה. אם לא ניתן להצביע על מטרה כזו (למשל במסגרת הליך עיצוב לפרטיות) אין הוא רשאי לעשות שימוש באמצעים אלה. זאת כאשר למעסיקים אסור להשתמש במידע שנאסף כתוצאה משימוש באמצעי מעקב שנועדו לבחינת שעות עבודתו של עובד, שלא למטרה לשמה נמסר.

אמצעי מעקב שבבחר על-ידי מעסיק צריך להיות תואם לתכלית המעקב. כך לדוגמה, מעסיק המבקש לנטר את היקף שעות העבודה של עובד, צריך לעשות שימוש באמצעים התואמים מטרה זו ולא באמצעים שנועדו לתכליות אחרות, כגון למעקב אחר פרודוקטיביות העובד במסגרת ניטור תכני האתרים בהם הוא גולש בשעות העבודה. כך, ככלל, מעקב אחר עובדים במתכונת של עבודה מרחוק אמור להתבצע במסגרת שעות העבודה בלבד.

קודם לשימוש באמצעי מעקב, מעסיק צריך לבחון את החלופות האפשרויות העומדות בפניו, ולבחור את החלופה מבין החלופות הרלבנטיות להגשמת התכלית שיישומה יפגע בפרטיות העובדים במידה הפחותה ביותר האפשרית.

על מעסיקים השוקלים להשתמש באמצעים דיגיטליים למעקב אחר עובדים בביתם להתחשב במידת הפגיעה בפרטיות העובדים ובני ביתם, שעה שהם בוחנים האם ובאילו אמצעים להשתמש ולבחון אם הפגיעה בזכות לפרטיות שעתידה להיגרם מהם היא ללא יחס ראוי לתועלת שהוא מביא בהגשמת המטרה שהציב כאמור לעיל.

### גילוי, שקיפות

לפי הפסיקה המובאת במסמך, עמדת הרשות היא שפגיעה בפרטיות במקום העבודה דורשת יידוע העובדים, כדי להשיג הסכמה מדעת במפורש או מכללא. כך על מעסיקים ליידע את עובדיהם על כך שיעשה שימוש באמצעים טכנולוגיים למעקב אחר התנהלותם במתכונת של עבודה מרחוק. יידוע זה צריך לכלול גם את המטרה שלשמה נעשה השימוש באמצעי המעקב.<sup>3</sup> בנוסף אומרת הרשות שעמדתה היא שכשניתנות מספר ברירות לעובד והמעסיק פורס בפניו את האפשרויות השונות – כך תיראה הסכמת העובד כחופשית ואמיתית יותר.

מעסיקים המבקשים להשתמש באמצעי מעקב שפגיעתם בפרטיות עובדים היא גבוהה – כגון אמצעים למעקב אחר פעילות העובד במחשבו ותכתובת הדואר האלקטרוני של העובד, או אמצעים מבוססים מידע ביומטרי (כגון שימוש בחיישן לקליטת שמע או מערכת לניטור תנועת עיניים) – אינם יכולים להסתפק ביידוע כללי, ועליהם לפרט בפני העובדים, בכתב ובשקיפות מלאה, על אופן ביצוע המעקב והשימוש במידע.<sup>4</sup>

---

3. ראו מזכרנו בנושא חובת יידוע במסגרת איסוף ושימוש במידע אישי [כאן](#).  
4. לפי הרשות, על מעסיק לפרט, לדוגמה, על אופן השימוש באמצעי המעקב, על סוג המידע שייאסף, תדירות ומועדי המעקב, השימוש שיעשה במידע שייאסף, היכן הוא יישמר ולכמה זמן.

בנוסף, לפי הרשות על המעסיק לקבוע את המדיניות בקשר לאמצעי המעקב האמורים, לרבות תוך ציון כללי האסור והמותר בשימוש במחשב וביישומיו בעת העבודה מרחוק. כן עמדת הרשות היא שלפי הפסיקה מן הראוי לעגן עקרונות אלה במפורש בחוזה העבודה ובתקנון הנהג במקום העבודה, ותוך היוועצות עם נציגות העובדים.

חרף האמור לעיל מדגישה הרשות כי אין בהסכמת עובדים כדי 'להכשיר' שימוש שאינו מידתי באמצעי מעקב, או כזה הנעשה שלא למטרה מוגדרת ולגיטימית, בעלת זיקה לאינטרסים הלגיטימיים של מקום העבודה.

עוד מבקשת הרשות להסדיר במסגרת המסמך שבכל הנוגע לשימוש באמצעי מעקב שאינם כרוכים במהותם באיסוף מידע אישי על אודות עובדים (כגון ניטור נתוני תקשורת בלבד בתיבת הדואר המקצועית של העובד), מבקשת הרשות לקבוע כי שימוש זה אפשרי ללא קבלת הסכמת העובד, אולם יש ליידעו על כך, וכי איסוף זה כפוף אף הוא לעקרונות הלגיטימיות והמידתיות שצוינו קודם לכן.

#### עקרונות נוספים

פרט לעקרונות המובאים לעיל, הרשות מדגישה עקרונות נוספים שיש להקפיד עליהם בבחינת האפשרות לעשות שימוש בטכנולוגיות מעקב ובעת השימוש בהם. העיקריים בהם לדעתנו -

צמצום מידע עודף. הרשות מבהירה כי לגישה ייתכנו מצבים (כתלות בסוג המידע האישי ומטרת איסופו) בהם על מעסיקים לבחון בתדירות גבוהה מזו המנויה בתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 ("תקנות אבטחת מידע"), את נחיצותו של מידע זה השמור במאגרים.

תסקיר השפעה על פרטיות וממונה פרטיות. הרשות מבקשת להדגיש את החשיבות בעריכת תסקיר השפעה על פרטיות, טרם השימוש באמצעים למעקב אחר עובדים.<sup>5</sup> כן מבקשת הרשות להדגיש בהקשר זה גם את התועלת הרבה שבמינוי ממונה הגנת פרטיות בארגון, שבין יתר תפקידיו, הוא גם הגורם המתאים והיעיל לתכנון ולבחינת הצעדים הננקטים בארגון למזעור הסיכון לפגיעה בפרטיות העובדים.<sup>6</sup>

5. ראו את מזכרנו בנושא [כאן](#).

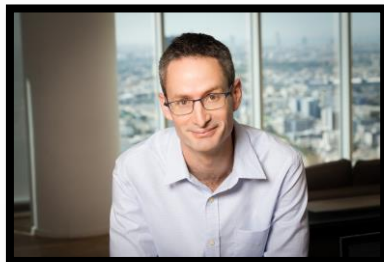
6. ראו את מזכרנו בנושא [כאן](#).

עיון ותיקון. הרשות מבהירה כי הוראות סעיפים 13 ו-14 לחוק הגנת הפרטיות חלות על מידע אישי שנאסף באמצעות אמצעי המעקב ותנון אף הוא לזכות העיון, התיקון והמחיקה בנסיבות מסוימות כאמור בסעיפים אלה.

נשמח לסייע לארגונכם להגיש התייחסות למסמך ולוודא עמידה בהוראות הגנת הפרטיות ואבטחת המידע החלות עליו.

לקריאת המסמך המלא יש ללחוץ [כאן](#).

\* המידע האמור לעיל הינו מידע כללי ותמציתי בלבד, הוא אינו מהווה חוות דעת או ייעוץ משפטי ויש לקבל עצה מקצועית נפרדת בטרם נקיטת פעולה משפטית או אחרת בקשר עם הנושאים אותם סקרנו.



עו"ד סער רוסמן  
שותף, מחלקת הייטק וטכנולוגיה  
[saar@agmon-law.co.il](mailto:saar@agmon-law.co.il)



עו"ד אסנת סרוסי פירסטור  
ראש מחלקת הייטק וטכנולוגיה  
[osnat@agmon-law.co.il](mailto:osnat@agmon-law.co.il)