



## מדריך למעבידים ולעובדים בנושא:

### הגנה על מידע אישי במקום

#### העבודה

רמ"ט הרשות למשפט, טכנולוגיה ומידע



### תוכן עניינים

3.....	תמצית.....	3
5.....	מבוא.....	5
7.....	חלק א' - עקרונות הגנת הפרטיות במידע במקום העבודה.....	7
7.....	1. מבוא - תחולת החוק.....	7
8.....	2. עקרון ראשון - הסכמה מדעת.....	8
9.....	3. עקרון שני - תכלית ראויה.....	9
10.....	4. עקרון שלישי - מידתיות.....	10
10.....	5. עקרון רביעי - שקיפות - מסירת הודעה על איסוף ושימוש במידע.....	10
11.....	6. עקרון חמישי - הגבלת מטרה :.....	11
11.....	7. עקרון שישי - סודיות ואבטחת מידע :.....	11
12.....	8. עקרון שביעי - חובות ביחס לביצוע פעולות במיקור חוץ :.....	12
12.....	9. עקרון שמיני - עיון ותיקון :.....	12
12.....	10. סיכום ביניים.....	12
13.....	חלק ב' - עיבוד מידע אישי במקום העבודה.....	13
13.....	1. שלב ראשון : ניהול המידע מתחיל בשלב הגיוס לעבודה - טרום העסקה.....	13
17.....	2. שלב שני : ניהול תיק עובד - לאחר הקבלה לעבודה ובעת העבודה.....	17
27.....	3. שלב שלישי : שמירה ומחיקת מידע לאחר סיום יחסי עובד - מעביד.....	27
29.....	חלק ג' - הסדרת השימוש בטכנולוגיית מידע במקום העבודה- ניטור.....	29
32.....	סיכום.....	32
33.....	נספח : ריכוז שאלות לבדיקה עצמית והמלצות.....	33



## תמצית

1. חוק הגנת הפרטיות, התשמ"א-1981 (להלן – החוק) מסדיר את החובות החלים על מי שאוסף ומעבד מידע לפי החוק. במסגרת יחסי עבודה נצבר מידע אישי רב ורגיש אודות העובד. מטרתו של מסמך זה להצביע על העקרונות החלים ביחס לזכות לפרטיות במידע במקום העבודה, ולהראות את אופן יישומם של עקרונות אלה לגבי מידע על אודות עובדים, שנאסף ונצבר בידי מעסיקים.
2. בנוסף, בשל ההתפתחויות הטכנולוגיות המשמעותיות של השנים האחרונות, מידע אישי אודות העובדים נאסף לא רק במערכות המידע הייעודיות לצרכי ניהול כוח האדם, המנוהלות ברגיל במחלקת משאבי האנוש של הארגון, אלא גם במערכות המידע ובטכנולוגיות המשמשות את שאר המחלקות של הארגון לצורך ביצוע העבודה, ולמטרות אישיות של העובדים, לרבות רשת המחשבים המשרדית הכללית, מערכת הדואר האלקטרוני, רשת האינטרנט וטלפונים חכמים ומחשבי לוח המסופקים לעובד מידי המעסיק.
3. המסמך משקף את עמדת רשם מאגרי מידע בעניין אופן העמידה בהוראות החוק בעת האיסוף העיבוד של מידע במקום העבודה.
4. בחלק הראשון של המסמך, מוצגים העקרונות הכלליים החלים על פרטיות במידע במקום העבודה. בחלק השני, נדון ישומם, בחלק השלישי נדונים היבטים מסויימים של מעקב הנובעים משימוש בטכנולוגית מידע, ובנספח מוצע שאלון לבדיקה.
5. **העקרונות המרכזיים שצריכים להנחות מעסיקים הנם:**
  - 5.1 בחינה שוטפת של היקף המידע הנאסף על ידי המעסיק, בכל השלבים של יחסי העבודה, מטרות האיסוף, וכי האיסוף והשמירה אינם מעבר לנדרש לצרכי העבודה.
  - 5.2 מיפוי המידע שנשמר על ידי המעסיק, מטרות השימוש שלו, ומי ניגש אליו.
  - 5.3 קיום הוראות קבע ואמצעים טכנולוגיים בתחום אבטחת המידע ביחס למידע זה, על מנת למנוע דליפה שלו או שימוש לרעה על ידי מורשי הגישה.
  - 5.4 הדרכה שוטפת למי שנגיש למידע אישי לגבי חובותיו לפי החוק כדי למנוע שימוש לרעה במידע.
  - 5.5 בקרה על קיום כל הוראות אלה גם כאשר הן מבוצעות במיקור חוץ.



5.6 קביעת מדיניות מפורשת לעניין שימוש בטכנולוגית מידע (מחשב אישי, טלפון חכם), המותר והאסור, ואת המקרים בהם מעביד עשוי לנטר שימושים אלה, במגבלות הפסיקה.

פרופ' רותם



## מבוא

1. בעולם העבודה המודרני, מעסיקים אוספים ומעבדים מידע אישי<sup>1</sup> אודות מועמדים לעבודה ועל עובדים בארגוניהם. איסוף ועיבוד המידע נעשה בדרך כלל במסגרת הפררוגטיבה של המעביד בניהול עסקו.<sup>2</sup> איסוף ועיבוד המידע נועדו לצורך קבלת החלטות בדבר קבלה לעבודה, קידום, מילוי חובות חוקיות ורגולטוריות שונות, שימור יכולת הניהול והשליטה של המעביד במקום העבודה, ובמקרים מסוימים כדי להגן על המעסיק מפני תביעות אפשריות של צדדים אחרים. בנוסף, ההתפתחויות הטכנולוגיות באמצעים ובכלים המשמשים את סביבת העבודה המודרנית מאפשרות גם התחקות או מעקב אחר פעילות העובד – החל בניטור גלישה באינטרנט ושימוש בדואר אלקטרוני, עבור לאיתור נתוני מיקום ושיחות הקשורות בטלפון שניתן לעובד במקום העבודה, וכלה באמצעי מעקב כגון מצלמות.
2. ההגנה על מידע אודות אדם הינה חלק מהזכות החוקתית לפרטיות הקבועה בסעיף 7 לחוק יסוד: כבוד האדם וחירותו, והמוסדרת בחוק הגנת הפרטיות, התשמ"א-1981 (להלן – החוק או חוק הגנת הפרטיות) שהפרתו עשויה להגיע כדי עבירה פלילית או עוולה אזרחית. החוק עצמו מנסה לאזן בין אינטרסים של המעסיק האינטרסים של העובדים לאוטונומיה, לכבוד, לפרטיות ולאנונימיות. במקרים מסוימים החוק משאיר מרחב פרשני למי שבא בגדרו ולמי שמפרשים אותו לצורך מימוש עפ"י דין (הרשויות האוכפות, בתי המשפט). במסגרת פרשנות החוק נדרש איזון בין זכויות המעביד כמעסיק לבין זכויות היסוד של העובד, תוך התחשבות בהכרת הדין בגישה מרחיבה לזכות העובד לפרטיות במקום העבודה.<sup>3</sup>
3. מטרתו של מסמך זה להצביע על העקרונות החלים ביחס לזכות לפרטיות במידע במקום העבודה, ולהראות את אופן יישומם של עקרונות אלה לגבי מידע על אודות עובדים, שנאסף ונצבר בידי מעסיקים. **המסמך משקף את עמדת רשם מאגרי מידע** בעניין אופן העמידה בהוראות החוק בעת האיסוף העיבוד וניהול המידע הממוחשב במאגר המידע המשרת מטרה זו. בהתאם לכך המסמך יכול לסייע למעסיקים בציות לחוק, כמו גם לשמש כלי עזר למועסקים להכיר את זכויותיהם בהקשר להגנת המידע האישי אודותם.
4. תחולתו של המסמך נוגעת לסוגיות פרטיות במידע אצל כל סוגי המעסיקים, פרטיים וציבוריים, מסחריים וללא כוונת רווח, אם כי הוא איננו דן באופן מקיף וממצה בהיבטים

<sup>1</sup> מידע מוגדר בסעיף 7 לחוק הגנת הפרטיות- "נתונים על אישיות של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונותיו", ועקרונות החוק הוחלו בפסיקת בתי המשפט גם על "ידיעה על עניינו הפרטים של אדם", תוך התבוננות על ההקשר בו מדובר. ראה למשל: ראה ע"א 439/88 **רשם מאגרי המידע נ' ונטורה**, פ"ד מ"ח (3), 808, ע"מ 9341/05 **התנועה לחופש מידע נ' רשות החברות הממשלתיות**, בפסקה 23.

<sup>2</sup> היקפה וגבולה של הפררוגטיבה של המעביד נותחו בפסיקת בית הדין הארצי לעבודה לאורך השנים. ראו למשל דב"ע 7/03 – 3 **נחום לבון נ' מ.ת.מ. מבני תעשייה ומלאכה בע"מ**, פד"ע לב, 584 ולאחרונה ע"ע 90/08 טלי איסקוב ענבר נ' מדינת ישראל (טרם פורסם, 08.02.2011) (להלן: עניין איסקוב)

<sup>3</sup> עניין איסקוב, לעיל ה"ש 2, בעמ' 21.



נוספים של פרטיות עובדים, שאינם קשורים לפרטיות במידע דווקא, כגון אלה הנדונים בפרק א' לחוק הגנת הפרטיות, ובסוגיות משיקות מחוץ לדיני הפרטיות, הנדונות בדברי חקיקה ספציפיים כגון חוק שוויון הזדמנויות בעבודה, התשמ"ח-1988 הנזכר להלן.

5. בחלק הראשון למדריך יוצגו העקרונות הכלליים החלים על איסוף ועיבוד מידע במקום העבודה. בחלק השני יידונו באופן קונקרטי יותר עקרונות אלה בהקשר למחזור החיים של ניהול המידע במקום העבודה. בחלק השלישי תידון סוגיית המעקב אחרי עובדים בעת השימוש בטכנולוגיות מידע.

6. למען הסר ספק, הניסוח במסמך זה הינו בלשון זכר וזאת מטעמי נוחיות בלבד. יש לקרוא את האמור בלשון זכר לפי העניין, כאילו נאמר בלשון נקבה.



## חלק א' - עקרונות הגנת הפרטיות במידע במקום העבודה

### 1. מבוא - תחולת החוק

1.1. מעסיקים צוברים במסגרת פעילותם מידע אודות עובדים ומועמדים לעבודה. נתונים כגון משכורת, השכלה, הכשרה מקצועית, תאריכי לידה ופרטי זיהוי נוספים של העובד ושל בני משפחתו, סוג הביטוח הפנסיוני, דיווחי שעות עבודה, השתייכותו של העובד לארגוני עובדים ולעתים גם חוות דעת רפואיות, פסיכולוגיות או תעסוקתיות אודות העובד. לאלה מצטרף מידע נוסף הנצבר במסגרת מערכות המידע של הארגון, כגון מסרי דואר אלקטרוני או רישומים אודות השימוש באינטרנט, שימוש באמצעי תקשורת אחרים (טלפון נייד, טלפון ניחן), וכן מידע אבטחתי ומנהלי אחר, כגון צילומים במצלמות מעקב. כל אלה מהווים מידע פרטי אודות העובד, אשר חוק הגנת הפרטיות חל עליו.<sup>4</sup>

1.2. עיבוד המידע האמור במערכות המידע של המעביד נעשה בדרך כלל בכל שלבי ההעסקה – משלב המועמדות עד סיום העסקת העובד, וגם לאחריה מתבצע לעיתים עיבוד של מידע קיים שנאסף קודם לכן. מערכת המידע משמשת להזנה, שמירה, ניתוח והפקה של מידע אודות אדם. מכאן שמבוצעות פעולות של עיבוד ממוחשב – במובן זה שהמערכת מאפשרת למי שמפעיל אותה, להזין, לצפות או להפיק מידע השמור בה – אודות אדם מסוים.

1.3. תכליתו המיוחדת של פרק ב' לחוק הגנת הפרטיות, היא להטיל חובות ביחס למי ששומר ומעבד מידע באופן ממוחשב, וזאת בשל הסיכונים המיוחדים לפרטיות הנובעים מצבירת המידע בפורמט הניתן לעיבוד ממוחשב. בין סיכונים אלה ניתן למנות את קלות ההעתקה, ההעברה והגילוי של המידע, וכן פוטנציאל החשיפה הבלתי מורשה שלו לגורמים רבים בו זמנית.

1.4. מכאן ש-"מאגר מידע" אינה הגדרה טכנולוגית אלא הגדרה משפטית – כלומר היא חלה על כלל מערכות המידע המכילות מידע אודות אנשים, וזאת משום הסיכונים לפרטיות הטמונים במערכות אלה. צורת ניהול המידע יכולה להיות מגוונת: מארגון גדול אשר מנהל את כל המידע במערכת מידע ארגונית אחודה (דוגמת מערכות ERP),

<sup>4</sup> על פרטיות במקום העבודה באופן כללי ראו גם ב- דב"ע 4-70/97 אוניברסיטת תל-אביב נ' ההסתדרות הכללית, פד"ע ל 385 (להלן: פסי"ד אוניברסיטת ת"א). בית הדין לעבודה קבע במספר מקרים כי לעובדים, ישנה זכות לפרטיות במקום העבודה ראה לדוגמה בש"א (ירושלים) 1372/99 אילן מנס נ' רשות השידור, תק-עב (1), 2000, 3032; בנוסף בית הדין לעבודה מגן על פרטיות של צדדים שלישיים, שאינם חלק מההליך המשפטי, אשר פרטיותם יכולה להיפגע, במקרים בהם ישנה פגיעה בפרטיות של עובד- על כך ראו למשל ב: ביה"ד האזורי לעבודה – תב"ע (אזורי ת"א) 7541/01 פרופ' שמעון עבוד נ' קרד גרד הישרדות מדעית בע"מ, תק-עב (2), 2002, 2903.



עד לעסק קטן המנהל את המידע במערכת הדואר האלקטרוני שלו וביישומים מקומיים כגון גיליונות אלקטרוניים ומעבדי תמלילים.

1.5. על רקע זה קובעים דיני הגנת הפרטיות הוראות על אופן השימוש והשמירה על מידע.

1.6. בעוד פרק א' לחוק הגנת הפרטיות דן בזכות לפרטיות באופן כללי, פרק ב' לחוק קובע הסדר ספציפי בנושא אחזקת מאגרי מידע וניהולם. בעניין זה יש להבהיר כי העיסוק הספציפי של המחוקק במאגרי המידע נועד להוסיף חובות על מי שצובר ומעבד מידע באמצעים ממוחשבים, ולא לתת הכשר לאסוף או להחזיק מידע כאשר הדבר אינו מותר מכוח הסכמה תקפה של נושא המידע או מכוח בסיס חוקי אחר.

1.7. לצד זכותו הלגיטימית של המעביד לנהל את עסקו ולצורך כך לאסוף או להשתמש במידע אישי, עליו להיות מודע לחובות הנגזרות מהחוק ומזכויות היסוד של העובד. הפרוגטיבה הניהולית כפופה לדרישות הסבירות, המידתיות, תום הלב וההגינות.<sup>5</sup> העובד זכאי לפרטיות מפני מעקב וחדירה לפרטיותו, וטענות הגנה של המעביד להצדקת הפגיעה בפרטיות יפורשו בצמצום ובדווקנות.<sup>6</sup> פגיעה בפרטיות, בשל עיבוד מידע שלא לפי הוראות החוק, בשל חשיפה למידע אישי או שימוש לא מורשה במידע אישי שמנוהל על ידו, חושפת את המעביד להליכי אכיפה אזרחיים ואף לחיוב לתשלום פיצוי ללא הוכחת נזק.<sup>7</sup> כן, יתכנו הליכי אכיפה על ידי הרשם העלולים להסתיים במקרים מסוימים גם בהטלתה של אחריות פלילית.

## 2. עקרון ראשון - הסכמה מדעת

2.1. ככלל, קובע סעיף 1 לחוק הגנת הפרטיות<sup>8</sup> את העיקרון היסודי המבסס את השליטה של אדם במידע אודותיו - האפשרות "להסכים" לשימוש<sup>9</sup> במידע אישי אודותיו. על מנת להגן על אותה הסכמה, החוק מוסיף וקובע כי על ההסכמה להיות "הסכמה מדעת",<sup>10</sup> כלומר כזו המאפשרת לנושא המידע המוסר את המידע לקבל על בסיסה החלטה בדבר הסכמה או אי הסכמה לעניין איסוף השימוש במידע.

<sup>5</sup> עניין איסקוב, לעיל ה"ש 2, בעמ' 12-13.

<sup>6</sup> שם, בעמ' 16-17.

<sup>7</sup> כאשר העוולה או העבירה כרוכה בהפרה של פרק א' לחוק - ראו סעיף 29א.

<sup>8</sup> נוסח סעיף 1 לחוק הגנת הפרטיות: "לא יפגע אדם בפרטיותו של זולתו ללא הסכמתו."

<sup>9</sup> סעיף 3 לחוק הגנת הפרטיות מגדיר שימוש: "לרבות גילוי, העברה ומסירה."

<sup>10</sup> הסכמה הנדרשת צריכה להיות הסכמה מדעת, כך נדרש באופן מפורש מאז התיקון לחוק משנת 2007, בו תוקן סעיף 3 לחוק





2.2. עם זאת, תובנה מקובלת בדיני העבודה בישראל,<sup>11</sup> בהתאם למקובל גם בדיני העבודה בעולם, היא שהסכמה של עובד או מועמד לעבודה, אינה משקפת בהכרח בחירה חופשית לגבי מהות התנאים הקשורים במשא ומתן לקראת **התקשרות ובהתקשרות**. זאת בשל פערי הכוחות המובנים בין המעביד לעובד.

2.3. מכאן שתוקפה של הסכמה של עובד לאיסוף או לשימוש במידע לפי החוק בידי מעביד, אינה בעלת משקל רב, אלא אם ברור מהנסיבות כי ניתנה באופן חופשי לגמרי.<sup>12</sup> לפי פסיקת בתי המשפט גם נקבע שיש לבחון את נסיבות השימוש במידע, בהתאם לעקרונות-העל של ההגנה החוקתית על מידע, שמקורם כיום בחוק יסוד: כבוד האדם וחירותו, תוך איזון בין האינטרסים הלגיטימיים של המעביד והעובד, ובמרכזם דרישת המידתיות.<sup>13</sup>

### 3. עקרון שני - תכלית ראויה

3.1. על המעביד לאסוף ולעבד מידע רק לתכלית ראויה.<sup>14</sup> עקרון זה, אשר נגזר מחוק יסוד: כבוד האדם וחירותו, תוחם את האפשרויות של איסוף ועיבוד מידע. משכך, יש לקבוע את המטרות הספציפיות לאיסוף ועיבוד המידע, ועל אלה לעלות בקנה אחד עם התכלית העסקית של המעביד והמטרות החיוניות למקום העבודה או להתבסס על מקור אחר, כגון דרישת גורמי פיקוח מסוגים שונים (כגון בטיחות בעבודה, רשות המיסים וכד') לאסוף את המידע. לכן, לדוגמה, מעביד אינו רשאי לאסוף מידע שאינו נדרש לצורך העסקה או מימוש התכלית העסקית של העסק.

3.2. לכן עבור כל פריט מידע שנאסף, על המעסיק להיות מסוגל לספק הסבר משכנע לתכלית איסוף המידע. על המעסיק גם לבחון מעת לעת את שדות המידע במערכות האיסוף שלו ובטפסים בהם הוא מבקש להשתמש, ולבחון אם אלו עדיין מקיימים את תכלית אסיפת המידע, ולשנותם בהתאם לצורך.

<sup>11</sup> ראו פס"ד אוניברסיטת ת"א, לעיל ה"ש 4, פסקה 22.

<sup>12</sup> דוגמה אפשרית היא הסכמה למסירת המידע לצורך קבלת הטבה או שירות שאינו מותנה בהמשך העבודה – למשל רכישת תווי שי, או מצב שבו מדובר בעובד בעל כוח מיקוח חזק במיוחד (כוכב טלוויזיה למשל, מול חברת הפקה)

<sup>13</sup> גם השימוש בהסכמים קיבוציים הוא פתרון אפשרי לבעיית ההסכמה הנובעת מפער הכוחות בין העובדים לבין המעבידים. ניהול מו"מ ומתן הסכמה של הארגון היציג עשויה לשמש תחליף מועצם להסכמה פרטנית של כל עובד בנפרד, וגם מצד המעסיקים מספק ההסכם הקיבוצי ודאות רבה יותר בהשוואה לשימוש במבחני המידתיות כמפורט לעיל. הסכם קיבוצי כללי המסדיר את זכות העובדים לפרטיות בשימוש במערכות מחשב במקום העבודה ואת זכויות המעסיקים לנטר את פעולות העובדים, נחתם ביום 25.6.2008 בין ההסתדרות לבין לשכת התיאום של הארגונים הכלכליים במשק.

<sup>14</sup> עקרון התכלית הראויה אינו קבוע מפורשות בחוק הגנת הפרטיות והוא נגזר בהתאם לחוק היסוד וממקורות נוספים – להרחבה על כך ראו במאמרו של מיכאל בירנהק "מעקב בעבודה: טיילור, בנתי'האם והזכות לפרטיות" **עבודה חברה ומשפט** יב 9, 17-18 (2010) (להלן: מ' בירנהק "מעקב בעבודה").



#### 4. עקרון שלישי - מידתיות

4.1 בהתאם למשפט העבודה בישראל, יש להחיל את עקרון המידתיות בשל חולשת ההסכמה ביחסי עבודה, כמבחן לביצוע האיזון בין זכויות המעביד לזכויות העובד ביחס לפרטיות.<sup>15</sup>

4.2 עקרון המידתיות מורכב משלושה מבחני משנה:<sup>16</sup>

4.2.1 האם ישנה התאמה בין האמצעי למטרה הלגיטימית שנבדקה?

4.2.2 האם האמצעי שנעשה בו שימוש הינו האמצעי שמביא לפגיעה מינימאלית בזכות?

4.2.3 האם קיים יחס ראוי בין התועלת מהשימוש באמצעי להגשמת התכלית - לבין הנזק שייגרם מהשימוש בו?

4.3 בהתאם לעיקרון יש לבחון שימוש באמצעים טכנולוגיים הפוגעים במידה הפחותה ביותר בפרטיות העובדים.

#### 5. עקרון רביעי - שקיפות - מסירת הודעה על איסוף ושימוש במידע

5.1 בעל מאגר האוסף מידע מאדם, חייב בהתאם לסעיף 11 לחוק, למסור למי שממנו נאסף המידע, הודעה בדבר השימושים במידע. הודעה כזו נדרשת גם לצורך קבלת הסכמה מדעת לפי החוק.

5.2 חובת ההודעה חשובה במיוחד ביחסי עובד-מעביד על רקע העדר הרלבנטיות המעשית, ברוב רובם של המקרים, של ההסכמה מדעת. יש להעיר כי קיום חובת ההודעה על מדיניות איסוף ועיבוד המידע של המעביד במסגרת חוזה העבודה, אינה פוטרת מהודעה נוספת במקרה של שינויים עתידיים במטרות השימוש במידע, כגון אלו הנובעים מתנאים חדשים שמציב המעביד או משינויים טכנולוגיים.

5.3 על המעביד ליידע, באופן מפורט וברור את כל עובדיו בדבר המידע אשר נאסף, מוחזק ומעובד אודותם, השימושים והמטרה לשמה מוחזק כל פריט של המידע. במידה שמידע מועבר לצדדים שלישיים, יש להודיע על זהותם והמטרה של העברת המידע.<sup>17</sup> הפרת החובה היא עבירה פלילית לפי סעיף 31א(א)(3) לחוק הגנת הפרטיות.

<sup>15</sup> ראו הצדקות לקיומו של עקרון המידתיות ביחסי עובד מעביד במאמרו של גיא דוידוב "עקרון המידתיות בעבודה" **עיוני משפט** לא 5 (2008).

<sup>16</sup> ראו דבי"ע אוניברסיטת תל אביב, ה"ש 2 לעיל, וענין איסקוב, ה"ש 4 לעיל. להרחבה ראו גם דוידוב, ה"ש 15 לעיל.  
<sup>17</sup> סעיף 11 לחוק הגנת הפרטיות קובע: "פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע תלווה בהודעה שצוינו בה-

(1) אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע לתויה ברצונו ובהסכמתו;



- 5.4 באופן מעשי, על המעביד להודיע לעובדיו את עיקרי מדיניות עיבוד המידע על ידו. מומלץ לפרסם ולעדכן מעת לעת במקום העבודה, הנחיה פנימית תמציתית ובהירה אשר תיקרא "מדיניות הפרטיות של החברה", ותבהיר נושא זה לעובדים.
- 5.5 יש לציין כי בית הדין הארצי לעבודה ממליץ למקום העבודה לשקול מינוי של "נאמני פרטיות בטכנולוגיות מידע במקום העבודה"<sup>18</sup>. עמדת הרשם הינה כי נושא זה הינו באחריות של מנהל המאגר, שכמובן יכול מנות בעל תפקיד בעל הכשרה מתאימה למלא חלק מחובות אלה.
6. עקרון חמישי - הגבלת מטרה:
- 6.1 עקרון יסודי בדיני הפרטיות, הינו כי השימוש במידע שנמסר על ידי אדם או התקבל למטרה חוקית מסוימת, לא ישמש אלא למטרה זו. כך, בהתאם לסעיף 2(9) לחוק, על המעביד לוודא כי כל השימושים הנעשים במידע ייעשו רק למטרה שלשמה נמסרו.<sup>19</sup> החובה לקיים את השימוש והמטרה הינה על המעביד בכל מקרה קונקרטי.
7. עקרון שישי - סודיות ואבטחת מידע:
- 7.1 הוראות אבטחת מידע נועדו למזער את הסיכונים למידע במערכות המידע המשמשות את מאגרי המידע. הסכנה עלולה להגיע מבחוץ (כגון פריצה למחשבים) או מבפנים (כגון פגיעה מכוונת או רשלנית בידי עובד).
- 7.2 על המעביד לבחון איזה מידע אישי מצוי במערכות המידע שלו, מהם הסיכונים לשימוש לרעה במידע (מבחוץ או מבפנים) ולפגיעה בעובד בשל כך, ולנקוט אמצעים מקובלים להגן על המידע. את האמצעים השונים שנקטים יש לבחון מעת לעת, לפי ההתפתחויות הטכנולוגיות, ולעדכן את רמת האבטחה בהתאם. במילים אחרות, החובה איננה רק חד-פעמית, אלא נמשכת כל עוד מוחזק המידע.
- 7.3 יודגש כי אבטחת מידע אינה רק אוסף של אמצעים טכניים, אלא בעיקר מחייבת מדיניות ונהלים ארגונים שיועברו לכלל העובדים העוסקים במידע. כך למשל, בכל הקשור לעיבוד מידע אישי אודות עובדים, למנהל משאבי האנוש תפקיד חשוב משום שמנהל משאבי האנוש הוא המגדיר מיהם המורשים הלגיטימיים לצפייה במידע בתיקי

(2) המטרה אשר לשמה מבוקש המידע;

(3) למי יימסר המידע ומטרות המסירה.

<sup>18</sup> עניין איסקוב, לעיל ה"ש 2, בעמ' 35.

<sup>19</sup> דרישה זו קבועה מפורשות בחוק הגנת הפרטיות בסעיף 2(9) אשר קובע מקרה אשר מהווה פגיעה בפרטיות בלשון: "שימוש בידעה על עניינו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה שנמסרה".



העובד, לאילו מטרות, ובאילו נסיבות ניתן למסור מידע מתיקים אלה לגורמים אחרים בארגון או במקרים מתאימים, ולפי הוראות הדין, מחוצה לו.

8. עקרון שביעי - חובות ביחס לביצוע פעולות במיקור חוץ:

8.1 ארגונים רבים מבצעים חלק מעיבוד המידע, ובכלל זה עיבוד מידע אישי, באמצעות נותני שירותים חיצוניים, כלומר בדרך של מיקור חוץ. נותני השירותים מכונים בחוק הגנת הפרטיות "מחזיק". חשוב להדגיש כי ארגון המעבד מידע אינו יוצא ידי חובותיו לפי החוק בכך שעיבוד המידע נעשה בידי קבלן משנה. הן המחזיק והן המעסיק כפופים להוראות הדין.

8.2 על ארגון המעבד מידע באמצעות מחזיק חלה החובה להסדיר בחוזה מחייב, כחלק מהגדרת השירות, גם את ההוראות הרלבנטיות החלות בתחום הגנת הפרטיות, ולוודא גם לאחר החתימה על החוזה, כי המידע האישי מנוהל כראוי. על ארגון המעביר מידע למיקור חוץ חובה נמשכת לוודא כי המידע מטופל כראוי (כלומר שנשמרים העקרונות השונים המפורטים כאן), לרבות קבלת מידע מהמחזיק או ביצוע בדיקות לשם בקרה, לפי העניין.<sup>20</sup>

9. עקרון שמיני - עיון ותיקון:

9.1 על המעביד לאפשר לכל עובד לעיין במידע אשר מוחזק אודותיו במקום עבודתו.<sup>21</sup> זאת במגבלה שיש לאפשר עיון במידע כל עוד העיון לא פוגע בפרטיות של עובדים אחרים או בחסיונות משפטיים אחרים. במידה שהמידע אינו מדויק, יש לאפשר את תיקון המידע.<sup>22</sup>

10. סיכום ביניים

10.1 על מעביד להביא בחשבון כי כאשר הוא אוסף ומעבד מידע אישי אודות עובדיו, חלים עליו העקרונות האמורים לעיל. בהמשך ההנחיה יוצג יישום של עקרונות אלו במסגרת יחסי עובד מעביד, בהתחשב במחזור החיים של המידע במקום העבודה. כמו-כן, יוצגו המלצות למימוש עקרונות אלו.

<sup>20</sup> ראו הנחיית רשם מאגרי המידע מס' 2/2011: "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי" - <http://www.justice.gov.il/NR/rdonlyres/805B34A2-6D8F-481E-A9B2-BEC934ECDA84/31589/22011.pdf>

<sup>21</sup> סעיף 13 לחוק הגנת הפרטיות קובע מפורשות: "(א) כל אדם זכאי לעיין... במידע שעליו מוחזק המוחזק במאגר מידע."

<sup>22</sup> סעיף 14 לחוק הגנת הפרטיות קובע: "(א) אדם שעיין במידע שעליו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל מאגר המידע... בבקשה לתקן את המידע או למוחקו."



## חלק ב' - עיבוד מידע אישי במקום העבודה

בפרק הקודם נסקרו בקצרה העקרונות המרכזיים של דיני הפרטיות הרלבנטיים למקום העבודה. כאמור, אין בכך מיצוי של החובות, וההתמקדות כאן היא בהגנת מידע אישי. בפרק זה ידונו בצורה מפורטת יותר מימוש העקרונות בשלבים השונים של הליך ההעסקה, וכן ביחס לסוגיות קונקרטיות הקשורות במקום העבודה.

לעתים קרובות מעבידים ועובדים אינם מודעים להיקף המידע האישי, מבחינת כמות ואיכות המידע, אשר אוסף המעביד במסגרת העסקתו של העובד, לרבות במסגרת שקילת מועמדותו לעבודה. חלק זה של המסמך נועד לאפשר למעביד לזהות היכן וכיצד הוא אוסף מידע אישי אודות מועמדים ועובדים, ולהחיל על כך את עקרונות החוק.

### 1. שלב ראשון: ניהול המידע מתחיל בשלב הגיוס לעבודה - טרום העסקה

1.1 בשלב הגיוס והמיון לעבודה, המעסיק אוסף מידע רב לגבי מועמדים פוטנציאליים לעבודה. בין אלה ניתן למנות ניסיון תעסוקתי, פרטי השכלה, מצב משפחתי, עיסוקים נוספים, כישורים שונים, ועוד.

1.2 בהמשך הליך המיון נאסף לעתים מידע אישי נוסף על אודות המועמד. מידע זה יכול להיאסף בראיונות אישיים, במבדקי הערכה, מעבר על המלצות, אימות המידע ועוד.

### 1.3 הגשת מועמדות לעבודה

1.3.1 מקובל כי הגשת מועמדות למקומות העבודה, הינה העברת מידע אודות המועמדים בצורת מסמך קורות חיים או טופסי מועמדות, וזהו רוב המידע אשר מועבר למעבידים בשלב הראשוני. קורות החיים והטפסים מכילים מידע רב אודות העובדים,<sup>23</sup> כאשר עקרונות הגנת הפרטיות חלים על פרטי מידע אלו.

### נקודות לבדיקה עצמית של המעביד:

- איזה מידע נשאל בטפסים? האם יש הכרח בכל אחד מפרטי המידע? המעסיק צריך להיות מסוגל להסביר את הרלוונטיות של כל פריט מידע שמתבקש.
- האם טפסי המועמדות/קורות החיים מועברים או יועברו גם לצדדים נוספים?
- אם כן –

<sup>23</sup> רוב מסמכי קורות החיים, אפילו הבסיסיים שבהם יענו להגדרה של עניניו הפרטיים של אדם לפי סעיף 2(9) ולפיכך חובות החוק חלות על קורות החיים. להרחבה על פרשנות סעיף 2(9) ראו: פרשת **ונטורה**, לעיל ה"ש 1, בעמ' 821-822.



1. למי ולאילו מטרה?
  2. האם העברה זו הכרחית?
  3. האם התקבלה ההסכמה מדעת לכך מצד המועמד, לפני איסוף ולפני העברת המידע?
- האם קורות החיים המתקבלים ממועמדים נשמרים כך שהם נגישים רק למי שצריך לגשת אליהם? האם ננקטו אמצעי אבטחה ונהלי הרשאת גישה מתאימים בעניין?

#### 1.4 ראיונות עבודה

1.4.1 במסגרת ראיונות עבודה, נאסף מידע על אודות המועמד, ונעשה עיבוד נוסף שלו. לעתים נעשית תרשומת מהראיון על מנת לאפשר הערכה משווה של כל המרואיינים. המידע הנאסף הינו מידע אישי מאוד על המועמד, ולא רק על ניסיונו התעסוקתי, אלא לעיתים גם על עניינים אישיים שונים כגון מצבו המשפחתי, עיסוקיו האחרים, הרגליו, כיצד הוא אוהב לבלות בזמן הפנוי, תוכניותיו לעתיד ועוד. מדובר במידע רגיש ביותר אודות העובד, אשר דורש תשומת לב יתרה.

#### נקודות לבדיקה עצמית של המעביד:

- אילו שאלות נשאלות? אין לשאול שאלות שאינן רלוונטיות להערכת התאמתו של העובד למקום העבודה. האיסור נובע הן מדיני הגנת הפרטיות, והן מדיני שוויון הזדמנויות בעבודה.
- האם נעשית תרשומת בזמן ראיונות?
- אם כן, האם התרשומות נשמרות בתום הליך המיון?
- איזה מידע נוסף נאסף בהליך המיון?
- אם כן, למי יש גישה במקום העבודה למידע זה? האם נקבעו נהלים מתאימים לשמירת המידע, למניעת העברתו לצדדים שלישיים?

#### 1.5 מבחני מיון והתאמה לעבודה

1.5.1 מעסיקים רבים עושים שימוש במבדקי התאמה כחלק מהליך מיון מועמדים לקבלה לעבודה או לצורך קידום עובדים. פעילות זו מבוצעת לעתים קרובות באמצעות מכוני מיון המתמחים בפעילות זו.





1.5.2 ביום 28.2.2012 פרסם רשם מאגרי המידע הנחייה מקיפה בדבר **'תחולת**

**הוראות חוק הגנת הפרטיות על הליכי מיון לקבלה לעבודה ופעילות מכוני מיון**"<sup>24</sup>. ההנחייה מופנית הן למעסיקים והן למכוני המיון וחלה על הליכי המיון בין אם מבוצעים אצל המעסיק עצמו, ובין אם נשלחים למיקור חוץ במכון חיצוני. ההנחיה מבהירה את מעמדם של המעסיקים ומכוני המיון ביחס למידע שנאסף על המועמדים, מפרטת אלו שימושים מותר למכונים לעשות במידע האישי הנצבר אצלם, ומה תוכן ההסכמה שהמעסיק ובמיוחד המכון נדרשים לקבל מן המועמדים כתנאי לעיבוד המידע. הנחייה מדגישה את החובה לאפשר למועמד לעיין בחוות הדעת שהוכנה עבור המעסיק כתוצאה של המבחנים.

1.5.3 כדי לעמוד בהוראות הדין המפורטות בהנחיה, רצוי שהמעסיק יסדיר בהסכם בינו לבין המכון את הזכויות והחובות במידע אודות המועמדים. כך למשל, ניתן לקבוע מה בדיוק השימוש שרשאי המכון לעשות במידע, כיצד ומי אחראי לאפשר את זכות העיון, ומה משך הזמן שהמידע יישמר במכון המיון.

1.5.4 לגבי **תוכנם** של מבחני המיון, נקבע בפסק הדין בעניין אוניברסיטת ת"א,<sup>25</sup> כי "בנושאים הפוגעים בפרטיותם של העובד או של המועמד לעבודה, רשאי המעסיק להציג שאלות רק לצורך "תכלית ראויה" ו"במידה שאינה עולה על הנדרש". שכן, הזכות לפרטיות המעוגנת בחוק-יסוד: כבוד האדם וחירותו, מגבילה את המעסיק בבואו לחשוף פרטים אישיים אודות מועמד לעבודה באמצעות מבחני התאמה."<sup>26</sup>

1.5.5 מכאן שגם האחריות הכוללת לכך היא של המעסיק, ועליו לבדוק כי המבחנים שמתבצעים על ידו או על ידי צדדים שלישיים אינם פולשניים או אוספים מידע עודף אודות המועמד, באופן שאינו מידתי או שאינו נדרש לתפקיד. כך למשל קיומו של מבחן השואל שאלות אישיות או שאלות שאינן נוגעות לתחום עיסוקו ותפקידו של המועמד/העובד.

<sup>24</sup> נוסח ההנחיה מפורסם באתר רמו"ט בכתובת:

<http://www.justice.gov.il/MOJHeb/ILITA/Hanchayot/HanchayotDB/HanchayotDB.htm>

<sup>25</sup> ראו פס"ד **אוניברסיטת ת"א**, לעיל ה"ש 3.

<sup>26</sup> ורדה וירט-ליבנה "הזכות לפרטיות אל מול האחריות הניהולית במיון מועמדים לעבודה – ההיבט המשפטי" **ספר שמגר ג'** (תשס"ג), 775, 805-804: "גבולות הפררוגטיבה נקבעים מקום בו קיימת פגיעה בפרטיות, ומאחר שאין חולק כי מבחנים, מעצם מהותם, מהווים הפרת זכות העובד לפרטיות הרי שאין לכלול את נושא המבחנים כחלק מפררוגטיבת המעביד לנהל את המפעל, ויש להציב לה גבולות".



נקודות לבדיקה עצמית של המעביד:

- האם מבדקי ההתאמה תואמים את תכלית ההעסקה? כלומר, האם לתפקיד ספציפי נדרש לבחון תכונה או מידע אישי מסוים?
- האם נעשה שימוש במכון חיצוני?
- האם ידוע לך כיצד המכון החיצוני אשר מבצע את מבדקי ההתאמה שומר על סודיות ואבטחת המידע אודות המועמדים לעבודה אצלך?
- האם קבעת עם המכון החיצוני נוהל שיגדיר מראש, מה השימוש שעושה המכון במידע וכיצד ניתנת זכות העיון למועמדים?
- האם המועמדים נשאלים שאלות אשר לפי חוק אסור לשאול אותן?
- יש לקבוע נהלים ברורים למסירת הפרטים על כל אלה למועמדים, בצורה בהירה וברורה, לפני ביצוע המבחן.

1.6 מידע אשר איסופו אסור

1.6.1 בנוסף לחוק הגנת הפרטיות ולעקרונות שתוארו לעיל, ישנן הוראות חוק נוספות האוסרות איסוף או בירור פרטי מידע מסוימים לצורך קבלה לעבודה או קידום בה.<sup>27</sup> בשל הוראות חוק אלה, מעבר להוראות דיני הפרטיות, אין לאסוף פרטי מידע רגישים של עובדים המפורטים בהוראות חוק אלו, לצורך קבלת החלטות לגבי עובד/מועמד במקום העבודה.

1.6.2 מידע אשר אין לבקש ממועמדים/עובדים:

1.6.2.1 מידע גנטי.<sup>28</sup>

1.6.2.2 שאלות לגבי מרשם פלילי.

1.6.2.3 שאלות לגבי פרופיל צבאי.<sup>29</sup>

1.6.2.4 בקשת פרטי מידע מסוימים כגון דת, לאום, נטייה מינית, הורות, שירות במילואים – מטילים על המעסיק להוכיח שלא הפלה את דורש העבודה בניגוד לדין.<sup>30</sup>

<sup>27</sup> ראו ס' 8 לחוק שוויון הזדמנויות בעבודה, התשמ"ח-1988 וחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח-1998, וכן סעיף 3 לחוק המרשם הפלילי ותקנת השבים, התשמ"א-1981 הקובע כי המרשם יהיה חסוי וכי לא יימסר מידע ממנו אלא בהתאם לחוק.

<sup>28</sup> ראו סעיף 29 לחוק מידע גנטי, התשס"א-2000, ס"ח 290.

<sup>29</sup> סעיף 2 לחוק שוויון הזדמנויות בעבודה, התשמ"ח-1988 ("חוק השוויון").

<sup>30</sup> סעיף 9(ג) לחוק השוויון.





1.6.2.5 איסורים נוספים לפי החוק והפסיקה הרלוונטיים לעיסוק, בהתאם  
למקום העבודה.

נקודות לבדיקה עצמית של המעביד:

- האם ננקטו צעדים למניעת איסוף מידע אסור?

**1.7 סיכום - המלצות כלליות לקיום עקרונות הגנת הפרטיות בשלב המועמדות לעבודה**

1.7.1 בקבלה לעבודה מומלץ כי המועמדים יתבקשו לספק את המידע על אודותיהם  
בטפסי מועמדות המורכבים משדות ("רובריקות") מוגבלים ומוגדרים למידע  
הנדרש למועמדותיהם, וזאת בכדי למנוע איסוף של מידע עודף, אשר אינו נדרש.

1.7.2 אם ברצונך לשמור על מידע אודות מועמדים גם לאחר שלא התקבלו למשרה  
עליה התמודדו כיוון שיש להם פוטנציאל להיות מועסקים בעתיד, עליך לבקש  
את הסכמתם לשמירת המידע אודותם.

1.7.3 במקרים בהם ברור כי הארגון אינו מעוניין להעסיקם, על מנת למזער את החשש  
מפני שימוש לרעה במידע, יש למחוק כל מידע אודות מועמדים אלו, מיד כאשר  
הוא אינו נחוץ.

1.7.4 הקפדה על שמירת עקרונות אלה גם בידי גורמים חיצוניים (מכוני מיון) שבהם  
המעסיק נעזר.

2. שלב שני: ניהול תיק עובד - לאחר הקבלה לעבודה ובעת העבודה

**2.1 איסוף מידע במהלך העבודה:**

2.1.1 לאחר הקבלה לעבודה של העובד, ממשיך המעסיק לאסוף מידע על העובד  
במסגרת יחסי העבודה. חלק מהמידע נדרש לצורך קיום חובותיו של המעביד  
כלפי העובד. חלק אחר נאסף בשל דרישות רגולטוריות המחייבות את האיסוף  
והשמירה שלו. אף שאיסוף מידע זה לא נעשה ביוזמת המעביד, עליו להקפיד  
ולשמור עליו בהתאם להוראות החוק, ובכלל זה למנוע שימוש לרעה בו.



2.1.2. דרישות התכלית הראויה והמידתיות מחייבות כי איסוף מידע נוסף מידי העובד, ייעשה לצרכים לגיטימיים בלבד הקשורים בקיום יחסי העבודה. במקביל, יש למנוע שימוש במידע למטרות שאינן מטרות הקשורות ביחסי העבודה, וכן למנוע שימוש לרעה במידע.

2.1.3. ביחס לאישורי מחלה, יצוין כי התקנות<sup>31</sup> ליישום חוק דמי מחלה,<sup>32</sup> קובעות כי על העובד להמציא תעודות מחלה וכי על התעודה להכיל בין היתר נתונים לגבי אבחון המחלה.<sup>33</sup> איסוף המידע בדבר אבחוני המחלות שבתעודת המחלה יוצר פוטנציאל לקיומו של "מאגר מידע רפואי" בידי המעביד. במידה שאין צורך לגיטימי למעביד לשמירת הנתון לגבי אבחון המחלה של עובדיו, על המעביד להימנע מלאגור מידע זה במאגר מידע. במקרים בהם יחליט המעביד כי ישנה סיבה לגיטימית לשמירת המידע אודות מחלת עובד, יהיה עליו להגדיר באופן ברור מי רשאי לגשת למידע ולאלו מטרות וכמו-כן, יהיה עליו להקפיד במיוחד על הוראות אבטחת המידע.

2.1.4. לעתים נדרש המעסיק להעמיד את העובד לבדיקת אלכוהול או סמים. כיוון שמדובר במידע רגיש, ניתן לעשות שימוש בבדיקות אך ורק במקרים בהם ישנו קשר בין תוצאות הבדיקות הצפויות לבין תכלית העבודה וכאשר מתקבלת ההסכמה מדעת ומראש של העובד לביצוע הבדיקה.

#### נקודות לבדיקה עצמית של המעביד:

- איזה מידע נאסף במהלך השוטף של יחסי העבודה?
- מהן מטרות האיסוף של המידע הנוסף?
- איפה נשמר מידע זה?
- למי בארגון קיימת גישה למידע שנאסף?

#### 2.2. עקרונות כלליים לניהול המאגר

2.2.1. מטרתו של פרק ב' להקפיד על שימוש חוקי במידע, למטרות הלגיטימיות לשמן נאסף ולמניעת שימוש לרעה או פגיעה במידע.

<sup>31</sup> תקנות דמי מחלה (נהלים לתשלום דמי מחלה), התשל"ז – 1976, ק"ת 4.

<sup>32</sup> חוק דמי מחלה, התשל"ו – 1976, ס"ח 46.

<sup>33</sup> ראו בג"ץ 4308/08 קו לעובד נ' שר התמ"ת ואח': בעתירה זו, אשר הוגשה לאחרונה, טענה האגודה לזכויות האזרח כי בקשה של אבחון המחלה אינה מידתית ופוגעת בזכות לפרטיות של העובד; בעקבות העתירה הודיע משרד התמ"ת על כוונתו לתקן התקנות, אולם במועד פרסום מסמך זה התיקון טרם בוצע.



2.2.2. המעביד הוא ה"בעלים" של מאגר המידע, כפי משמעותה של בעלות זו על פי חוק הגנת הפרטיות והוא האחראי המרכזי לקיום החובות הנוגעות לקיום המאגר וניהולו לפי החוק. בהתאם לסעיף 7 לחוק הוגדר גם נושא משרה בהקשר החובות לפי החוק, שהינו "מנהל המאגר", כלומר נושא המשרה האחראי באופן אישי לקיום הוראות החוק. לפי החוק "מנהל המאגר" הינו "המנהל הפעיל של גוף שבבעלותו או בהחזקתו מאגר מידע, או מי שמנהל כאמור הסמיכו לעניין זה".

2.2.3. גם לאחר הקבלה לעבודה, מעבידים נוהגים לנהל "תיק עובד", בו נאסף מידע אודות העובד ובו נצבר מידע שוטף הקשור ביחסי העבודה. על ניהול תיק העובד במערכת מידע ממוחשבת, חל כאמור פרק ב' לחוק.

2.2.4. לעתים, פעילות העיבוד נעשית במיקור חוץ ("outsourcing"), כאשר מאגר המידע מצוי בידי צד שלישי, שאינו המעסיק עצמו, אשר נקרא בחוק "מחזיק". במקרים אלה, המידע התקבל אמנם מעובד של המעסיק, אולם פעולות העיבוד השוטפות, ומכאן גם השמירה, נעשית בידי צד שלישי.

2.2.5. נסקור להלן את חובותיו המרכזיים של בעל המאגר, מנהל המאגר, והמחזיק (ככל שקיים כזה). יובהר כי ביצוע הפעילות במיקור חוץ אינה מפחיתה מאחריותו הכוללת של בעל המאגר לקיום הוראות החוק, אלא לכל היותר משנה את המיקוד שלהן, מחובות הקשורות בביצוע ישירות על ידי המעסיק לחובות הקשורות בהסדרה של השירות בחוזה ופיקוח על קיום הוראות החוק. תחילה יסקרו העקרונות החלים על ניהול המאגר באופן כללי, ולאחר מכן המימוש של השינויים הנדרשים כאשר המאגר מנוהל במיקור חוץ.

#### נקודות לבדיקה עצמית של המעביד:

- מי הוא מנהל המאגר לפי החוק?
- מי קובע את מטרות השימוש במידע ומבקר זאת בארגון?
- האם חלק מהמידע נצבר אצל נותני שירות במיקור חוץ?

#### 2.3. ניהול המידע ואבטחת מידע:

2.3.1. סעיף 17 לחוק קובע כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע". בסעיף 7 מוגדר



הביטוי "אבטחת מידע" – "הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין".

2.3.2. הוראות בתחום אבטחת המידע משמשות אדן מרכזי לקיום הוראות החוק, משום שהן מביאות לצמצום החשש מפני שימוש לרעה או פגיעה במידע. יישום עקרונות המשנה המפורטים להלן נועד לסייע במימוש תכליות החוק - כלומר הגנה על זכויות נושאי המידע במאגר המידע, מפני שימוש לרעה הפוגע בפרטיות.

2.3.3. בנוסף, עמידה בעקרונות אלה גם תאפשר לארגון להציג לצדדים שלישיים – לקוחותיו, ספקיו, בתי משפט ורשם מאגרי מידע את אופן פעולתו ואופן התמודדותו עם חובותיו לפי החוק. כך, בעת אירוע שמהווה פגיעה בפרטיות במאגר מידע, מצבו של ארגון שנקט אמצעים סבירים למנוע את התרחשות הפגיעה, יהיה שונה מארגון שלא נקט אמצעים סבירים כאלה. להלן מפורטים הנושאים העיקריים הנוגעים לאבטחת מידע בטיפול במידע אודות עובדים.

2.3.4. בהתאם להוראות אלה, על המעסיק חלה אחריות לנהל את מאגר המידע באופן שהמידע יישמר בהתאם לדרישות אבטחת המידע. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986, מגדירות חובות אלה באופן קונקרטי יותר לגבי סוגי מאגרים מסוימים.<sup>34</sup>

2.3.5. לצד הוראות תקנות אלה, פרסמה רמ"ט נייר עמדה ובו הצעה לטיטת תקנות חדשות בנושא זה. התקנות מפורטות יותר מהנוסח הקיים.

2.3.6. להלן יוצגו דגשים לקיום חובות אלה בהקשר של ניהול מאגרי מידע בתחום יחסי העבודה.

#### נקודות לבדיקה עצמית של המעביד:

- האם לארגון יש מדיניות אבטחת מידע?
- האם קיים בארגון ממונה על אבטחה לפי סעיף 17 לחוק?
- אילו בקורות כלליות קיימות על קיום הוראות אבטחת המידע בארגון?

<sup>34</sup> רמ"ט פרסמה נייר עמדה בנושא זה, המציע הסדרה שלמה ומעודכנת יותר של נושא זה, ביחס למאגרי מידע באופן כללי. ראו: [http://www.justice.gov.il/NR/rdonlyres/8D081CC2-225B-4269-95F7-BF6860654DA4/18194/tyutat\\_takanot\\_avtachat\\_meida\\_100112.pdf](http://www.justice.gov.il/NR/rdonlyres/8D081CC2-225B-4269-95F7-BF6860654DA4/18194/tyutat_takanot_avtachat_meida_100112.pdf)



## 2.4 מיפוי והגדרת המידע המצוי במאגר

2.4.1. הטיפול בניהול המידע ושמירה עליו מפני שימוש לרעה צריכים להיות חלק משגרת ניהול המידע בפרט וניהול הארגון בכלל, ויש לבחון אותם מעת לעת ולעדכןם בהתאם להתפתחויות טכנולוגיות ולאיומים השונים על המידע.

2.4.2. בעל מאגר המידע צריך להכיר את פעילות עיבוד המידע המבוצעת על ידו, האפיון של המידע המצוי במאגר, דרגות הרגישות שלו, ולבחון את הסיכונים השונים לפעילות זו ולאופן ההתמודדות עימם. הגדרה ברורה של הנהלת הארגון בנושא זה משמשת נקודת מוצא חיונית לקבלת החלטות ומימוש האחריות הניהולית של בעל המאגר.

2.4.3. על הארגון להגדיר את הדברים במסמך אחיד על מנת לוודא תיאום בין נושאי המשרה השונים בתוך הארגון, בהקשר לחובותיהם השונות לפי תקנות אלה (כגון מנהל מערכות המידע, מנהל משאבי אנוש, קב"ט וכדומה).

2.4.4. כאשר מדובר על מעסיק המעביר את המידע לחו"ל, למשל כאשר מדובר בחברה בין-לאומית, ומבלי לגרוע משאר החובות לפי החוק, העברת המידע צריכה להיעשות בהתאם להוראות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001.<sup>35</sup>

### שאלות לבדיקה עצמית של המעביד:

- מהו המידע הנאסף ומנוהל על עובדים?
- האם יש מידע בעל רגישות מיוחדת (כגון מידע ביומטרי, בדיקות רפואיות, בדיקות פסיכולוגיות, נתונים סוציו-אקונומיים אחרים)?
- היכן נשמר המידע אודות עובדים ולמי יש גישה אליו?
- למי נדרשת הרשאה לגישה למידע ובאיזה אופן?
- מהם הסיכונים המרכזיים לפגיעה בשלמות המידע, חשיפתו או שימוש בו שלא כדין?
- האם מועבר מידע לחו"ל?

<sup>35</sup> תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001, ק"ת 900. ראו <http://www.justice.gov.il/NR/rdonlyres/8AA951FB-D9A5-498C-99B1-86647875D44C/9092/TakanotHul.pdf>



## 2.5. הוראות לעניין אבטחה פיזית:

2.5.1. יש לוודא כי מערכות המידע יישמרו במקום מוגן, אשר מתקיימים בו אמצעים למניעה של כניסה וחדירה למתחם ללא הרשאה. עמדות קצה המאפשרות גישה למידע אודות עובדים, לא יהיו נגישות פיזית לעובדים שאינם מורשים לכך, או לגורמים אחרים (כגון לקוחות, ספקים או נותני שירותים), ומחוץ לשעות הפעילות של הארגון.

### שאלות לבדיקה עצמית של המעביד:

- היכן נשמרות מערכות המידע המכילות את המאגר?
- האם בארגון מקפידים לנעול את החדרים בהם נשמר מידע?
- האם יש מערכות בקרה ואבטחה המנטרות את הגישה למערכות מחוץ לשעות הפעילות של הארגון?

## 2.6. הקפדה על גישה מורשית בלבד למידע

2.6.1. הדעת נותנת כי הגישה למאגרי המידע על עובדים צריכה להיות ככלל בידי מחלקת משאבי אנוש בלבד, ובמסגרתה רק בידי בעל התפקיד אשר מטפל בעובדים באופן ספציפי.

2.6.2. מכאן שבאחריות הממונה על משאבי אנוש במאגר, בתיאום עם הממונה על האבטחה, לקבוע את הסוגים וההיקף של ההרשאות לגישה למידע אודות עובדים. הקצאת ההרשאות תבוסס על גישת "צריך לדעת" שמשמעותה: אם עובד לא צריך גישה למידע מסוים לצורך עבודתו, אז הוא לא יקבל גישה לאותו מידע. כך למשל מתכנת בחברה אינו זקוק להרשאה לתיקים האישיים של יתר העובדים.

2.6.3. כאשר מדובר במערכות מידע אחרות, שאינן באחריות מחלקת משאבי אנוש, כגון מערכות ניהול קבצים המאפשרות שמירת מידע אישי, או מערכות הדואר האלקטרוני, האחריות התפעולית הכוללת היא של הנהלת הארגון ושל מנהל מערכות המידע. גם במערכות אלה יש לקבוע את סוגי ההרשאות ומטרתן. ככלל, כאשר מדובר על גישה למידע המנוהל על ידי העובד עצמו, יש ליידע אותו בטרם גישה למידע אודותיו, ורק בידי גורמים מוסמכים לביצוע תחזוקה או טיפול שוטף במערכות המידע.





2.6.4. על מנת לוודא כי הוראות אלה נשמרות, יש ליישם אמצעים מקובלים של תיעוד הגישה למאגרים, שמטרתם לוודא כי מי שניגש למידע במאגר המידע אכן מורשה לכך בהתאם להגדרות שתוארו לעיל.

#### שאלות לבדיקה עצמית של המעביד:

- מי מורשה גישה למידע?
- האם ההרשאות מבוססות על צורך ארגוני והאם יש מי שיש לו גישה עודפת?
- האם קיים ניהול מסודר של סיסמאות ואמצעי בקרה אחרים?

#### 2.7. אבטחת תקשורת וניהול מאובטח של מערכות מחשוב

2.7.1. בארגונים רבים קיימות רשתות מחשבים אשר מאפשרות גישה נרחבת למערכות המידע בהתאם להרשאות שניתנו. יסוד מרכזי באבטחה לוגית של מערכות המידע, מחייב התמודדות עם האיומים הנובעים מקישוריות וגישה למערכות המידע.

2.7.2. אמצעים מרכזיים המפחיתים את הסיכון למידע הינם:

2.7.2.1. הפרדה: מוצע להפריד בין מערכות המחשוב המשמשות את מאגרי המידע

אודות העובדים לבין שאר מערכות המחשב. הפרדה זו אינה חייבת להיות מוחלטת. קיימות מספר שיטות להפרדה זו, וביניהם: מערכת חומת אש פנימית, מערכת לחלוקת רשתות, ועוד.

2.7.2.2. הגנות מיוחדות לקישוריות לרשת האינטרנט: במקרה בו המערכות מתחברות לרשת האינטרנט, יש להתקין על גביהן אמצעי הגנה סבירים מפני חדירה לא מורשית, או תוכנות מזיקות.

2.7.2.3. גישה מרחוק: יש לקיים מנגנוני אבטחה כאשר ישנה אפשרות לגישה מרחוק למערכות המחשב ולמידע במקום העבודה. בארגונים בהם עובדים יכולים לגשת מרחוק למשאבי הארגון, ובכלל זה מערכות המידע המכילות מידע אודות עובדים יש ליישם אמצעים המבטיחים כי נשמרת רמת ההרשאה שנקבעה בארגון, וכי רק עובדים מורשים ניגשים למידע.

2.7.2.4. מעקב ובקרה: מוצע לקבוע הוראות לעניין רישומים אוטומטיים במערכות המידע של הארגון, וכי אחראי האבטחה או צוותו יעשו שימוש ברישומים סטנדרטיים, ובמידת הצורך ובהתאם לארגון, גם יוטמעו בארגון מנגנונים ייעודיים המנהלים רישום אוטומטי אודות פעילות ברשת הארגון.



שאלות לבדיקה עצמית של המעביד:

- האם מערכות המידע של הארגון מחוברות לאינטרנט? במידה שכן, האם יושמו אמצעי אבטחה והגנה מקובלים?
- האם ניתן לגשת מרחוק אל משאבי המידע של הארגון? האם עובדים יכולים לגשת למידע מהבית?
- האם יש תיעוד שוטף של הגישה והשימוש במידע?

**2.8. הדרכת עובדים ביחס לחובותיהם בתחום הגנת הפרטיות**

2.8.1. הגורם האנושי הינו גורם סיכון משמעותי בתחום אבטחת מידע. תובנה מקובלת המבוססת על לימוד של תקלות אבטחה, מלמדת כי שיעור גבוה של תקלות שכאלה נובע מהתנהלות כוח האדם בארגון.

2.8.2. כחלק ממערך הצעדים הננקטים על מנת לשמור על אבטחת המידע שבמאגר, יש לוודא כי ייקלטו לעבודה הקשורה למאגר המידע, רק עובדים המתאימים לעבודה זו, מבחינת אמינותם ויושרם. את רמת הסיווג הנדרש יש להתאים לרגישות המידע במאגרים, ולאופי הארגון שבו מתעתד המועמד לעבוד.

2.8.3. יש להבהיר לעובד החדש, בטרם יקבל גישה למאגרים, את חובותיו לפי חוק הגנת הפרטיות המפורטות במדריך זה, ולפי מדיניות הארגון. את הבהרת חובותיו ניתן לממש בצורה של הדרכה מובנית לעובדים חדשים, שתועבר על ידי אחראי אבטחת המידע, או על ידי גורם מתאים אחר, ורצוי אף באמצעות חוברת מידע בסיסית המבהירה נושא זה.

2.8.4. טרם קבלת הגישה למאגר, ולאחר הבהרת החובות לפי חוק לעובד החדש, יחתום העובד על התחייבות לשמירת סודיות בקשר למידע אליו הוא נחשף במסגרת עבודתו עם מאגרי המידע של הארגון, התחייבות זו תואמת להוראות סעיף 16 לחוק.

2.8.5. בנוסף על האמור לעיל, על מנת לרענן את חשיבות אבטחת המידע ואת החובות הנובעות ממנה, מוצע לערוך בארגון פעילויות הדרכה תקופתיות. פעילויות ההדרכה יכללו סקירה של מסמכי האבטחה המחייבים בארגון.





2.8.6. יש לוודא כי עובדים מודעים לסכנה שגורמים שונים ינסו לרמות או להונות אותם על מנת לגרום להם להוציא מידע מהמאגר בדרכי מרמה<sup>36</sup> ואת חובתם של העובדים לבדוק כי מידע המופק מהמאגר ניתן רק למי שזכאי לכך.

שאלות לבדיקה עצמית של המעביד:

- האם נקבעה מדיניות לעניין שימוש העובדים במאגרי המידע בארגון?
- האם עיקרי המדיניות הובאה לידיעת העובדים?
- כיצד נבדקת מהימנות עובדים בארגון בעת מתן הרשאות גישה למידע?
- האם עובדים בעלי הרשאות גישה למידע מהמאגר תודרכו לגבי אפשרויות הונאה שלהם?

2.9. **מיקור חוץ (OUTSOURCING)**<sup>37</sup>

2.9.1. ארגונים רבים בוחרים לבצע את עיבוד המידע, ולעתים גם את איסופו, בעזרת חברות חיצוניות. המשמעות היא שלצד שלישי שאינו המעביד עובר מידע רב לצורך מתן שירות למעביד.

2.9.2. **העברות אלו אינן פוטרות את הארגון מחובותיו לפי החוק.** חובתו של הארגון המעביר מידע לצד שלישי, לקבוע אמצעים משלימים שמטרתם התמודדות עם הסיכונים הנובעים מהעברת המידע לצד שלישי.

2.9.3. על המעסיק לנקוט אמצעים סבירים על מנת לוודא כי הקבלן עמו הוא מתקשר הוא מהימן, ומסוגל לעמוד בחובותיו בתחום הגנת המידע והפרטיות.

2.9.4. סביר להניח שקבלת שירות של מיקור חוץ מעוגנת בחוזה המסדיר את כלל ההיבטים העסקיים והמסחריים של השירות. במסגרת זו יש להתמודד עם הסיכונים לאבטחת המידע הקשורים במיקור החוץ, ולהסדיר הוראות הקשורות גם לאופן קיום הוראות החוק בחוזה ובין היתר:

2.9.4.1. המידע שרשאי הגורם החיצוני לעבד;

2.9.4.2. מטרת עיבוד המידע והשימושים המדויקים שיעשו בו;

2.9.4.3. מערכות המחשוב של המאגר שהגורם החיצוני רשאי לגשת אליהם;

<sup>36</sup> לעניין החשש מהתחזות לאחר ראו הנחית רשם מאגרי מידע מס' 1-2010 "דרישת מינימום לתהליכי אימות זהות של נושא מידע לצורך מתן גישה למידע שעליו במאגר מידע" <http://www.justice.gov.il/NR/rdonlyres/64980C3E-A940-457D-92F8-404FD6A9D0A2/20341/12011.pdf>

<sup>37</sup> ראו הנחית רשם מאגרי המידע מס' 2/2011, בנושא "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי", ה"ש 20 לעיל.



2.9.4.4 סוג העיבוד שהגורם החיצוני רשאי לעשות;

2.9.4.5 משך תוקפה של ההתקשרות;

2.9.4.6 החובות בתחום אבטחת המידע החלות על הגורם החיצוני.

שאלות לבדיקה עצמית של המעביד:

- האם מידע מועבר לגורם המטפל בו במיקור חוץ?
- מהם התפקידים שמבצע הקבלן עבור המעסיק?
- היכן מוגדרות חובותיו של המחזיק ביחס למידע?
- מהי מדיניות האבטחה של הקבלן?

**2.10. סיכום - המלצות כלליות לקיום עקרונות הגנת הפרטיות לאחר הקבלה לעבודה ובעת העבודה**

2.10.1 יש להקפיד ולצבור מידע רק כאשר קיים צורך ממשי ומבוסס במידע זה. זאת אף בהינתן היתר מצד התקנות.

2.10.2 ריכוז הטיפול באישורי מחלה יהיה על ידי עובדים שיוסמכו לכך במפורש.

2.10.3 על העובד המטפל במידע הרפואי הרגיש, להיות מודע לחובת הסודיות שחלה עליו ולדאוג לכך שהמידע אינו יוצא משליטתו ושהוא אינו משתף אותו עם עובדים אחרים בארגון אשר אינם נדרשים למידע זה. יש לנקוט גם אמצעי אבטחת מידע מתאימים להגנה על המידע.

2.10.4 לקבוע מסמך מדיניות מטעם ההנהלה המסדיר נושאים אלה וקובע הוראות ואחריות בסוגיות עקרוניות הקשורות בניהול המידע.

2.10.5 יש לוודא כי מערכות המידע יישמרו במקום מוגן, אשר מתקיימים בו אמצעים למניעה של כניסה וחדירה למתחם ללא הרשאה.

2.10.6 למנות עובד (ובכלל זה נושא משרה שהוא בעל תפקיד אחר) שיהיה "ממונה אבטחת מידע" שתפקידו לוודא כי הארגון מממש את חובותיו בתחום אבטחת המידע, והוא כפוף ומדווח ישירות להנהלת הארגון.

2.10.7 לערוך מיפוי מסודר של רכיבי המערכות ותיאור מבנה הרשת של מערכות המחשבות של המאגר, וקביעת הרשאות לגישה למידע במאגר.



2.10.8 לקבוע נוהל קבלת הרשאות וסיסמאות המסדיר את הטיפול בגישה למערכות המידע של הארגון, ולהפיצו בארגון.

2.10.9 ליידע את העובד הרלוונטי בטרם גישה למידע המנוהל ברגיל על ידי העובד עצמו.

2.10.10 הפצת נוהל פנים ארגוני קצר וברור ובו הסברים בסיסים הקשורים בחובות העובדים.

2.10.11 החתמת עובד בטרם קבלת הגישה למאגר ולאחר הבהרת חובותיו על התחייבות לשמירת סודיות בקשר למידע אליו הוא נחשף במסגרת עבודתו עם מאגרי המידע.

2.10.12 מומלץ לבצע בארגון פעילויות הדרכה תקופתיות הכוללות בין היתר סקירה של מסמכי האבטחה בארגון והסבר על חובתם לבדוק למי נמסר מידע מהמאגר.

2.10.13 לקבוע איש קשר מוסמך מטעם הקבלן (הוא "המחזיק" בלשון חוק הגנת הפרטיות) שיהיה אחראי על קיום הוראות החוזה, ויהיה המקביל של ממונה האבטחה אצל המחזיק.

2.10.14 לכלול בחוזה הוראות בעניין זכותו של בעל המאגר המעסיק לקבל לפי דרישתו מידע אודות פעילות המחזיק על מנת לבחון שהוא אכן מקיים את דרישות האבטחה שנקבעו בהסכם.

### 3. שלב שלישי: שמירה ומחיקת מידע לאחר סיום יחסי עובד - מעביד

3.1 ככלל, בעת סיום יחסי עובד-מעביד, יש למחוק מידע שאינו נדרש עוד, זאת על מנת למנוע שימוש לרעה במידע.

3.2 עם זאת, במקרים בהם עולה צורך לשמור את המידע לצרכים עסקיים לגיטימיים גם בתום ההעסקה, כגון התגוננות מתביעות (לא יותר מתקופת ההתיישנות) – ניתן לשמור על המידע, אולם יש לקבוע לעניין השמירה הוראות מחמירות המבטאות את הגבלת המטרה – לצרכי ארכיון בלבד.



3.3 בהתאמה, יש לקבוע מגבלות על הגישה למידע רק למי שנדרש למידע זה לצורכי התגוננות בתביעות או טיפול אחר מול הרשויות. לדוגמה, לאחר סיום העסקת העובד, רק היועץ המשפטי של הארגון יהיה מורשה גישה לתיקו האישי, לפי צורך משפטי.

שאלות לבדיקה עצמית של המעביד:

- האם מערכות המידע של הארגון מכילות גם מידע אודות מי שאינו מועסק יותר בארגון?
- האם מידע כאמור נשמר יותר מאשר תקופת ההתיישנות הרלבנטיות?
- האם ניתן להגביל את הגישה למידע כאמור עד תום תקופת ההתיישנות ולאחר סיום ההעסקה לגורמים בודדים בארגון בלבד?



## חלק ג' - הסדרת השימוש בטכנולוגיית מידע במקום העבודה - ניטור

1. היקף רב של מידע אישי אודות העובדים נאסף לא רק במערכות המידע הייעודיות לצרכי ניהול כוח האדם, המנוהלות ברגיל במחלקת משאבי האנוש של הארגון, אלא גם במערכות המידע ובטכנולוגיות המשמשות את שאר המחלקות של הארגון לצורך ביצוע העבודה, ולמטרות אישיות של העובדים, לרבות רשת המחשבים המשרדית הכללית, מערכת הדואר האלקטרוני, רשת האינטרנט וטלפונים חכמים ומחשבי לוח המסופקים לעובד מידי המעסיק.
2. פסק דינו של בית הדין הארצי לעבודה **בפרשת איסקוב**<sup>38</sup>, כולל קביעות עקרוניות וחשובות בסוגיית הפרטיות ביחסי עבודה בכלל ובהקשר של השימוש בטכנולוגיות מידע בפרט – תוך דיון מקיף בשאלה הקונקרטית שעמדה בפני בית הדין: גבולות האסור והמותר במעקב אחר תכתובת הדואר האלקטרוני של העובדים.
3. קביעה עקרונית אחת של בית הדין, המשליכה על כל סוגי הטכנולוגיה בהן משתמש העובד במקום העבודה ועל כל סוגי המידע הנאסף באמצעותן, הסירה ספק והבהירה **שלעובד יש מרחב של פרטיות המלווה אותו גם במקום העבודה**, בלא קשר לזכות הקניין של המעסיק במקום העבודה ובציוד בו העובד עושה שימוש. בהתאם, העובדה שמחשב הוקצה לעובד לצורך עבודה ושיש למעסיק זכות קניינית עליו, וגם אפשרות טכנית לנטר ולאחזר כל מידע המצוי בו, אינה מפקיעה את זכות העובד לפרטיות על ענייניו האישיים, ובפרט על תכתובותיו האישיות.
4. קביעה עקרונית נוספת של בית הדין היא **שעל המעסיק לקבוע מדיניות מפורשת ומפורטת בנוגע לשימוש העובדים בטכנולוגיות מידע ולהודיע על כך לעובדים**. קביעה זו נובעת מדרישת ה"הסכמה מדעת" שבחוק, המציבה רף גבוה של יידוע ושל פירוט ביחס לפגיעה האפשרית בפרטיות. חובת יידוע העובדים מצאה ביטוייה בפסק הדין גם תחת הדיון בעיקרון השקיפות. נקבע, כי המעסיק חייב להביא לידיעת העובדים בפירוט את כללי המדיניות הנוהגת ביחס לשימוש בטכנולוגיות מידע ולפרט נסיבות המצדיקות לדידו ניטור כללי או ספציפי של מידע. בית הדין קבע, כי מכוח עיקרון זה יש לכלול בהתקשרות החוזית עם העובד בעת הקבלה לעבודה את מדיניות המעסיק.
5. בסוגיה הספציפית עליה נסובה הפרשה – חדירה לתכתובת הדואר האלקטרוני של העובד – כלל פסק הדין דיון מקיף וממצה וקבע שורה של תנאי סף שזו תמציתם: הראשון, כי נקבעה מדיניות כללית סבירה, וזו הוצגה לעובד בפירוט, ואף ניתנה לה הסכמתו; השני, שניתנה

<sup>38</sup> פסק דינו של בית הדין הארצי לעבודה מיום 08.02.2011 בעניין ע"ע 90/08 איסקוב נ' מדינת ישראל – הממונה על חוק עבודת נשים ובר"ע 285/08 אפיקי מים – אגודה חקלאית שיתופית נ' רז פישר (להלן – פרשת איסקוב). עתירה לבג"צ כנגד פסק דינו של בית הדין הארצי, נמחקה בידי בית המשפט העליון ביום 5.12.2011 לאחר שהעותרים החליטו למשוך את העתירה ולפיקח פסק דינו של בית הדין הארצי לעבודה מגלם דין מחייב.



הסכמתו הספציפית והמפורשת של העובד, בגין כל פעולת מעקב וחדירה בנפרד, בשים לב לסוגים השונים של תיבות הדואר<sup>39</sup>; השלישי, שמטרת החדירה עומדת בעיקרון הלגיטימיות, המצריך קיומן של נסיבות חמורות ויוצאות דופן של פגיעה באינטרס לגיטימי של המעסיק; הרביעי, כי החדירה עומדת בעיקרון המידתיות החוקתית; החמישי, כי השימוש במידע המופק יוגבל על פי עיקרון צמידות המטרה, כך שייעשה בו שימוש רק לצורך המטרה הלגיטימית, הנובעת מקיומן של נסיבות חריגות של פגיעה במעסיק.

שאלות לבדיקה עצמית של המעביד:

- האם מתבצע ניטור של שימוש ברכיבי טכנולוגית מידע?
- מהן המטרות לשמן מתבצע הניטור?
- מי מבצע את הניטור?
- האם ניתנה התראה על הניטור לעובדים?

6. סיכום - המלצות כלליות לקיום עקרונות הגנת הפרטיות בשימוש במערכות מידע - ניטור

- 6.1 ככלל על המעסיק לפעול על פי הקו המנחה כי לעובד יש מרחב של פרטיות המלווה אותו גם במקום העבודה.
- 6.2 על המעסיק לקבוע מדיניות מפורשת ומפורטת בנוגע לשימוש העובדים בטכנולוגיות מידע ולהודיע על כך לעובדים בשלב ההתקשרות החוזית עם העובד בעת הקבלה לעבודה.
- 6.3 בנוגע לחדירה לתכתובת הדואר האלקטרוני של העובד בפרט יש לוודא כי:
  - 6.3.1 נקבעה מדיניות כללית סבירה, וזו הוצגה לעובד בפירוט, ואף ניתנה לה הסכמתו.
  - 6.3.2 ניתנה הסכמתו הספציפית והמפורשת של העובד, בגין כל פעולת מעקב וחדירה בנפרד.

<sup>39</sup> **בתיבת דואר פרטית** של העובד (כגון תיבה אינטרנטית מסוג Gmail) – אסר בית הדין לבצע פעולה כלשהי אפילו ניתנה הסכמתו הספציפית של העובד; בתיבה פרטית מסוג זו אפשר יהיה לבצע ניטור רק לאחר קבלת צו מתאים מבית משפט מוסמך. זאת לאור התפיסה כי תיבה מסוג זה כמוה כחצריו הפרטיים של העובד.



6.3.3 מטרת החדירה עומדת בעיקרון הלגיטימיות, המצריך קיומן של נסיבות חמורות ויוצאות דופן של פגיעה באינטרס לגיטימי של המעסיק.

6.3.4 החדירה עומדת בעיקרון המידתיות החוקתית.

6.3.5 השימוש במידע המופק יעשה רק לצורך המטרה הלגיטימית, הנובעת מקיומן של נסיבות חריגות של פגיעה במעסיק.

פרופ' רותם רובין





## סיכום

במסגרת היחסים המורכבים בין העובד למעביד, בכל שלביו – מטרום העסקה, בזמן העסקה ועד לסיום העסקתו של העובד, נעשה עיבוד של מידע רב אודות העובד במקום העבודה. רובו של העיבוד נעשה למטרות לגיטימיות, אשר נדרשות לניהול התקין של העסק.

עם זאת, עיבוד המידע באופן שאינו תואם את עקרונות הגנת הפרטיות חובה בתוכו פוטנציאל רב לפגיעה בפרטיותו של העובד. כפי שפורט לעיל במסמך זה, למרות פער הכוחות במערכת היחסים בין העובד למעביד, אין למעביד זכות מוחלטת לעשות כרצונו במידע אודות העובדים במקום העבודה.

עקרונות הגנת הפרטיות חלים בכל שלבי התעסוקה ועל המעבידים להיות מודעים וליישם ככל שהם מעבדים ומנהלים מאגרי מידע במסגרת הניהול השוטף של העסק.

אי-עמידה בעקרונות ובניהול התקין של פעילות עיבוד המידע במאגר המידע, אשר מכיל מידע אודות עובדים, עלול להביא את המעביד למצב בו התאגיד בו הוא מנהל את עסקיו מבצע הפרה של חוק הגנת הפרטיות, ואף במקרים מסוימים יכול למצוא המעסיק עצמו חב בחובות אישיות כנגד הפרות של חוק הגנת הפרטיות במקום העבודה. במקרים אלו עלולות לחול סנקציות כלכליות ובמקרים החמורים אף סנקציות פליליות.

בשל כך, על כל מעביד נתונה האחריות לדאוג ליישום ולביצוע של העקרונות אשר עלו במסמך זה. ליישום היעיל והנכון של עקרונות אלו, הובאו מספר שאלות ונקודות לבדיקה עצמית. בכדי להגיע לציות מרבי להוראות החוק, ולהימנע מפגיעה בפרטיות של העובדים מומלץ לבצע בדיקה של הנקודות הנ"ל מעת לעת ולתקן ליקויים ככל שניתן.





**נספח: ריכוז שאלות לבדיקה עצמית והמלצות**

לנוחות הקורא, מרוכזות בזאת עיקרי השאלות לבדיקה עצמית וההמלצות הכלולות בפרקים השונים של המסמך, באמצעות הטבלה הבאה:

פרק	תת נושא	שאלות לבדיקה	המלצות כלליות
חלק א' - ניהול המידע משלב הגיוס לעבודה - טרומ העסקה	הגשת מועמדות לעבודה (עמ' 13-14)	איזה מידע נשאל בטפסים והאם יש הכרח בכל אחד מפריטי המידע?	המעסיק צריך להיות מסוגל להסביר את הרלוונטיות של כל פריט מידע שמתבקש.
		<ul style="list-style-type: none"> <li>האם טפסי המועמדות/קורות החיים מועברים גם לצדדים נוספים?</li> <li>אם כן -                             <ul style="list-style-type: none"> <li>למי ולאילו מטרה?</li> <li>האם העברה זו הכרחית?</li> <li>האם התקבלה ההסכמה מדעת לכך מצד המועמד, לפני איסוף ולפני העברת המידע?</li> </ul> </li> </ul>	בקבלה לעבודה מומלץ כי המועמדים יתבקשו לספק את המידע על אודותיהם בטפסי מועמדות המורכבים משדות ("רובריקות") מוגבלים ומוגדרים למידע הנדרש למועמדותיהם, וזאת בכדי למנוע איסוף של מידע עודף, אשר אינו נדרש.
		האם קורות החיים המתקבלים ממועמדים נשמרים כך שהם נגישים רק למי שצריך לגשת אליהם? והאם ננקטו אמצעי אבטחה ונהלי הרשאת גישה מתאימים בעניין?	
	ראיונות עבודה (עמ' 14)	אילו שאלות נשאלות במהלך ראיון העבודה?	אין לשאול שאלות שאינן רלוונטיות להערכת התאמתו של העובד למקום העבודה. האיסור נובע הן מדיני הגנת הפרטיות, והן מדיני שוויון הזדמנויות בעבודה.
		<ul style="list-style-type: none"> <li>האם נעשית תרשומת בזמן ראיונות? אם כן -</li> <li>האם התרשומות נשמרות בתום הליך המיון? אם כן -</li> <li>למי יש גישה במקום העבודה למידע זה? האם נקבעו נהלים מתאימים לשמירת המידע, למניעת העברתו לצדדים שלישיים?</li> </ul>	<ul style="list-style-type: none"> <li>אם ברצונך לשמור על מידע אודות מועמדים גם לאחר שלא התקבלו למשרה עליה התמודדו כיוון שיש להם פוטנציאל להיות מועסקים בעתיד, עליך לבקש את הסכמתם לשמירת המידע אודותם.</li> <li>במקרים בהם ברור כי הארגון אינו מעוניין להעסיקם, על מנת למזער את החשש מפני שימוש לרעה במידע, יש למחוק כל מידע אודות מועמדים אלו, מיד כאשר הוא אינו נחוץ.</li> </ul>
	מבחני מיון והתאמה לעבודה (עמ' 14-16)	האם מבדקי ההתאמה תואמים את תכלית ההעסקה? כלומר, האם לתפקיד ספציפי נדרש לבחון תכונה או מידע אישי מסוים?	יש לקבוע נהלים ברורים למסירת הפרטים למועמדים, בצורה בהירה וברורה, לפני ביצוע המבחן.



פרק	תת נושא	שאלות לבדיקה	המלצות כלליות
		<p>האם נעשה שימוש במכון חיצוני?</p> <p>האם ידוע לך כיצד המכון החיצוני אשר מבצע את מבדקי ההתאמה שומר על סודיות ואבטחת המידע אודות המועמדים לעבודה אצלך?</p> <p>האם קבעת עם המכון החיצוני נוהל שיגדיר מראש, כיצד ומי רשאי לעיין במידע?</p> <p>כיצד ניתנת זכות העיון וזכות התיקון למועמד לעבודה?</p> <p>האם המועמדים נשאלים שאלות אשר לפי חוק אסור לשאול אותן?</p>	<ul style="list-style-type: none"> <li>יש להקפיד על עקרונות שמירת המידע כאשר המועמד לא מתקבל לעבודה (ראו המלצות לעיל בתת נושא ראיונות עבודה), גם כאשר המידע מוחזק בידי גורמים חיצוניים (מכוני מיון) שבהם המעסיק נעזר.</li> </ul>
	מידע אשר איסופו אסור (עמ' 16-17)	<p>האם ננקטו צעדים למניעת איסוף מידע אסור?</p>	
חלק ב' - ניהול תיק עובד - לאחר הקבלה לעבודה ובעת העבודה	איסוף מידע במהלך העבודה (עמ' 17-18)	<p>איזה מידע נאסף במהלך השוטף של יחסי העבודה?</p> <p>מהן מטרות האיסוף של המידע הנוסף?</p> <p>איפה נשמר מידע זה?</p> <p>למי בארגון קיימת גישה למידע שנאסף?</p>	<p>כך לדוגמא, בכל הקשור לנושא אי כשירות בעקבות מחלה, ריכוז הטיפול באישורי מחלה יהיה על ידי עובדים שיוסמכו לכך במפורש, על העובד המטפל במידע הרפואי הרגיש, להיות מודע לחובת הסודיות שחלה עליו. כמו כן, יש לנקוט גם אמצעי אבטחת מידע מתאימים להגנה על המידע.</p>
	עקרונות כלליים לניהול המאגר (עמ' 18-19)	<p>מי הוא מנהל המאגר לפי החוק?</p> <p>מי קובע את מטרות השימוש במידע ומבקר זאת בארגון?</p> <p>האם חלק מהמידע נצבר אצל נותני שירות במיקור חוץ?</p>	
	ניהול המידע ואבטחת מידע (עמ' 19-20)	<p>האם לארגון יש מדיניות אבטחת מידע?</p> <p>האם קיים בארגון ממונה על אבטחה לפי סעיף 17 לחוק?</p> <p>אילו בקורות כלליות קיימות על קיום הוראות אבטחת המידע בארגון?</p>	
	מיפוי והגדרת המידע המצוי במאגר (עמ' 21)	<p>מהו המידע הנאסף ומנוהל על עובדים?</p> <p>האם יש מידע בעל רגישות מיוחדת (כגון מידע ביומטרי, בדיקות רפואיות, בדיקות פסיכולוגיות, נתונים סוציו-אקונומיים אחרים)?</p> <p>היכן נשמר המידע אודות עובדים? ולמי יש גישה אליו?</p> <p>למי נדרשת הרשאה לגישה למידע ובאיזה אופן?</p>	<ul style="list-style-type: none"> <li>לקבוע מסמך מדיניות מטעם ההנהלה המסדיר נושאים אלה וקובע הוראות ואחריות בסוגיות עקרוניות הקשורות בניהול המידע.</li> <li>למנות עובד (ובכלל זה נושא משרה שהוא בעל תפקיד אחר) שיהיה "ממונה אבטחת מידע" שתפקידו לוודא כי הארגון</li> </ul>



המלצות כלליות	שאלות לבדיקה	תת נושא	פרק
<p>מממש את חובותיו בתחום אבטחת המידע, והוא כפוף ומדווח ישירות להנהלת הארגון.</p> <ul style="list-style-type: none"> <li>לערוך מיפוי מסודר של רכיבי המערכות ותיאור מבנה הרשת של מערכות המחשבות של המאגר, וקביעת הרשאות</li> </ul>	<p>מהם הסיכונים המרכזיים לפגיעה בשלמות המידע, חשיפתו או שימוש בו שלא כדין?                      האם מועבר מידע לחו"ל?</p>		
<p>יש לוודא כי מערכות המידע יישמרו במקום מוגן, אשר מתקיימים בו אמצעים למניעה של כניסה וחדירה למתחם ללא הרשאה.</p>	<p>היכן נשמרות מערכות המידע המכילות את המאגר?                      האם בארגון מקפידים לנעול את החדרים בהם נשמר מידע?                      האם יש מערכות בקרה ואבטחה מחוץ לשעות הפעילות של הארגון?</p>	<p>הוראות לעניין אבטחה פיזית (עמ' 22)</p>	
<ul style="list-style-type: none"> <li>לקבוע נוהל קבלת הרשאות וסיסמאות המסדיר את הטיפול בגישה למערכות המידע של הארגון, ולהפיצו בארגון.</li> <li>ליידע את העובד הרלוונטי בטרם גישה למידע המנוהל ברגיל על ידי העובד עצמו.</li> </ul>	<p>מי מורשה גישה לכל אחד ממאגרי המידע?                      האם ההרשאות מבוססות על צורך ארגוני והאם יש מי שיש לו גישה עודפת?                      האם קיים ניהול מסודר של סיסמאות ואמצעי בקרה אחרים?</p>	<p>הקפדה על גישה מורשית בלבד למידע (עמ' 22-23)</p>	
	<p>האם מערכות המידע של הארגון מחוברות לאינטרנט? במידה שכן, האם יושמו אמצעי אבטחה והגנה מקובלים?                      האם ניתן לגשת מרחוק אל משאבי המידע של הארגון? האם עובדים יכולים לגשת למידע מהבית?                      האם יש תיעוד שוטף של הגישה והשימוש במידע?</p>	<p>אבטחת תקשורת וניהול מאובטח של מערכות מחשוב (עמ' 23-24)</p>	
<ul style="list-style-type: none"> <li>הפצת נוהל פנים ארגוני קצר וברור ובו הסברים בסיסיים הקשורים בחובות העובדים.</li> <li>החתמת עובד בטרם קבלת הגישה למאגר ולאחר הבהרת חובותיו על התחייבות לשמירת סודיות בקשר למידע אליו הוא נחשף במסגרת עבודתו עם מאגרי המידע.</li> <li>מומלץ לבצע בארגון פעילויות הדרכה תקופתיות הכוללות בין היתר סקירה של מסמכי האבטחה בארגון והסבר על חובתם לבדוק למי נמסר מידע מהמאגר.</li> </ul>	<p>האם נקבעה מדיניות לעניין שימוש העובדים במאגרי המידע בארגון?                      האם עיקרי המדיניות הובאה לידיעת העובדים?                      כיצד נבדקת מהימנות עובדים בארגון בעת מתן הרשאות גישה למידע?                      האם עובדים בעלי הרשאות גישה למידע מהמאגר תודרכו לגבי אפשרויות הונאה שלהם?</p>	<p>הדרכת עובדים ביחס לחובותיהם בתחום הגנת הפרטיות (עמ' 24-25)</p>	
<ul style="list-style-type: none"> <li>לקבוע איש קשר מוסמך מטעם</li> </ul>	<p>האם מידע מועבר לגורם המטפל בו</p>	<p>מיקור חוץ</p>	



המלצות כלליות	שאלות לבדיקה	תת נושא	פרק
<p>הקבלן (הוא "המחזיק" בלשון חוק הגנת הפרטיות) שיהיה אחראי על קיום הוראות החוזה, ויהיה המקביל של ממונה האבטחה אצל המחזיק.</p> <ul style="list-style-type: none"> <li>לכלול בחוזה הוראות בעניין זכותו של בעל המאגר המעסיק לקבל לפי דרישתו מידע אודות פעילות המחזיק על מנת לבחון שהוא אכן מקיים את דרישות האבטחה שנקבעו בהסכם.</li> </ul>	במיקור חוץ?	(OUTSOURCING)  (עמ' 25-26)	
	מהם התפקידים שמבצע הקבלן עבור המעסיק?		
	היכן מוגדרות חובותיו של המחזיק ביחס למידע?		
	מהי מדיניות האבטחה של הקבלן?		
	<p>האם מערכות המידע של הארגון מכילות גם מידע אודות מי שאינו מועסק יותר בארגון?</p> <p>האם מידע כאמור נשמר יותר מאשר תקופות ההתיישנות הרלבנטיות?</p> <p>האם ניתן להגביל את הגישה למידע כאמור עד תום תקופת ההתיישנות ולאחר סיום ההעסקה לגורמים בודדים בארגון בלבד?</p>	<p>חלק ג' - שמירה ומחיקת מידע לאחר סיום יחסי עובד – מעביד  (עמ' 27-28)</p>	
	<p>האם מתבצע ניטור של שימוש ברכיבי טכנולוגית מידע?</p> <p>מהן המטרות לשמן מתבצע הניטור?</p> <p>מי מבצע את הניטור?</p> <p>האם ניתנה התראה על הניטור לעובדים?</p>	<p>הסדרת השימוש בטכנולוגיית מידע במקום העבודה – ניטור (עמ' 29-31)</p>	
<p>ככלל על המעסיק לפעול על פי הקו המנחה כי לעובד יש מרחב של פרטיות המלווה אותו גם במקום העבודה.</p> <p>על המעסיק לקבוע מדיניות מפורשת ומפורטת בנוגע לשימוש העובדים בטכנולוגיות מידע ולהודיע על כך לעובדים בשלב ההתקשרות החוזית עם העובד בעת הקבלה לעבודה.</p> <p>בנוגע לחדירה לתכתובת הדואר האלקטרוני של העובד בפרט יש לוודא כי:</p> <ul style="list-style-type: none"> <li>נקבעה מדיניות כללית סבירה, וזו הוצגה לעובד בפירוט, ואף ניתנה לה הסכמתו.</li> <li>ניתנה הסכמתו הספציפית והמפורשת של העובד, בגין כל פעולת מעקב וחדירה בנפרד.</li> <li>מטרת החדירה עומדת בעיקרון הלגיטימיות, המצריך קיומן של נסיבות חמורות ויוצאות דופן</li> </ul>			



המלצות כלליות	שאלות לבדיקה	תת נושא	פרק
<p>של פגיעה באינטרס לגיטימי של המעסיק.</p> <ul style="list-style-type: none"> <li>• החדירה עומדת בעיקרון המידתיות החוקתי.</li> <li>• השימוש במידע המופק יעשה רק לצורך המטרה הלגיטימית, הנובעת מקיומן של נסיבות חריגות של פגיעה במעסיק.</li> </ul>			

פרסום להפצת