



עדכון לקוחות | מחלקת דיני עבודה

פרטיות במקום העבודה

ספטמבר, 2019

לקוחות ועמיתים יקרים,

במסגרת יחסי העבודה וחיי העבודה מעסיקים רבים נדרשים לאיסוף, שמירה וניטור מידע, שחלקו נחשב מידע אישי. פעולות יומיומיות המבוצעות בהקשר זה חוסות תחת דיני הגנת הפרטיות ומתבצעות על רקע תהליך גלובאלי של עליית המודעות והגברת הרגולציה בנושא שמירת הפרטיות, אל מול התפתחות טכנולוגית של אמצעי איסוף ומעקב.

חשוב לכל העוסקים בתחום להכיר את הצמתים הרלבנטיים, לאתר גורמי סיכון ולקבוע נורמות התנהלות העולות בקנה אחד עם הוראות הדין, לשם התנהלות תקינה והקטנת החשיפה המשפטית.

ברשימה זו נסקור, בתמצית בלבד, את התחנות המרכזיות בהן נדרש המעסיק לבחון את התנהלותו בראי דיני הגנת הפרטיות:

1. מאגרי מידע
2. אמצעים לניטור מידע במקום העבודה
3. איסוף מידע אישי ושמירתו לאורך חיי העבודה
4. יחסי עבודה קיבוציים
5. דיני הגנת הפרטיות בעולם ושאלת הציות והכפיפות אליהם

1. מאגרי מידע

חלק בלתי נפרד מניהול משאבי אנוש כולל איסוף ושמירה של מידע אישי לגבי עובדים ומועמדים לעבודה, ובכלל זה כתובת, מספר תעודת זהות, מצב משפחתי, ניסיון מקצועי, השכלה, מסמכים רפואיים, פרטי חשבון בנק וכיו"ב. המידע הנאסף בהקשר זה נחשב לרוב כ"מידע רגיש" ושמירתו באמצעים ממוחשבים מחייבת לרוב ניהולו של "מאגר מידע" בהתאם להוראות חוק הגנת הפרטיות, התשמ"א-1981 ("חוק הגנת הפרטיות") והתקנות שהותקנו מכוחו.

ואלה הן ההוראות המרכזיות בנוגע לאיסופו וניהולו של המידע על ידי המעסיק –

• חובת רישום

מאגר מידע המכיל מידע רגיש חייב ברישום בפנקס מאגרי המידע המנוהל על ידי רשם מאגרי המידע במשרד המשפטים. בקשה לרישום מאגר מידע מתבצעת על ידי הגשת טופס רשמי לרשות להגנת הפרטיות ("הרשות"). רישום מאגר אינו כרוך בתשלום או באגרה שנתית.

• הסכמת העובד

פניה לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע צריכה להיות מלווה בהודעה, שיצינו בה: (1) אם חלה חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו של העובד ובהסכמתו; (2) המטרה לשמה מבוקש המידע; (3) למי יימסר המידע ומטרות המסירה.

בהתאם לפסיקת בתי המשפט, יש לקבל הסכמה מפורשת בכתב מכל עובד ביחס לאיסוף ושמירת המידע הנאגר בעניינו בחברה וכן ביחס לנסיבות בהן המידע יימסר לגורמים חיצוניים.

• חתימת הסכמים עם צדדים שלישיים בעלי גישה למאגר מידע או למידע

בהתאם לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017 ("תקנות אבטחת מידע"), בהתקשרות עם גורם חיצוני למתן שירות במסגרתו ניתנת גישה למאגר מידע יש לבחון את סיכוני אבטחת המידע. כמו כן יש לקבוע הוראות חוזיות בעניין המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות; סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות; משך ההתקשרות; אופן השבת המידע לידי הבעלים בסיום ההתקשרות; אופן יישום החובות שהמחזיק חייב בהן לפי התקנות; ועוד.

כאשר מדובר בהתקשרות עם גורם חיצוני למתן שירותים במיקור חוץ הכרוכים בעיבוד מידע אישי, יש לפעול גם בהתאם להנחיית הרשות, הקובעת שורה של פעולות שיש לנקוט לעניין זה, ובכלל זה בחינה מקדימה של הלגיטימיות להוצאת הפעילות למיקור חוץ; הגדרה ברורה של אופי השירות ומטרת השימוש במידע; דרישות אבטחת מידע ושמירה על סודיות כדי למנוע זליגה של המידע; הבטחת מתן זכות עיון ותיקון לאדם לגבי המידע נוגע; הדרכה והטמעה של חובות הפרטיות בקרב עובדי הקבלן; וקביעת הוראות ביחס למשך שמירת המידע הנמסר לקבלן לצורך ביצוע השירות ומחיקתו עם גמר ההתקשרות.

• זכות עיון ותיקון של מידע

חוק הגנת הפרטיות קובע את זכותו של נושא מידע (למשל, העובד) לעיין במידע שעליו האגור במאגר מידע, לבקש לתקן או למחוק מידע שאינו נכון, ברור, שלם או מעודכן, את חובתו של בעל מאגר מידע לאפשר את

זכות העיון ואת הדרכים והתנאים לעיון בו. האמור חל על כל סוג של מידע, שנשמר דיגיטלית, בכל פורמט, לרבות הקלטות קוליות של שיחות טלפון וצילומי וידאו.

- **אבטחת מאגרי מידע**

תקנות אבטחת מידע, שנכנסו לתוקף ביום 8 במאי 2018, קובעות הסדר רחב ומקיף לעניין ההגנה הפיזית והטכנולוגית על מאגרי מידע וניהולם, בהתאם לרגישות המידע הכלול במאגר, כמות נושאי המידע ומספר מורשי הגישה למידע.

התקנות קובעות שורה של הוראות והנחיות לעניין אמצעי אבטחת המידע שיש להנהיג ביחס למאגרי המידע בארגון, כגון: הוראות לעניין אבטחה פיזית וסביבתית של המאגר; ניהול הרשאות גישה; תיעוד ודיווח על אירועי אבטחה; וכו'.

- **שיתוף מידע מחוץ לישראל**

תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001 קובעות כי אין להעביר מידע ממאגר מידע בישראל אל מחוץ לגבולותיה, אלא אם כן דין המדינה אליה מועבר המידע מבטיח רמת הגנה שאינה פחותה מרמת ההגנה הקבועה בדין הישראלי או בהתקיים תנאים מסוימים הקבועים בתקנות (למשל, הסכמת נושאי המידע; המידע מועבר למאגר מידע במדינה המקבלת מידע ממדינות החברות בקהילה האירופית; ועוד). בנוסף, על בעל מאגר המידע להבטיח, בהתחייבות בכתב של מקבל המידע, כי מקבל המידע נוקט אמצעים מספיקים לשמירה על הפרטיות של נושאי המידע, וכי הוא מבטיח שהמידע לא יועבר לכל אדם זולתו.

2. אמצעים לניטור מידע במקום העבודה

מעסיקים רבים נוהגים לעשות שימוש באמצעים טכנולוגיים שונים תוך מעקב אחר עובדיהם. במסגרת פרק זה נסקור בקצרה את אמצעי הניטור והמעקב השכיחים בקרב מעסיקים, לצד התייחסות הדין והפסיקה לגבולות השימוש בהם.

- **שעון נוכחות ביומטרי**

על רקע החובה בדין לפקח על שעות העבודה של העובדים ולנוכח הרצון למנוע דיווחי נוכחות כוזבים, נוהגים מעסיקים רבים להתקין במקום העבודה שעון נוכחות ביומטרי.

בפסק הדין בעניין **עיריית קלנסווה**¹, נקבע על ידי בית הדין הארצי לעבודה כי מידע ביומטרי הוא מידע פרטי-אישי. את הפגיעה בפרטיות ניתן "להכשיר" במקרה בו ניתנה הסכמה מדעת ומרצון של העובד ובכפוף להוכחת עמידתו של המעסיק בתנאים קפדניים נוספים שנקבעו לעניין זה (ובניהם: שיקולי תכלית, מידתיות וסבירות).

¹ ע"ק (ארצי) 7541-04-14 הסתדרות העובדים הכללית החדשה – עיריית קלנסווה (פורסם בבנו, 15.03.2017).

על מעסיק המבקש להציב במקום העבודה שעון נוכחות ביומטרי מוטלת החובה לקבל מעובדיו הסכמה קונקרטית, מדעת ומרצון חופשי, לאחר שעובדיו קיבלו את מלוא המידע בכל הנוגע למערך התועלות והסיכונים הכרוך בהפעלת המערכת. בהעדר הסכמה שכזו לא ניתן לכפות על העובדים לעשות שימוש בשעון הביומטרי.

על רקע זה, מומלץ למעסיקים אצלם מותקן שעון נוכחות ביומטרי ומבקשים להוסיף לעשות שימוש בשעון נוכחות זה, או למעסיקים השוקלים הצבת שעון נוכחות ביומטרי, לקיים דיון ולקבל ייעוץ נקודתי בנוגע ליישום הפרמטרים שנקבעו בפסק הדין של בית הדין הארצי.

- **ניטור אמצעי תקשורת במקום העבודה – מחשבים וטלפונים סלולריים**

בשנת 2011 התווה בית הדין הארצי לעבודה, בפסק הדין שניתן בעניין **איסקוב**², את הקווים המנחים בעניין "האסור והמותר" בנוגע לניטור תכתובות דואר אלקטרוני של עובדים.

בהתאם להלכת **איסקוב**, על המעסיק לקבוע מדיניות מאוזנת בכל הנוגע להקצאת מרחב וירטואלי-פרטי לעובד בשימושי המחשב במקום העבודה וכן בעניין מעקב אחר תכתובת דואר אלקטרוני של עובד במחשב שהועמד לשימוש. במסגרת מדיניות זו על המעסיק לפרט, בין היתר, את אופי המעקב הצפוי להתקיים בתכתובת הדואר האלקטרוני; הטכנולוגיות בהן ייעשה המעקב; הנסיבות בגינן ייעשה בהן שימוש; סוג המידע שייאסף; תדירות המעקב; השימוש שיעשה במידע; כיצד, היכן ולכמה זמן יישמר המידע; וכו'.

מעבר ליידוע העובדים, המעקב צריך לעמוד במספר תנאים: **תנאי הלגיטימיות** – הגבלת המעקב והשימוש במידע שהופק כתוצאה ממנו למטרות חיוניות למקום העבודה; **תנאי המידתיות** – יש לבחון ולבחור את האמצעי שיפגע במידה הפחותה ביותר בפרטיותו של העובד; **עקרון צמידות המטרה** – איסוף המידע מוגבל אך ורק לצורך השגת המטרה המקורית לשמה נאסף.

אף שבפרשת איסקוב התווה בית הדין הארצי כאמור את הכללים למעקב ולניטור אחר תכתובת דואר אלקטרוני של עובדים, הרי שאמות המידה שנקבעו בפסק הדין משמשות, הלכה למעשה, גם לבחינת הלגיטימיות והמידתיות של פעולות מעקב וניטור מצד מעסיק אחר שימוש בכלים אלקטרוניים אחרים במקום העבודה.³

- **שימוש במצלמות אבטחה לצורך מעקב אחר עובדים**

במסגרת הנחיית רשם מאגרי מידע בדבר "שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי העבודה"⁴, חידדה הרשות להגנת הפרטיות את כללי האסור והמותר בכל הקשור להצבת מצלמות מעקב במקום העבודה, שנקבעו עוד קודם בפסיקת בתי הדין לעבודה.

הרשות הבהירה בהקשר זה, כי בדומה לכללים שנקבעו בכל הקשור לתכתובת הדואר האלקטרוני של העובד, גם בכל הנוגע להתקנת מצלמות המעקב הפרווגטיבה הניהולית של המעסיק כפופה לדרישות סבירות, מידתיות, תום הלב והגינות. מידת הלגיטימיות של מיקום התקנת המצלמה מושפעת מהציפייה הסבירה של העובד לפרטיות באזורים השונים במקום העבודה. כך, התקנת מצלמות במרחבים פרטיים שנועדו למנוחת

² עע (ארצי) 90/08 איסקוב ענבר – הממונה על חוק עבודת נשים (פורסם בבנו, 8.2.2011).

³ ראו לדוגמה: סע"ש (אזורי ת"א) 60161-06-16 בלקאר – בלקין (פורסם בבנו, 27.8.2019).

⁴ הנחייה זו מהווה נדבך משלים להנחיית הרשם מס' 4/2012 שכותרתה "שימוש במצלמות אבטחה ומעקב במאגרי התמונות הנקלטות בהן".

העובדים תתאפשר במקרים חריגים בלבד, כאשר התועלת מהתקנת המצלמות תעלה משמעותית על הפגיעה בפרטיות העובד (ובכל מקרה הדבר כרוך בידיעתו של העובד ובהסכמתו). התקנת מצלמות סתר ללא ידיעת העובד עלולה לעלות כדי עבירה פלילית. על המעסיק אף להציב שילוט מתאים בכניסה לכל אזור כיסוי של המצלמות.

על המעסיק לגבש מדיניות ברורה ומפורטת בדבר אופן השימוש במצלמות, היקף השימוש ומטרותיו. המעסיק נדרש להציג את המדיניות לעובדים; לשוב וליידע אותם בדבר יישומה; ולבחון את הצורך לרעננה מעת לעת, במטרה להתאימה למגמות המתפתחות בתחום.

מעבר לאמור, על מעסיק לעמוד גם בהנחיות הכלליות שבהנחית רשם מאגרי המידע בדבר "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן", הקובעות חובות לעניין שילוט מתאים, משך זמן לשמירת המידע, מתן זכות עיון במידע, וכו'.

נוכח חשיבות הדברים, אנו ממליצים לקיים עמנו היוועצות פרטנית בנושא, על מנת לבחון את אופן יישום הנחיית הרשות להגנת הפרטיות.

• איכון מיקומם של עובדים

מעסיקים רבים מציידים את עובדיהם באמצעים טכנולוגיים, באמצעותם יש ביכולתם לפקח אחר מסגרת שעות עבודתם של העובדים. לרוב פעולת האיכון מתבצעת באמצעות מכשירים סולריים, רכב עם אמצעי ניווט וכיו"ב. שימוש באמצעים אלה עלול להיות כרוך בפגיעה בפרטיות העובד.

בפרשת **פישר תעשיות פרמצבטיות**⁵, נעתר בית הדין הארצי לבקשה של מעסיק לקבלת דו"ח איכון של טלפון סלולארי שהועמד לרשות עובד. בהתאם לפסיקה, מעסיק רשאי בנסיבות מסוימות לעקוב אחר מיקום עובדיו **במסגרת שעות העבודה**, אך לשם כך עליו לעמוד בדרישת הסבירות והמידתיות.

חיזוק לכך ניתן לאחרונה בפסיקה של בית המשפט המחוזי בתל אביב בעניין **עמותת חברות הסיעוד**⁶, בה נקבע כי דרישה מעובדים לדווח על נוכחותם באמצעות יישומון המותקן בטלפון הנייד אמנם פוגעת בפרטיותם, אולם מדובר בפגיעה מידתית שנועדה למטרה לגיטימית.

על אף שהדבר אינו מחויב מכוח הפסיקה, אנו ממליצים לקבוע **מדיניות ברורה** ביחס לאופן השימוש בטלפון והאפשרות הקיימת לניטור מיקומו; **ליידע** את העובדים באשר למדיניות; וכן **לעגן** את העקרונות במפורש בחוזה העבודה ובנוהל הנהוג במקום העבודה.

⁵ ע"ע (ארצי) 40711-04-17 **פישר תעשיות פרמצבטיות בערבון מוגבל – שטטר** (פורסם בנבו, 4.3.2018).

⁶ עת"מ (מחוזי ת"א) 28857-06-17 **עמותת חברות הסיעוד נ' משרד הביטחון** (פורסם בנבו, 1.7.2019).

3. איסוף מידע אישי ושמירתו לאורך חיי העבודה

בפרק זה נתייחס בקצרה לשלבים מרכזיים בהם נצבר מידע בעניין עובדים לרבות מועמדים לעבודה, לצד התייחסות הדין והפסיקה לגבולות איסופו של המידע והשימוש בו.

• הליכי התאמה והערכה במכוני מיון

מעסיקים רבים נוהגים להפנות מועמדים או עובדים למבחני התאמה. בהתאם לפסיקת בית הדין הארצי לעבודה, ככלל רשאי מעסיק להעמיד מועמד לעבודה או עובד למבחני התאמה, כל עוד מדובר במבחנים **מהימנים ותקפים**, וכל עוד השימוש בהם נעשה תוך הקפדה על עקרונות של **שוויון, הגנה על הפרטיות, מידתיות ותום לב**.

בהתאם להנחיית הרשות להגנת הפרטיות, מעסיק המבקש לעשות שימוש במידע אישי על מועמד כדי להחליט אם לקבלו לעבודה, נדרש לקבל את **הסכמתו המפורשת**. על המעסיק לקבוע רשימה מוגבלת של מורשי גישה לתוצאות הבחינות. למעסיק עצמו אסור לאסוף מידע שאינו נדרש למטרת הליך קבלת המועמד, ואם נאסף מידע עודף שאינו דרוש למטרה זו – אסור למעסיק לשמור אותו.

הנחיית הרשות להגנת הפרטיות מפרטת אילו שימושים מותר למכוני המיון לעשות במידע האישי שנאסף אצלם; מה תוכן ההסכמה שהמעסיק, ובמיוחד מכון המיון, נדרשים לקבל מהמועמדים כתנאי לעיבוד המידע; וכיצד יש לממש את זכותו של המועמד לעיין במידע האישי שנאסף בעניינו.

• בדיקות רקע לעובדים

ככלל, אין מניעה לערוך בדיקות רקע על מועמדים לקבלה לעבודה. אולם, על בדיקות הרקע להתבצע באופן השומר על פרטיות המועמד, באופן הרלבנטי למשרה, בסבירות ובתום לב.

ככלל, **מעסיק אינו רשאי להיחשף למרשם הפלילי של המועמד או לבקש מהמועמד שימציא לו עותק מהמרשם הפלילי**, ואין בהקשר זה משמעות להסכמת העובד.

בראשית שנת 2021 עתיד להיכנס לתוקף חוק המידע הפלילי ותקנת השבים, התשע"ט-2019, ולהביא לביטולו של חוק המרשם הפלילי ותקנת השבים, התשמ"א-1981. החוק החדש אוסר לדרוש מידע מהמרשם הפלילי גם באופן עקיף (לדוגמה באמצעות קבלת תצהיר או מענה לשאלון).

חשיפה משפטית קיימת אף במקרה של בירור מידע הקשור לאחת העילות המוגנות על פי חוק שוויון ההזדמנויות בעבודה, התשמ"ח-1988 (מין, נטייה מינית, מעמד אישי, הריון, גיל, גזע, דת, לאום, ארץ מוצא, מקום מגורים ועוד). מעבר לכך, מעסיק אינו רשאי לדרוש ממועמד לעבודה את הפרופיל הצבאי שלו או מידע גנטי, או לעשות שימוש במידע כאמור.

בשים לב לחשיבות הדברים, אנו ממליצים לשוב ולרענן את ההנחיות בנוגע לראיונות עבודה ולאיסורים החלים בהקשר זה. כמו כן, אנו ממליצים לשוב ולבחון את הטפסים השונים המועברים למילוי על ידי מועמדים לעבודה.

- **איסוף מידע מרשתות חברתיות**

ככלל, ההנחה היא כי מידע המצוי ברשתות חברתיות, ובכלל זה בדף פייסבוק ציבורי של העובד, אינו מידע החוסה תחת הגנת הפרטיות. בהתאם לכך וככלל, מעסיק רשאי לבצע בדיקה של מידע פומבי המפורסם ברשתות החברתיות אודות עובד או מועמד לעבודה. עם זאת, ובנוסף לכללים הרלוונטיים לכל בדיקת רקע, על בדיקות אלו להתבצע תוך מתן משקל למהימנות המידע המפורסם בפלטפורמות אלו.

- **מידע רפואי בעניינו של עובד**

הנחת היסוד בפסיקה היא כי יש לראות בחיוב עובד או מועמד לעבודה לבצע בדיקה רפואית כפגיעה בזכות האדם לשלמות גופו, כבודו ופרטיותו. עם זאת, ניתן לדרוש מעובד לבצע בדיקות רפואיות תקופתיות במקרים מתאימים, כאשר מקור החובה קבוע בחקיקה או בהסכם (אישי או קיבוצי).

בהעדר חובה על פי הדין לביצוע בדיקות רפואיות לתפקיד מסוים **יש להגביל את הדרישה לבדיקה או למסירת מידע רפואי למקרים בהם קיים בכך צורך, בקשר לתפקיד המוטל על העובד.**

הצורך להגן על פרטיות העובדים בא לידי ביטוי גם בביטול תקנת משנה 2(א)(2) לתקנות דמי מחלה (נהלים לתשלום דמי מחלה), התשל"ו-1976, כך שכיום נמחקה האבחנה הרפואית מאישורי המחלה המוגשים למעסיק. בנוסף, ככל שתעודת המחלה ניתנה על ידי רופא קופת חולים, אין המעסיק רשאי להעמיד את העובד לבדיקה רפואית, גם אם התעורר אצלו ספק לגבי תוכן התעודה.

- **שמירת מידע**

כפי שפורט לעיל, בהתאם לדיני הגנת הפרטיות ניתן להחזיק במידע אישי בעניינו של אדם אך ורק לפרק הזמן ההכרחי למימוש המטרות שלשמן נאסף המידע.

לרוב, שמירת מידע אישי אודות עובדים למשך תקופת ההתקשרות מול העובד ושבע שנים לאחר מכן (תקופת ההתיישנות במרבית העילות מכוח יחסי עבודה) נחשבת תקינה. שמירת מידע אישי לתקופות ארוכות מכך דורשת מטרה ספציפית ולגיטימית, הקשורה באופן ישיר להעסקתו של העובד (לדוגמה: מעסיק המשלם תשלומים לעובד לאחר פרישתו) או הוראה בחוק המתירה את שמירת המידע.

4. יחסי עבודה קיבוציים

במקומות עבודה מאורגנים, נדרש המעסיק לא אחת להסדיר סוגיות המערבות פגיעה אפשרית בפרטיות על ידי גיבוש הסכמה קיבוצית (או לפחות תוך קיום היוועצות עם נציגות העובדים).

בפרשת **איסקוב** שנסקרה לעיל, ציין בית הדין הארצי כי מן הראוי שהמדיניות בכל הנוגע לשימוש בדואר אלקטרוני וניטורו תגובש בהסכמת ארגון העובדים, על דרך של הסכם או הסדר קיבוצי.

בפרשת **עיריית קלנסווה**, שעסקה באפשרות השימוש בשעון נוכחות ביומטרי, לא הכריע בית הדין הארצי באפשרות לפיה הסכמה בהקשר זה תינתן במישור הקיבוצי, אם כי הנטייה הייתה שלא לראות בהסכמה במישור הקיבוצי כמספקת. בפרשת **עמותת חברות הסייעוד** עמד בית המשפט המחוזי בתל אביב על כך שבשים לב לפגיעה בפרטיות יש צורך בהסכמה חופשית ומדעת של הפרט, ואין די בהסכמה במישור הקיבוצי.

5. דיני הגנת הפרטיות בעולם ושאלת הציות והכפיפות אליהם

מעבר לדינים ולכללים המקומיים החלים על מעסיקים הפועלים בישראל, לא אחת כפופים מעסיקים גם להוראות דין, לרגולציה ולהנחיות של מדינות זרות ושל גופים רב לאומיים.

האיחוד האירופי – ביום 25 במאי 2018 נכנסה לתוקף הרגולציה הכללית הנוגעת להגנה על מידע באיחוד האירופי (GDPR - General Data Protection Regulation). בהמשך, תחולת ה-GDPR הורחבה גם ליתר המדינות החברות באזור הכלכלי האירופי.

הכללים בהקשר זה מסדירים את איסוף המידע האישי אודות יחידים במדינות האיחוד האירופי, שמירתו, עיבודו והעברתו לאחר, וכן מסדירים את זכויות נושאי המידע (למשל גישה למידע ומחיקתו) ואת יתר החובות החלות על גופים המעבדים מידע אישי (למשל מינוי קצין אבטחת מידע).

ההגדרה ל"מידע אישי" תחת ה-GDPR הורחבה באופן משמעותי, וחלה על כל מידע אודות אדם מזהה או שניתן לזהויו, במישרין או בעקיפין, במיוחד בדרך של התייחסות למזהה כדוגמת שם, מספר מזהה, מידע על מיקום, מזהה אינטרנטי (למשל כתובת IP), ועוד.

הכללים והאיסורים שנקבעו בהקשר זה חלים על כל גורם השולט במידע כאמור או העוסק באיסופו או עיבודו, שמקום מושבו במדינות האיחוד האירופי, או לחילופין **שמקום מושבו מחוץ למדינות האיחוד האירופי**, כאשר אותו גורם מציע מוצרים או שירותים לתושבי האיחוד, או לחילופין מנטר את התנהגותם של תושבי האיחוד.

הפרשנות ביחס לתחולת ה-GDPR ביחס לגורמים שמקום מושבם מחוץ למדינות האיחוד האירופי היא רחבה למדי. בין היתר, על מנת לענות על השאלה האם חברה מסוימת מציעה מוצרים או שירותים באיחוד האירופי, ייבחנו גורמים כגון קיומו של אתר אינטרנט בשפה הנוהגת באחת ממדינות האיחוד; האפשרות לרכוש מוצרים או שירותים באמצעות מטבע מקומי; קמפיינים פרסומיים המכוונים לתושבי האיחוד; שימוש בשם מתחם הכולל את התיבות EU או סיומת מדינתית; ועוד.

כמו כן, הכללים והאיסורים חלים גם על גורמים שמקום מושבם מחוץ למדינות האיחוד האירופי, אשר מעבדים מידע אישי בעבור, או מטעם, גורמים שמקום מושבם באיחוד האירופי (למשל, ספקי משנה שמקום מושבם מחוץ למדינות האיחוד).

לא למותר לציין, כי בעקבות כניסת ה-GDPR לתוקף, גופים רב-לאומיים רבים בחרו לאמץ ולהחיל מדיניות פנימית אחידה בנוגע לסטנדרט הגנת המידע האישי, בכל זרועות הגופים, לרבות אלו שאינם בהכרח כפופים ישירות לתחולת ה-GDPR.

קליפורניה – בינואר, 2020 צפויה להיכנס לתוקף רפורמה בדיני הגנת הפרטיות בקליפורניה – California Consumer Protection Act ("**CCPA**") . החקיקה החדשה תרחיב באופן משמעותי את החובות המוטלות על חברות האוספות מידע פרטי אודות תושבי קליפורניה (למשל, חובות יידוע אודות איסוף מידע, מימוש זכויות נושאי המידע, ועוד). בדומה לרפורמה שקיבלה ביטוי באיחוד האירופי עם הכניסה לתוקף של כללי ה-GDPR, גם לחקיקה החדשה בקליפורניה תהיה תחולה אקס-טריטוריאלית.

נשמח לסייע לכם במיפוי נקודות הממשק במקום העבודה עם דיני הגנת הפרטיות; בניתוח ממשקים אלה וזיהוי הגורמים הרלוונטיים, מבית ומחוץ, לכל אחד מהם; ובבניית אמצעי בקרה על מנת לוודא כי אתם פועלים בהתאם לדיני הגנת הפרטיות, תוך הקטנת החשיפות המשפטיות.

בברכה,

מחלקת דיני עבודה

הרצוג פוקס נאמן

אנשי קשר:

מוריה תם-הרשושנים | שותפה

מחלקת דיני עבודה

03-692-2045 📞

tam@hfn.co.il 📧

אורלי ג'רבי | שותפה

ראשת מחלקת דיני עבודה

03-692-2045 📞

gerbi@hfn.co.il 📧