

29 בינואר 2024

לכבוד
עו"ד גלעד סממה – ראש הרשות
באמצעות מייל ppa@justice.gov.il

**התייחסות מכון תכלית – מסמך מדיניות בנושא איסוף ושימוש
במידע ביומטרי במקום העבודה**

נבקש להתייחס לעמדת רשות הגנת הפרטיות (להלן: "הרשות") בנושא איסוף ושימוש במידע ביומטרי במקומות עבודה. אין ספק, מדובר במהלך מבורך בשל הסיכונים הכרוכים בנטילת מידע ביומטרי. נייר זה מבקש לחזק את עמדת הרשות, וזאת באמצעות החמרת התנאים להסכמה חופשית, חיזוק חובת היידוע המוצעת ושינוי מנגנון שמירת ומחיקת המידע באופן שנועד להבטיח את הזכות לפרטיות, תוך ייחוס משקל ליחסים המורכבים של עובדים ומעסיקים והפגיעות הרבה שיש במידע ביומטרי.

תמצית עמדתנו

- פערי הכוחות הקיימים ביחסי עובד-מעביד מעוררים ספק באם עובד מסוגל להסכים לבקשת המעסיק לאיסוף מידע ביומטרי באופן מודע, חופשי ומרצון. אנו מציעים לשקול שנית את עמדת הרשות בעניין זה, ובמידה והסכמה של עובד במסגרת עבודתו עדיין תיחשב להסכמה חופשית, מוצע להוסיף תנאים אשר יבטיחו ככל הניתן שלא הופעלו על העובד לחץ או תמריצים הפוגעים בהסכמה.
- הרשות מבקשת כי המעסיק יסביר לעובד על המשמעות של איסוף מידע ביומטרי על מנת לאפשר לעובד הסכמה מדעת. אנו מסכימים עם החלטת חובת יידוע, ומציעים כי ההסבר ישלב התאמות הנדרשות לעובדים בעלי רמות שונות של אוריינות דיגיטלית על מנת שהחובה תעמוד גם במבחן מהותי וגם במבחן טכני.
- מוצע להפוך את ברירת המחדל המוצעת בעניין שמירת מידע כדי שמידע שאינו נחוץ יימחק אוטומטית, במקום לבקש כי מעסיק יבחן בעצמו את נחיצות השמירה מעת לעת. שינוי זה יעניק בחזרה מן השליטה לעובד, שנמצא בעמדת נחיתות מול המעסיק.

א. פערי הכוחות בין מעסיקים לעובדים והסכמה חופשית ומרצון

בשנים האחרונות נרשמה עלייה בשימוש במערכות ביומטריות במסגרות עבודה לבדיקת נוכחות ושעות עבודה של עובדים. תופעה זו מצטרפת לשורה של אמצעים הננקטים במקומות עבודה בעולם המערבי, בהם צילום, תיעוד וכן תיעוד ביומטרי מוצאים את עצמם בידיהם של מעסיקים אשר אמונים על הגינות ומסירת עובדיהם. שימוש בכלים טכנולוגיים אלו ובפרט מידע ביומטרי, המידע האישי והרגיש ביותר, מעלה חשש לפגיעה בפרטיות. כדי למזער את הפגיעה הפוטנציאלית, מקובל לבקש כי איסוף המידע ייעשה או על פי דין, ובהסכמה.

בהתאם, בנייר של הרשות צוין כי הסכמה חופשית ומדעת של עובדים לאיסוף ושמירת מידע ביומטרי שלהם מהווה תנאי בסיסי בלעדיו לא ניתן להכשיר את מהלך האיסוף. כפי שמסבירה הרשות, בפסקה

29 לנייר, ההסכמה צריכה להתקבל באופן מודעת, בצורה מפורשת או מכללא, ובנוסף חשוב כי תעמוד לעובד אפשרות לבחור בין מערכת ביומטרית למערכת שאינה ביומטרית. לתחושתנו, לא ברור בכלל שביחסי עובד-מעביד ישנה אפשרות, אם תיאורטית או מעשית, לפיה ההסכמה של עובד תהיה באמת מדעת, חופשית ומרצון.

הדווחת המיוחדת מטעם האו"ם לזכות לפרטיות בחנה שאלה זו לאור מקורות מרכזיים אודות איסוף מידע אישי, דוגמת הנחיות האו"ם וה-OECD למדינות החברות בארגונים אלו, התקנות הכלליות בדבר הגנת מידע של האיחוד האירופי (להלן: GDPR) ועוד. כפי שנסביר, לגישה ישנם חמישה רכיבים מצטברים להסכמה: על ההסכמה להינתן בצורה חופשית, ספציפית, באופן מודע, חד-משמעי ועל ההסכמה להיות בר-ביטול.¹

נבקש לשים דגש על חופשיות ההסכמה. המועצה האירופית להגנת מידע (European Data Protection Board - EDPB), גוף האיחוד האירופי האמון על פרשנות התקנות האירופיות בדבר הגנת מידע (להלן: GDPR), מציעה מועילה פרשנות למרכיב חופשיות ההסכמה. לגישת המועצה, כאשר יש מצב של פערי כוחות בין המבקש לאסוף את המידע ונושא המידע, בין אם מדובר בגוף שלטון לעומת הפרט או יחסי עובד-מעביד, קשה להכשיר את המהלך על בסיס הסכמת נושא המידע (במקום שאין הסכמה מפורשת בדיון).² מעבר לכך, ביחס למקומות עבודה בפרט, קבעה המועצה כי לאור התלות הנוצרת מיחסי עובד-מעביד, הסבירות שעובד יהיה מסוגל לסרב ללא חשש, או לתת הסכמה חופשית ומרצון למעסיקו בתשובה לבקשה, קלושה. על כן, מבהירה המועצה כי לא ניתן לבסס הכשרת מהלך איסוף מידע ביומטרי של עובד מאת מעסיקו על בסיס הסכמת העובד בלבד. המועצה מסייגת כי רק במקרים יוצאי דופן, בהם ניתן להוכיח כי ההסכמה חופשית ושאינה השלכות מזיקות בכלל להיעדר מתן הסכמה, ייתכן כי ניתן יהיה להתבסס על הסכמת העובד. עוד צוין כי כאשר המעסיק יכול להוכיח שלא תהינה השלכות שליליות לסירוב וכי אותו עובד ייחנה מתנאים זהים למי שמוסר את המידע, בהקשר של איסוף המידע, הסכמה תיחשב לחופשית.

בנוסף, סקירה של ארגון העבודה העולמי (International Labor Organization - ILO) ציינה כי על אף שמרבית תקנות הגנת המידע מסביב לעולם מבססות איסוף ושמירת מידע אישי של עובדים על הסכמה מדעת, מלבד ה-GDPR לפיה כאמור יש קושי בהכשרת ההסכמה, מנגנון זה לא עומד בתנאים אשר נציבות זכויות אדם של האו"ם מציבה לאיסוף מידע.³ לאור הספק ביחס לאפשרות להסכים באופן חופשי בהקשרי עבודה, ארגון העבודה העולמי מעלה חשש כי במקרים רבים זכויות עובדים נפגעים ביחס לאיסוף המידע האישי שלהם.

גם בית הדין האירופי לזכויות אדם (ECHR) התבקש לפסוק בשאלות של איסוף מידע במקומות עבודה במספר מקרים, בהם המידע נאסף באופן מוסתר או גלוי.⁴ מרבית המקרים התמקדו בצילום מקומות עבודה או איסוף התכתבויות שהועברו בשרת של החברה, ומאלו עולה כי בית הדין אינו סובר שאיסוף

¹ OHCHR, A/77/196 Principles underpinning privacy and the protection of personal data (2022), <https://www.ohchr.org/en/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data>.

² EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 (2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

³ ILO, Improving Workers' Data Rights, https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---actrav/documents/publication/wcms_862219.pdf.

⁴ ECHR, Guide to the Case-Law of the European Court of Human Rights - Data Protection (2022), paras. 148-161 https://www.echr.coe.int/documents/d/echr/Guide_Data_protection_EN.

מידע מהווה הפרה עקרונית של הזכות לפרטיות, כעניין שבעקרון, אלא יש לבחון האם ההסכמה ניתנה מראש, כאשר גם עיקרון צמידות המידע למטרה יכולים להכריע אם מדובר באיסוף תקין או לא. בנוסף, מעניין לציין כי בית הדין קבע שקיומו של חשש סביר לפיו התנהגות פוגענית חמורה נעשתה יכול להצדיק קביעת מנגנון איסוף מידע אישי במקומות עבודה – למשל הטרדה מינית או התעמרות – כאשר המטרה היא חשיפת או מניעת אותה התנהגות.⁵

גם בישראל, פער הכוחות בין עובדים למעסיקים משמעותי, במיוחד כיום על רקע פגיעות השוק בעקבות מלחמת חרבות ברזל. הסבירות שעובד ירגיש חופשי להסכים או לסרב לנטילת מידע ביומטרי – המידע האישי ביותר הקיים אודותיו – מוטלת בספק, שכן מעסיקים יכולים להפעיל לחץ ישיר או עקיף, תמריצים או אימים מפורשים או מוסתרים, כאשר העובד עלול לחשוש באופן טבעי או מאי נעימות או אפילו מתוצאה חריפה יותר כלפי מעמדו התעסוקתי. על כן, אנו מציעים לשקול האם ובאילו תנאים ניתן להתבסס על הסכמת העובד לאיסוף מידע ביומטרי. בנוסף, נציין כי כחלק מן הרצון להבטיח את המשך עמידתה של מדינת ישראל בדרישת התאימות של האיחוד האירופי ב-GDPR, ראוי כי, ככל הניתן, הדין הישראלי ובפרט החלטות מדיניות חדשות יתאמו את הסטנדרטים הקבועים בתקנות. עמידה בדרישת התאימות של האיחוד האירופי הכרחית לכלכלת ישראל, שיתוף פעולה בינלאומי מסחרי ודיפלומטי וכן לתדמיתה כמדינה השומרת באופן ראוי על הזכות לפרטיות. לכן, אנו מבקשים להסב את תשומת לב הרשות לעמדתה של המועצה לפיה עובדים אינם מסוגלים להביע הסכמה חופשית אלא במקרים מסוימים בהם יש הקפדה מיוחדת על מרכיב החופשיות.

ככל שלשיטת הרשות יש מקום להתבסס על הסכמה חופשית של עובד, אנו ממליצים כי יתווספו תנאים להבטחה כי אותה הסכמה ניתנת באופן חופשי ככל הניתן, נקי מלחץ או תמריצים למיניהם. למשל, מוצע שלצד הסכמת העובד, המעסיק יצהיר בדבר היעדר השלכות שליליות לסירוב נטילת מידע ביומטרי. לחלופין, ניתן לבקש ממעסיקים אשר מצויים מאגר ביומטרי במקומות עבודה לפרט מהי המדיניות ביחס להסכמה או בחירה האם להשתתף במאגר ומהן החלופות עבור מי שמסרב, על מנת שהרשות תוכל לבחון בעצמה האם מופעלים תמריצים גלויים או נסתרים. לבסוף, על מנת לוודא כי העובד מסכים באופן חופשי ומדעת, מוצע כי ההסכמה תינתן באופן מפורש בלבד, בכתב ככל הניתן כדי לוודא שהעובד מבין את המשמעות המלאה של הסכמתו.

ב. התאמת חובת היידוע לאוכלוסיות בעלי אוריינות דיגיטלית נמוכה

בפסקה 27 לנייר, נכללת רשימה של פרטים אשר חובה ליידע את העובד אודותיהם על מנת לקבל את הסכמתו מדעת. צוין כי יש ליידע את העובד על משמעות האיסוף באופן נרחב, ובפרט לכלול מטרת איסוף המידע, זהות הגורם האחראי על המאגר, אופן הבטחת המידע, הסכנות האפשריות וזכויות העובד בדבר עיון ותיקון המידע. הודגש כי ההסברים צריכים להינתן בשפה ברורה ומובנת. אנו מברכים על הכללת חובת יידוע מפורטת, אולם, כמפורט בנייר, לא כל עובד נהנה מאותה רמת ידע אודות טכנולוגיה ביומטרית וטכנולוגיית מעקב, השפעותיהם על החברה ועל פרטיותם או אמצעי הגנה מקובלים, ולכן הפרטים אשר מוצע לכלול אינם מספקים על מנת לעמוד בדרישת יידוע מהותית, אשר

⁵ ECHR App. Nos. 1874/13, 8567/13, Lopez Ribalda and others v. Spain (2019).

מיידיעת כל עובד ללא הבחנה בין רמת הידע המקדים שלו – ולא רק טכנית, לפיה מעסיקים יוכלו לסמן "V" על הסברת המשמעויות באופן שלא דווקא מעניק את הידע הנדרש לכל עובד. בעידן הדיגיטלי נוצר סט כלים וידע אודות השימוש בטכנולוגיה דיגיטלית, הן באופן אישי ביחס ליכולת להתמצא עם כלים דיגיטליים והן מבחינת ידע כללי אודות הטכנולוגיה הקיימת ומה היא מסוגלת ליצור. ידע וכישורים אלו נקראים ביחד "אוריינות דיגיטלית" ועל פי המדד המקובל ביותר אוריינות זו כוללת חמישה סוגי כישורים: אוריינות במידע ונתונים, תקשורת ושיתוף פעולה, יצירת תוכן דיגיטלי, בטיחות ופתרון בעיות.⁶ כחלק מכישורי בטיחות דיגיטלית, האיחוד האירופי מציע לכלול את היכולת לזהות דרך להגן על מידע אישי וזיהוי הסכנות הכרוכות בשיתוף מידע במרחב הדיגיטלי. כאשר רמות שונות של אוריינות דיגיטלית פוגעות כשלעצמן, שכן רמה גבוהה יותר מקנה ידע ויכולות מתקדמות, הן גם משפיעות על הממשק בין אנשים לחברה בה הם חיים – ובהקשר שלנו, ביחס ליכולת להגן על פרטיות של עצמך ולהכיר בהשלכות השימוש בטכנולוגיות שונות.⁷ בעידן הדיגיטלי, ניכר השימוש הרחב בטכנולוגיות מעקב, על ידי גורמים פרטיים ורשמיים, והסכנה הן של שימוש לרעה במידע או בגניבה או דליפה והגעת המידע לידיים הלא נכונות משמעותית. כאשר אנשים לא מכירים את מגוון הכלים הטכנולוגיים אשר מופעלים בחברה שלהם, וכיצד ניתן לשמור על עצמם ועל הפרטיות שלהם, היכולת שלהם לממש את זכותם לפרטיות נפגעת באופן עמוק. מעבר לכך, יש המבחינים בין אוריינות דיגיטלית תפקודית – שהיא היכולת הנדרשת להתמצא ולהשתלב במרחב הדיגיטלי – לבין אוריינות דיגיטלית ביקורתית (critical digital literacy) שהיא היכולת להבין כיצד תכני אינטרנט נוצרים, וכיצד העידן הדיגיטלי משפיע על הכלכלה, דמוקרטיה בכלל.⁸ נטען כי אוריינות דיגיטלית ביקורתית נדרשת על מנת להבין באופן הוליסטי כיצד ברצונך להשתתף בחברה – ובהקשר שלנו, ללא הבנה כללית של מערכות מידע ביומטריות וההשלכות המגוונות היכולת לקבל החלטה מדעת נפגעת. נדגיש שוב כי ישנן השלכות מרחיקות לכת להטלת מידע ביומטרי. מאגרים ביומטריים מחזיקים כמות עצומה של מידע אישי ורגיש, ועל כן, הסכנה הכרוכה בדליפת חומר או אף תקיפת סייבר גדלה. איננו זרים בישראל להשלכות מרחיקות הלכת של תקיפות סייבר על מאגרי מידע. נדגיש כי לא מדובר בתופעה נדירה או יוצאת דופן: על פי מערך הסייבר הלאומי והלשכה המרכזית לסטטיסטיקה, בשנת 2021, אחד מתוך כל חמישה עסקים (18%) בישראל חווה תקיפת סייבר.⁹ החשש איננו רק מדליפת המידע הקיים, אלא ישנן סכנות נוספות אותן יש להביא בחשבון – בהם סכנה לשימוש במידע ביומטרי לזיוף או גניבת זהות.¹⁰ כאשר מידע ביומטרי הופך למידע שמרבים להשתמש בו במגזר הפרטי, יש

⁶ Riina Vuorikari et. al., *DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes*, EUR 31006 EN (2022), <https://publications.jrc.ec.europa.eu/repository/handle/JRC128415>.

⁷ Faizatush Sholikhah, *The Role of Digital Literacy in Raising Cybersecurity Awareness*, Center for Digital Society (19.1.22), <https://digitalsociety.id/2022/01/19/the-role-of-digital-literacy-in-raising-cybersecurity-awareness/>.

⁸ Gianfranco Polizzi, *Information literacy in the digital age: why critical digital literacy matters for democracy* in INFORMED SOCIETIES (Stephane Goldstein ed.) pg. 2 (2020), https://books.google.co.il/books?hl=en&lr=&id=KRPRDwAAQBAJ&oi=fnd&pg=PA1&dq=right+to+information+digital+literacy&ots=OI7_OC_Cyr&sig=U02cJHu8edowuijtpuaR61eF2UE&redir_esc=y#v=onepage&q=right%20to%20information%20digital%20literacy&f=false.

⁹ מערך הסייבר הלאומי, אחד מחמישה עסקים בישראל חווה תקיפת סייבר (2021) <https://www.gov.il/he/departments/news/cyberweeknews>

¹⁰ ר' למשל, Biometric Authentication Benefits and Risks, Identity Management Institute, at <https://identitymanagementinstitute.org/biometric-authentication-benefits-and-risk>

חשש מוגבר כי לא יינקטו אמצעי הגנה מספקים כגון הצפנה ואבטחת מידע ברמה גבוהה, וכי יקלו בחשיבותו או תתפתח שאננות ביחס להגנה אליו, מה שיגביר את הפגיעות של מי שמסכים למסור מידע ביומטרי במקום עבודתו. מדובר במידע עם חשיבות אדירה, בעל ערך כלכלי רב, אשר שחקנים שונים יכולים לנצל בקלות, והשלכות הניצול יכולים לפגוע באופן חמור באדם אשר המידע הביומטרי שלו שימש לזיוף או עבירה אחרת.

על כן, על מנת לעמוד בדרישת ידוע מהותית לכלל אוכלוסיות העובדים, ובמיוחד אלו עם רמת אוריינות דיגיטלית נמוכה או מזערית החשופים יותר לסכנת ניצול, חשוב לוודא כי המידע מוכן להסביר את המשמעות של מסירת המידע לבעלי רמות שונות של אוריינות דיגיטלית. מוצע לכלול הסברים אודות האופן שבו מידע ביומטרי עובד, באופן טכני ומהותי, והסיכונים הכרוכים בשימוש לרעה בו, בנייר או בנספח אשר יוכלו לשמש מעסיקים ויבטיחו שאנשים אשר נפגעים מהפער הדיגיטלי לא ייפגעו באופן לא מידתי ממסירת מידע ביומטרי באופן לא מודע.

ג. מחיקת מידע ששמירתו אינו נחוצה

בפסקה 42 הרשות ממליצה שהמעסיק יבחן מעת לעת את נחיצות המשך שמירת המידע ויצמצם מידע כאשר אין עוד צורך בהמשך שמירתו. חובת מחיקה שכזו מוכרת כאחד ממנגנוני הגנת הפרטיות המוכרים. למשל, ב-GDPR לנושא מידע זכות למחיקת מידע במקרה ואין עוד צורך בשמירתו בהתאם למטרה לשמה המידע נאסף. כך, לשיטת האיחוד האירופי, חובת המחיקה היא אמצעי עמו ניתן לקדם את עיקרון צמידות למטרה, עיקרון אשר הרשות מדגישה את נחיצותו לשמירה על הזכות לפרטיות. על כן, יש חשיבות מוגברת בחיזוק חובת המחיקה, ובהקשר שלנו אנו מציעים להפוך את ברירת המחדל כך שמידע ביומטרי של עובדים יימחק באופן אוטומטי תוך זמן סביר בהתאם לצורך לשמו הוא נאסף (אם לצורך בדיקת נוכחות חודשית, למשל, מחיקה בסוף כל רבעון משאיר מספיק זמן לאמת את הדיווח). ככל שמעסיק חש שבמקרה ספציפי נדרש לשמר את המידע לתקופה ארוכה יותר, ניתן להרשות לו להאריך את השמירה של אותו פריט מידע, אך מדובר בהחלטה יוצאת דופן על בסיס חשש ספציפי ומבוסס. שינוי זה הופך את ברירת המחדל לשמירה על פרטיות העובד וחיזוק הזכות להישכח, ומאפשר החרגה רק במידת הצורך, במקום לשים את הנטל על המעסיק. מעבר לכך, ניתן לכלול חובת הנמקה אשר תחול על המעסיק במקרה של הארכת שמירת המידע. בנוסף, כאשר מדובר בעובד מדינה אשר אחראי על שמירה ומחיקת המידע, מוצע לכלול סנקציה בגין אי עמידה בדרישות המחיקה.

ד. סיכום

מידע ביומטרי הוא המידע האישי ביותר אשר יש לאדם, וכאשר מדובר במאגר מידע המנוהל על ידי גורמים פרטיים יש חשש מוגבר אודות פגיעה בזכות לפרטיות באמצעותו. מעבר לכך, לאור יחסי העובד-מעביד המורכבים ופערי כוחות בין בעל המידע לנושא המידע יש חשיבות מיוחדת באמצעי הגנה מספקים. על כן, ברצוננו לחזק את העקרונות המוצעים של הרשות ולהציע מקומות בהם ניתן להטיב את ההגנה בהתאם לניסיון וידע המצטבר בקהילה הבינלאומית.

כפי שהסברנו, אנו מציעים להחמיר את התנאים להסכמה חופשית, בשל פערי הכוחות ביחסי עובד-מעביד, והחשש בדבר היכולת לקבל במסגרת יחסים אלו הסכמה מודעת, חופשית ומרצון. בנוסף, אנו מציעים לחזק את חובת היידוע המוצעת ושינוי מנגנון שמירת ומחיקת המידע באופן אשר נועדים להבטיח את מקומה של הזכות לפרטיות, אגב התחשבות בשיקולים של הכללה דיגיטלית, ותוך ייחוס משקל ראוי לסכנות הרבות המגולמות בנטילה וניהול של מידע ביומטרי.



ד"ר טל מימרן

ראש תכנית,

תכלית – המכון למדיניות ישראלית



עו"ד עדן פרבר

חוקרת,

תכלית – המכון למדיניות ישראלית