

סקירה על ה-Data Use and Access Act בבריטניה ותובנות לחקיקה בישראל

מאת עו"ד רבקי דב"ש

חשון תשפ"ו

נובמבר 2025

המכון הישראלי למדיניות טכנולוגיה – FPF-Israel

תוכן עניינים

3	סקירה על ה-Data Use and Access Act בבריטניה ותובנות לחקיקה בישראל
3	1 - מבוא
4	2 - מבנה ה-DUAA
4	2.1 - חלק 1 - גישה למידע אודות לקוחות ולמידע עסקי (Access to Customer Data and Business Data) –
4	2.2 - חלק 2 - שירותי אימות דיגיטלי (Digital Verification Services) -
5	2.3 - חלק 3 - רישום לאומי לנכסים תת-קרקעיים (National Underground Asset Register) -
5	2.4 - חלק 4 - רישומי לידות ופטירות (Registers of births and deaths) –
5	2.5 - חלק 5 - הגנת מידע אישי ופרטיות (Data Protection and Privacy) –
5	2.6 - חלק 6 - הוועדה למידע (The Information Commission) -
5	2.7 - חלק 7 – הוראות נוספות לגבי שימוש ונגישות למידע (Other provision about use of, or access to, data) –
6	2.8 - חלק 8 - הוראות שונות (Final provisions) –
6	3 – ההסדר המתוקן ביחס להגנת מידע אישי
6	3.1 – שימושים לצרכי מחקר וסטטיסטיקה (סעיפים 67-68 ל-DUAA)
7	3.2 - אינטרסים לגיטימיים מוכרים (סעיף 70 ל-DUAA)
8	3.3 - הגבלת מטרת השימוש (סעיף 71 ל-DUAA)
8	3.4 - גמישות בהגדרת מידע רגיש (סעיף 74 ל-DUAA)
9	3.5 - עיון במידע (סעיפים 76-78 ל-DUAA)
10	3.6 – קבלת החלטות אוטומטיות (Automated Decision Making – ADM) (סעיף 80 ל-DUAA)
11	4 - מועצת המידע (Information Commission) – חלק 6 לחוק
11	4.1 שינוי ארגוני - מבני
11	4.2 – הרחבת סמכויות האכיפה של הרגולטור
12	4.3 – חובות שקיפות מוגברות (סעיפים 95 ו-102 ל-DUAA)
12	5 - סיכום

סקירה על ה-Data Use and Access Act בבריטניה ותובנות לחקיקה בישראל

1 - מבוא

ב-19 ביוני 2025 אושר בבריטניה החוק לשימוש וגישה למידע (Data Use and Access – DUAA Act). החוק מייצג שינוי פרדיגמה בגישה הבריטית לנתונים – מתפיסת הגנה על נתונים, לתפיסה המבקשת לשרטט שימוש מושכל בהם, תוך ניסיון למנף איתם יכולות מבלי לפגום בהגנה על מידע אישי. החוק מציג משטר נתונים גמיש יותר מזה המוצג באיחוד האירופי, תוך ניסיון לשמר את התאימות של ההסדר החדש ל-GDPR.

החוק מאגד תחתיו מספר תחומים שכולם עוסקים בתחום השימוש במידע במטרה לרתום את כוחם של נתונים (אישיים ושאינם אישיים) לטובת צמיחה כלכלית, תמיכה בממשל דיגיטלי מודרני, ובשיפור חייהם של אנשים – כך לפי פתיחת דברי ההסבר לחוק.

הוראות החוק נכנסות באופן מדורג לתוקף – בין חודשיים ל-12 חודשים. נצביע על כך שבפרקטיקת החקיקה בה נעשה שימוש, ניתנו סמכויות רבות לדרג המיניסטריאלי לקבוע תקנות, שחלקן יוצרות את ההסדר המהותי, מסמכי מדיניות וקודי התנהגות, וזאת במטרה לשמר גמישות שנדרשת בעת העיסוק בתחומים טכנולוגיים חדשניים.

החברה האזרחית בבריטניה הביעה חשש על ההקלות שערכה החקיקה בתחום הגנת המידע האישי. הקלות אלו באות לידי ביטוי בהפחתת השקיפות והמחויבות לזכויות נושאי מידע, ההיתר הרחב יותר שניתן לשימוש בהחלטות מבוססות תהליכים אוטומטיים ומתן סמכויות רבות מדי בידי הדרג המיניסטריאלי.¹

בנוסף, לא ברור האם האיחוד האירופי אכן יראה את המשטר החוקי החדש כתואם את עקרונות ה-GDPR החלטה בנושא נדחתה לדצמבר 2025. עם זאת, נציבות האיחוד האירופי העריכה כי השינויים בחוק ה-DUAA שומרים על רמת הגנה שוות ערך על נתונים אישיים לזו הקיימת באיחוד האירופי, וכבר פרסמה טיוטת החלטת התאמה (adequacy decision) לגבי החוק החדש בבריטניה.² מועצת

¹ ראו לדוגמא את המסמכים של ארגוני החברה האזרחית הבאים, בנושא הסתייגותם וחששותיהם מהחוק: [Big Brother Watch](#), [EDRi](#) ודיווח של ארגון [Statewatch](#) על מכתב של עשרות ארגונים שפנו לממשלה בעקבות הצעות החוק והחששות שלהן מפגיעה בזכויות אדם.

² https://commission.europa.eu/document/download/6f636fa0-30d4-4c05-a713-64484ad913fa_en?filename=Draft%20Renewal%20of%20EU%20adequacy%20decision%20for%20the%20UK%20under%20the%20GDPR.pdf

הגנת המידע האירופית (EDPB) פרסמה לאחרונה מספר המלצות³ בנוגע לנושאים שיש להמשיך ולפקח עליהם באופן שוטף על ידי הנציבות, וכן לגבי תחומים שבהם נדרש ניתוח נוסף במסגרת ההחלטה הסופית על ההתאמה.

מעניין לבחון בעין ישראלית את התפיסה הכוללת שמציגה הממשלה הבריטית, כמו גם את ההסדרים הספציפיים.

מטבע הדברים אנו נתמקד במסמך זה בהוראות ה-DUAA הרלוונטיות להסדרים הנוגעים לניהול מידע אישי, אולם חשוב כי לפני שנצלול לתחום זה, לתת את ההקשר הרחב יותר של החוק, בקצרה.

2 - מבנה ה-DUAA

ה-DUAA נחלק ל-8 חלקים מרכזיים –

2.1 - חלק 1 - גישה למידע אודות לקוחות ולמידע עסקי (Access to Customer Data and Business Data)

חלק זה מגדיר מסגרת חוקית ליצירת "סכמות נתונים חכמות" שיאפשרו ללקוחות לבקש מספקי שירותים (כמו ספקי תקשורת או שירותים פיננסיים) לשתף את נתוניהם עם צדדים שלישיים מורשים, במטרה לאפשר ללקוחות להשוות מחירים בקלות, לעבור בין ספקים, ולקבל שירותים מותאמים אישית.

מרבית ההוראות ייקבעו בתקנות, מתוך מטרה לשמר גמישות נורמטיבית בתחום זה.

2.2 - חלק 2 - שירותי אימות דיגיטלי (Digital Verification Services)

חלק זה מקים מסגרת חוקית סטטוטורית לשירותי זהות דיגיטלית בבריטניה, ומעניק בסיס חוקי למשרד לזהויות ותכונות דיגיטליות (OfDIA) לפקח על ספקי שירותי אימות דיגיטלי ולהעניק להם "סימן אמון" ממשלתי. המסגרת כוללת הוראות הגנת פרטיות מחמירות כגון: איסור מפורש על פרופילינג למטרות שיווק צד שלישי, איסור על יצירת מאגרי נתונים גדולים שעלולים לחשוף מידע רגיש, חובת קבלת הסכמה מפורשת לכל שיתוף נתונים, ועקרון מזעור נתונים. השימוש בזהויות דיגיטליות נשאר וולונטרי.

³https://www.edpb.europa.eu/news/news/2025/draft-uk-adequacy-decisions-edpb-adopts-opinions_en

גם בחלק זה ניתנות סמכויות רבות בידי השרים, אולם מדובר בעיקר בסמכויות לקביעת מסמכי מדיניות וקודי התנהגות, ולא הסדרה ברמה נורמטיבית של חקיקת משנה.

2.3 - חלק 3 - רישום לאומי לנכסים תת-קרקעיים (National Underground Asset Register)

חלק זה מחייב חברות תשתית (גז, מים, חשמל ותקשורת) לספק נתונים למפה דיגיטלית לאומית של צינורות וכבלים תת-קרקעיים במטרה לשפר את הבטיחות והיעילות בעבודות בנייה ותחזוקה על ידי מניעת פגיעה בתשתיות תת-קרקעיות.

גם בחלק זה הסדרים רבים מותנים בקביעת תקנות על ידי הדרג המיניסטריאלי.

2.4 - חלק 4 - רישומי לידות ופטירות (Registers of births and deaths)

חלק זה מעביר את רישום הלידות והפטירות בבריטניה למערכת דיגיטלית. מדובר בפרק קצר וטכני יחסית. ההוראות בתחום הגנת המידע האישי מוגנת מכח החוק שהקים את המרשם ב-1953, וכן בהסדרים הכלליים להגנת מידע אישי בבריטניה, ועל כן אין לגביהם פירוט מיוחד בחקיקה החדשה.

2.5 - חלק 5 - הגנת מידע אישי ופרטיות (Data Protection and Privacy)

חלק זה מתייחס לשינויים ב-GDPR הבריטי, ומהווה את החלק הארי של החקיקה. נרחיב לגבי חלק זה בהמשך הסקירה.

2.6 - חלק 6 - הוועדה למידע (The Information Commission)

חלק זה מחליף את משרד הנציב למידע (ICO) בוועדה למידע חדשה עם מבנה ממשל תאגידי. הוועדה תכלול מועצת מנהלים ומנהל כללי, ותקבל סמכויות אכיפה מוגברות. נרחיב לגבי חלק זה בהמשך הסקירה.

2.7 - חלק 7 – הוראות נוספות לגבי שימוש ונגישות למידע (Other provision about use of, or access to, data)

זהו חלק הטרוגני מאוד, הכולל נושאים שלא התאימו לפרקים האחרים ועוסק בהוראות נקודתיות יותר. ישנן מספר הוראות מעניינות שמעניין להכיר, כגון:

- סמכות לקבוע בתקנות מתן גישה לנתונים של רשתות חברתיות לחוקרים עצמאיים (סעיף 125);
- מנגנון לשימור מידע ברשתות חברתיות במקרה של מות ילד, כאשר חוקר מקרי מוות חושד שהרשת מעורבת במותו, ומתן גישה למידע שנשמר להורים השכולים (סעיף 124);
- סמכות להכיר במוצרי אמון כגון חתימה דיגיטלית, חותמות זמן וכו' ממדינות זרות כמהימנים ושוי ערך למוצרים בריטיים מוסמכים (סעיף 132);

○ דרישה להערכת השפעה כלכלית ודוח מקיף על זכויות יוצרים ובינה מלאכותית (סעיפים 135-136) ועוד.

הוראות הנוגעות להגנת המידע האישית שזורות בהוראות הפרק בדרכים שונות (כגון דרישת פסאודונימיזציה במידע ביומטרי מחו"ל, מגבלות זמן לשימור נתונים ואיסור מוחלט על שיתוף מידע עם רשויות זרות ככל שהדבר יפר את חוקי הגנת המידע האישית בבריטניה), אך במרבית הסעיפים נקבע כי חוק ה-GDPR הבריטי וחוק הגנת המידע מ-2018 גוברים.

2.8 - חלק 8 - הוראות שונות (Final provisions)
הוראות פרוצדורליות הנוגעות לחוק כגון: שם החוק, מועד התחולה, המדינות עליהן חל ההסדר ועוד.

3 – ההסדר המתוקן ביחס להגנת מידע אישי

התיקון ביחס להגנת המידע האישית משמעותי ומעלה מספר נקודות מעניינות. אין במסמך זה כדי לבצע סקירה מלאה של כלל ההוראות של התיקון לחוק בעניין הגנת המידע האישית, אלא להאיר זרקור להסדרים שיש בהם עניין לשיטתנו למומחה הפרטיות בישראל, תוך ניסיון להשוות ולהעלות שאלות ביחס להסדר הישראלי ולמקומות שאליו ניתן לפתח אותו.

החוק מתקן את ה-Data Protection Act 2018, ואת ה-GDPR כפי שאומץ בבריטניה. בחלק מהמקרים מדובר בתיקוני נוסח, ובחלקם בהוספת סעיפים וחלקים שלמים לחוק.

להלן השינויים המרכזיים בחוק שיש בהם לשיטתנו לעניין את העוסק בתחום הגנת המידע האישית בישראל.

3.1 – שימושים לצרכי מחקר וסטטיסטיקה (סעיפים 67-68 ל-DUAA)

ב-GDPR שימוש לצרכי מחקר וסטטיסטיקה מוכר כשימוש מותר לצורך עיבוד מידע אישי. ה-DUAA מוסיף להגדרות הנוגעות למחקר פרשנות מרחיבה, ומכאן מרחיב את העוגן החוקי לעיבוד מידע על בסיס זה. ההרחבה מטמיעה פרשנות שניתנה להגדרת המחקר בדברי ההסבר של הנוסח הרשמי של ה-GDPR ובמסמכים של רגולטורים באירופה, באופן שמייצר ודאות גדולה יותר.

התיקון מגדיר "מחקר" גם אם הוא נועד לצרכי פיתוח טכנולוגי או הדגמה, ובתנאי שניתן לתאר אותם כ"מדעיים", וכן מחקר יסודי או יישומי. מחקר גנאלוגי נכנס גם הוא במפורש בגדר מחקר היסטורי לפי התיקון.

ביחס למחקר בתחום בריאות הציבור, התיקון מצמצם מעט את ההגדרה וקובע כי הוא ייכנס להגדרת מחקר אם הוא מבוצע אך ורק לטובת האינטרס הציבורי. נדמה כי דיוק זה נועד להחריג מחקרים לטובת רווח כלכלי בלבד.

ביחס לאפשרות לקבל הסכמה לצרכי מחקר, התיקון הבריטי מעביר מדברי ההסבר ל-GDPR ביחס ל"הסכמה רחבה" מספר הוראות, כגון, האפשרות לקבל הסכמה רחבה במקום בו אי אפשר לזהות את מטרות המחקר במועד ההסכמה, האפשרות לתת לאדם להסכים רק לחלקים מסוימים במחקר ועוד.

בנוסף, בסעיף 86 לתיקון, נוספים לחוק אמצעי הגנה ייחודיים לתחום המחקר, הארכיונים והסטטיסטיקה. הסעיף קובע תנאים מקדמיים לעיבוד מידע למטרות אלו כגון שללא עיבוד המידע לא ניתן להשיג את מטרות המחקר; שמקום בו נושא המידע עלול להפגע באופן ספציפי מהמחקר, לא יכירו בקיומו של המחקר, כהגנה מספקת; שעורך המחקר מבטיח קיומם של אמצעים טכניים וארגוניים שמטרתם כיבוד עקרון המינימליזציה של המידע ועוד.

בישראל אין הסדרה כלל של שימוש בנתונים לצרכי מחקר וסטטיסטיקה, ואף הם, ככל עיבוד מידע אחר בישראל מותנים בהסכמה. מוצע כי בעת הסדרה כאמור תנתן הדעת לניסוח הבריטי המגדיר בצורה ברורה יותר את התנאים לשימושים מותרים אלו תוך התייחסות לייחודיותם.

3.2 - אינטרסים לגיטימיים מוכרים (סעיף 70 ל-DUAA)

תיקון החוק מייצר בסיס חוקי חדש לעיבוד מידע - "אינטרסים לגיטימיים מוכרים". התוספת הראשונה מפרטת אלו אינטרסים מוכרים כאלו. עיבוד מידע על בסיס אינטרסים אלו, פוטר את בעל השליטה מלבצע הערכת אינטרסים לגיטימיים (LIA - Legitimate Interests Assessment), חובה הקיימת ב-GDPR. הערכה כאמור היא חובה בירוקרטית שיש בצידה השקעת משאבים וזמן מבעל השליטה. עם זאת, מבחן ההכרחיות (Necessity Test) של עיבוד המידע להשגת האינטרסים, עדיין נדרש.

הקטגוריות בתוספת 1 כוללות תחומים כגון שמירה על בטחון ובטיחות הציבור, מניעת פשיעה, הגנה על קטנים וחסרי ישע, מצבי חירום ועוד. המטרה היא לעודד את אותם חברות לעשות שימוש במידע האישי שברשותן, בכפוף לאמור בחוק, במטרה לקדם אינטרסים חשובים שבסופו של יום מובילים להגנה טובה יותר על המידע האישי המצוי ברשותן.

סעיף זה הוא סעיף המנסה לבחון ראיה כוללת של שימוש בנתוני מידע אישי לצרכים בעלי אינטרס ציבורי חזק, גם על חשבון היתר לעיבוד מידע נקודתי. לאור הנושאים המוגדרים בתוספת הראשונה, בפועל במקרים רבים מדובר בהקלה בירוקרטית של גופים ממשלתיים וציבוריים ביחס לעיבוד מידע שעשויים להיות לו השלכות אקוטיות על האדם הבודד. מעניין יהיה לראות כיצד הפתח האמור ייושם בפועל.

מכל מקום, ישראל נדרשת קודם כל להסדיר את העוגנים החוקיים הבסיסיים לעיבוד מידע לגיטימי נוסף על הסכמה, הסדר עקרוני וחסר בדין הישראלי.

3.3 - הגבלת מטרת השימוש (סעיף 71 ל-DUAA)

התיקון עושה שינוי משמעותי בהגבלת מטרת השימוש במידע אישי, כצמוד למטרה. מקובל להכיר גם במטרות נגזרות מהמטרה המקורית, ככאלו המתירות עיבוד מידע אישי. סעיף 71 לתיקון מקים חזקה הקובעת כי ניתן להכיר בהתאמה בין שתי מטרות לעיבוד מידע לצורך הכרה בחוקיות העיבוד, אם מתקיימים שני התנאים הבאים:

1. המטרה החדשה עונה על אחד התנאים המנויים בתוספת השנייה שעוסקת ברובה בפעילות מתחום האינטרס הציבורי (מניעת פשיעה, הגנה על חסרי ישע וכד');
2. המטרה החדשה עונה על אחד התנאים החדשים שנקבעו בתיקון המכיר בעיבוד מידע כחוקי (lawfulness).

מדובר בחזקה שאם שני התנאים בה מתקיימים, יראו את העיבוד כנגזר מהמטרה המקורית וכחוקי.

ככל שהחזקה האמורה לא מתקיימת, נקבעו בתיקון מבחנים שיכולים להצביע על תאימות מטרות כגון: ההקשר בו נאסף המידע והיחסים בין נושא המידע לבעל השליטה; ההשפעות של העיבוד הנוסף על נושאי המידע; קיומם של הגנות מספקות ועוד.

החזקה מייצרת ודאות רבה יותר אצל מעבדי המידע, מכיוון שההסדר הקיים ב-GDPR מחייב ניתוח עובדתי ונורמטיבי של מקרה של עיבוד מידע נוסף. החזקות מאפשרות להגדיר מהי הציפייה המוכרת ככזו שמאפשרת עיבוד מידע כנגזרת מהמטרה הראשונית, ומכאן כעיבוד נוסף לגיטימי. עם זאת, גם הכרה במטרה הנוספת כמטרה תואמת את המטרה המקורית לעניין ההסכמה אינה מספקת – כיוון שנדרש לבחון שגם למטרה החדשה יש בסיס עיבוד חוקי.

מדובר בשינוי משמעותי ביחס לקיים ב-GDPR ושוב בעיקר אל מול גופי בטחון ואכיפה. יש החוששים מעיבוד מידע ללא ידיעתו ושליטתו של האדם בשונה מהמקובל במשטר האירופי.

בישראל, בה העוגן היחיד לעיבוד חוקי של מידע הוא הסכמה, הצורך ביצירת חזקות שיאפשרו להכיר במטרות חדשות כתואמות את המטרה המקורית לה ניתנה הסכמה – הכרחית. עם זאת, בהנתן הדרישה הנוספת למציאת עוגן חוקי לעיבוד מידע גם ביחס למטרה החדשה, מחזירה בישראל את הדרישה להסכמה, ומכאן כי אימוץ תפיסה כאמור ללא הוספת עוגני עיבוד חוקיים, אינו רלוונטי לעת הזו בישראל.

3.4 - גמישות בהגדרת מידע רגיש (סעיף 74 ל-DUAA)

סעיף 74 לתיקון נותן סמכות לשר לשנות בתקנות את קטגוריות המידע הרגיש – להוסיף או להפחית קטגוריה. ההבנה היא שהשינויים הטכנולוגיים עלולים להוביל ליצירת קטגוריות רגישות חדשות, כמו שבעבר היה עם מידע ביומטרי, או לאיין קטגוריה שהיום מוגדרת בחוק. תפיסה זו מתחברת לניסיון לייצר משטר רגולטורי גמיש שמאפשר שינויים והתאמות שלא בחקיקה ראשית.

מוצע גם בישראל לצבוע את המקומות שדורשים גמישות רגולטורית רבה יותר, ומה הם האזורים שניתן להעביר לשינוי והתאמה במסגרת חקיקת משנה בלבד.

3.5 - עיון במידע (סעיפים 76-78 ל-DUAA)

ה-DUAA מציע תפיסה מחודשת ביחס לניהול בקשות לעיון במידע של נושאי המידע, במטרה לייצר איזון מחודש בין זכות הגישה למידע של נושא המידע, לבין הנטל המוטל על בעלי השליטה. בבקש להתמקד במספר הסדרים ספציפיים בנושא זה -

3.5.1 הארכת המועד למתן מענה (סעיף 76)

ככלל על בעל השליטה לתת מענה לבקשה לעיון במידע תוך 30 יום. עם זאת, התיקון קובע כי בעל השליטה יכול לעצור את מירוח הזמן ככל שהוא ממתין לאימות זהות, להבהרת היקף הבקשה, או לקבלת תשלום אגרה במקרים שהבקשה מוגזמת או בלתי מבוססת.

3.5.2 חיפושים כמענה לבקשת מידע (ס' 78)

התיקון קובע כי בעל שליטה אינו חייב לספק את מלוא המידע המבוקש בבקשת עיון במידע, אלא רק את המידע שניתן לספק על בסיס חיפוש סביר ומידתי. לפי דברי ההסבר, השינוי נועד להקל על ארגונים שמתקשים להשיב לבקשות עיון מורכבות, לדוגמה: כאלו הדורשות חיפושים במערכות רבות, גיבויים ישנים וארכיונים. הוא גם נועד למנוע ניצול לרעה של בקשות לעיון במסגרת הליכים משפטיים, כאשר המטרה היא רק להכביד על בעל השליטה ולא לממש את זכות הגישה עצמה.

3.5.3 מידע שיש להעביר לעיון נושא המידע (סעיף 77)

התיקון מקל על בעלי השליטה לדחות בקשות לעיון של נושאי מידע. הוא מאפשר לדחות בקשות שאינן מבוססות או מוגזמות, והוריד מאפשרות זו את הדרישה הקיימת ב-GDPR כי דחיית בקשות כאמור תהיה רק אם חוסר הביסוס או ההגזמה ברורים בעליל. התיקון מוסיף חזקה סטטוטורית הקובעת כי בקשה חוזרת למידע תוך פחות משישה חודשים, תחשב כמוגזמת אלא אם המבקש הצליח להצביע על שינוי במצב שמצדיק את הבקשה החוזרת.

בישראל, סעיף 13 לחוק הגנת הפרטיות מעניק זכות עיון במידע, אך אינו מגדיר היקף החיפוש הנדרש. מסקירת פסקי הדין והספרות המשפטית בישראל נדמה כי נכון למועד זה נעשה שימוש מינורי בזכות לעיון, ועל כן לא ברור עד כמה הנטל על ארגונים כבד בעת מימוש הזכות. עם זאת, מצב זה עשוי להשתנות עם תיקון מס' 13 הגורם להעלאת מודעות ציבורית מחד ולהגברת הסנקציות הפוטנציאליות מאידך.

יש להניח כי בפועל, בעלי השליטה במאגרי מידע בישראל מספקים רק את המידע הזמין בקלות וכי הם אינם משיבים לבקשות שאינן מבוססות או מוגזמות. מכאן כי מוצע לבחון תיקון בחוק הישראלי שגם אם לא יאמץ את ההסדר הבריטי במלואו, יוביל לקביעת מסגרת ברורה יותר ביחס למימוש זכות העיון במאגרי מידע באופן שתקח בחשבון גם את הנטל והעלות של מימוש זכות זו אצל בעל השליטה.

3.6 – קבלת החלטות אוטומטיות (Automated Decision Making – ADM) (סעיף 80 ל-DUAA)

התיקון מציע תפיסה מחודשת ביחס לקבלת החלטות אוטומטיות על נושאי מידע, ובכלל זה פרופיילינג. ההסדר מקל יותר מאשר ההסדר הקיים ב-GDPR, במטרה לעודד חדשנות בתחום הבינה המלאכותית ולמקם את בריטניה כמרכז AI עולמי. המעבר ממודל מגביל למודל מתיר עם הגנות פרוצדורליות, מבטא תפיסה שלפיה ADM אינו בהכרח מזיק, ושהסיכונים ניתנים לניהול באמצעות שקיפות, הסבר וזכות לסקירה אנושית. עם זאת, יש גם חששות משמעותיים מפגיעה בזכויות, אפליה אלגוריתמית, וחוסר שקיפות אפקטיבית עמם ההסדר הבריטי החדש מנסה להתמודד.

3.6.1 הגבלות על קבלת החלטות אוטומטיות

החלטה משמעותית⁴ המתבססת באופן מלא או חלקי על עיבוד מידע רגיש (קטגוריות מיוחדות של מידע אישי), אינה יכולה להתקבל על בסיס החלטה אוטומטית⁵ אלא אם מתקיים אחד מהתנאים הבאים –

1. נושא המידע נתן הסכמה מפורשת לעיבוד המידע האישי;
2. ההחלטה הכרחית לכריתת חוזה בין נושא המידע לבעל השליטה או לביצועו, או שההחלטה נדרשת ומורשית על ידי החוק;
3. העיבוד נדרש מסיבות של עניין ציבורי.

3.6.2 אמצעי הגנה לקבלת החלטות אוטומטיות

החוק קובע הגנות לצד ההיתר המסוים לקבל החלטות באופן אוטומטי. ההגנות כוללות –

1. העברת מידע לנושא המידע ביחס להחלטות שהתקבלו אודותיו בהתבסס על החלטות אוטומטיות;
2. מתן אפשרות לנושא המידע –
 - 2.1 לטעון טענות כנגד ההחלטה;
 - 2.2 לדרוש התערבות אנושית בקבלת ההחלטה;

⁴ החלטה משמעותית היא החלטה בעלת השלכות משפטיות על נושא הנתונים, או משפיעה עליו באופן משמעותי דומה.

⁵ משמעות החלטה אוטומטית על פי החוק הוא החלטה המבוססת על עיבוד אוטומטי של נתונים אישיים, ללא מעורבות אנושית משמעותית.

2.3 לערער על ההחלטה.

תחום הבינה המלאכותית טרם הוסדר בישראל באופן נורמטיבי, למעט מספר הנחיות ממשלתיות. התיקון הבריטי מציע מודל המבקש לבסס הגנות נדרשות בשל שימוש במערכות לקבלת החלטות אוטומטיות, ולא רק להגביל את היכולת לעשות שימוש במערכות כאמור.

4 - מועצת המידע (Information Commission) – חלק 6 לחוק

4.1 שינוי ארגוני - מבני

חלק 6 לתיקון קובע כי סמכויותיו של נציב המידע הבריטי אשר עמד בראש ה-ICO, יועברו ל"מועצת המידע". בנוסף, התיקון מוסיף על סמכויות הפיקוח של הנציבות. התיקון בחלק זה אינו תיקון סמנטי בלבד, והוא מקדם רפורמה מבנית ותפקודית בגוף הרגולטורי – סוגיה מעניינת במיוחד עם כניסת תיקון 13 לתוקף, תיקון שהתמקד בהסדרת סמכויות הרשות להגנת הפרטיות בישראל.

המודל המבני מחליף את נציב המידע – מינוי של אדם יחיד אשר נושא באחריות אישית לכל החלטות הארגון - למועצת המידע. מועצה זו היא גוף תאגידי עם אחריות משותפת, אשר לה מועצת מנהלים הקובעת מדיניות אסטרטגית, ומנכ"ל האחראי על ניהול הארגון באופן יומיומי. המודל החדש מקים מועצה בה חברים מומחים במגוון תחומים, במקום נושא משרה אחת שגם אם הוא בעל ידע רחב, אינו בהכרח מתמקצע בתחומים מרובים כפי שניתן לקבל ממינוי גוף בעל ריבוי חברים.

בנוסף, ניתן לראות בהגדרת מטרותיה של המועצה, והעקרונות על פיהן היא פועלת, את הרוח הכללית של החוק הנותנת מקום לחדשנות לצד החשיבות בהגנת מידע אישי (סעיף 91). המטרה העיקרית של המועצה היא (בתרגום חופשי) "להבטיח רמת הגנה מתאימה למידע אישי, תוך התייחסות לאינטרסים של נושאי מידע, בקרים ואחרים ולענייני אינטרס ציבורי כללי, ולקדם אמון ציבורי ובטחון בעיבוד מידע אישי".

עם זאת, החוק מונה את הנושאים להם המועצה צריכה לתת את הדעת בעת קידום מטרותיה. בין היתר החוק מצוין את הצורך להתייחס לחדשנות, תחרות, מניעה, חקירה, גילוי והעמדה לדין של עבירות פליליות, שמירה על ביטחון ציבורי וביטחון לאומי והגנה מיוחדת לילדים.

4.2 – הרחבת סמכויות האכיפה של הרגולטור

נוסף על השינוי המבני, התיקון מעניק סמכויות חדשות למועצה, שלא היו בידי הנציבות, ביניהם –

- זימון עדים לראיונות לתשאול פורמלי. עד כה הסמכות של הנציבות כללה רק דרישת מסמכים (סעיף 100 לתיקון);

- הצגת דרישה לבעל שליטה ליצור ולהציג דוחות מומחים טכניים מקצועיים במימון בעל השליטה (סעיף 98 לתיקון);
 - הבהרה כי דרישת מידע מאת המועצה כוללת גם דרישת מסמכים (סעיף 97 לתיקון).
 - בנוסף, מוטלים על המועצה תפקידים חדשים ובהם –
 - פיקוח על שירותי אימות דיגיטלי (DVS)
 - פיקוח על סכמות נתונים חכמים (Smart data)
 - מעורבות בפיקוח על הגנת הנתונים במסגרת המפה הלאומית של תשתיות תת קרקעיות (NUAR)
 - תפקידים בתחום מניעת הלבנת הון הקשורים לעיבוד נתונים.
- כל אלו הופכים את מועצת המידע לגוף המעורב בניהול נתונים גם באופן אקטיבי, ומרחיב את שדה הפעילות והאחריות של המועצה.

4.3 – חובות שקיפות מוגברות (סעיפים 95 ו-102 ל-DUAA)

סעיפים 95 ו-102 לתיקון מטילים חובות דיווח חדשות במטרה להגביר את השקיפות והאחריות של המועצה. חובות אלו מטילים על המועצה לפרסם ניתוח ביצועים שנתי באמצעות אינדיקטורים מדידים (KPIs), וכן לפרסם דוח שנתי על פעולות רגולטוריות הכולל אופי החקירות, הזמן שנדרש והסמכויות שהופעלו. נעיר כי גם בתיקון מס' 13 נדרשת הרשות להגנת הפרטיות להציג דו"ח מפורט אחת לשנה לשם הגברת השקיפות. מטבע הדברים ישנה חפיפה משמעותית בין התוכן שהוגדר בחוק הבריטי לזה שהוגדר בחוק הישראלי.

בהנתן המיקוד של תיקון מספר 13 בחוק הישראלי בסמכויות האכיפה של הרשות להגנת הפרטיות, מעניין במיוחד להשוות בין שני ההסדרים השונים.

התיקון הבריטי מבקש לייצר רשות מגוונת יותר במומחיות שלה, ובהיקף הנושאים בהם היא עוסקת, תוך יצירת איזונים מובנים שעליה לשקול בהפעלת סמכויותיה. לעומת זאת תיקון 13 העמיק את יכולת הפיקוח של הרשות, והעלה את גובה העיצומים הכספיים באופן משמעותי, אולם הוא לא הרחיב את התחומים בהם הרשות פועלת, ובכך המניע אותה באופן שאולי תואם יותר את המורכבות שבדיני הגנת הפרטיות לעת הזו.

5 - סיכום

ה-DUAA מייצג שינוי משמעותי בגישה הבריטית לניהול נתונים. ממשטר מגן בעיקרו, למשטר המבקש לאזן בין הגנה על פרטיות לבין מיצוי הפוטנציאל הכלכלי והחברתי של נתונים. החוק מציע מסגרת גמישה יותר מה-GDPR האירופי, תוך שמירה, בהתבסס על טיטת ההערכה של נציבות האיחוד האירופי, על רמת הגנה מספקת שתאפשר שימור ההכרה בתאימות מצד האיחוד האירופי.

השינויים המרכזיים בתחום הגנת המידע כוללים הרחבת בסיסי העיבוד החוקיים (אינטרסים לגיטימיים מוכרים), גמישות בשימוש במידע למחקר ולמטרות משניות, הקלות לבעל השליטה במימוש זכות העיון, ומעבר ממודל מגביל למודל מאפשר בתחום קבלת החלטות אוטומטיות. במקביל, החוק מחזק את המסגרת הרגולטורית באמצעות הקמת מועצת המידע, הרחבת תחום האחריות של המועצה, והרחבת סמכויות האכיפה של הרגולטור.

מנקודת מבט ישראלית אנו סבורים כי החקיקה הבריטית מציעה מספר תובנות רלוונטיות:

ראשית, ההכרה בצורך בגמישות רגולטורית בתחומים טכנולוגיים מהירי התפתחות, באמצעות האצלת סמכויות לדרג המיניסטריאלי והרגולטורי. עם זאת יש לחדד את השאלה עד לאיזה גבול יש לאפשר גמישות כאמור. **שנית**, ההבנה שהגנת פרטיות יכולה לייצר הסדרים מאפשרים, ולא רק הסדרים מגבילים. **שלישית**, החשיבות של הסדרה ברורה לשימושים ספציפיים כמו מחקר מדעי והחלטות אוטומטיות, תחומים שטרם הוסדרו בישראל באופן מקיף.

עם זאת יש לזכור כי ה-DUAA מעורר גם חששות ממתן סמכות רבות מדי בדרג המבצע, ופגיעה רבה מדי בזכויות הפרט בשם החדשנות, היבטים שהודגשו על ידי מועצת הגנת המידע האירופית (EDPB) בחוות דעתה על טיוטת החלטת ההתאמה. האתגר המרכזי שעומד בפני בריטניה, ושגם ישראל תתדרש להתמודד איתו בעת גיבוש תיקון מס' 14, הוא כיצד ליצור מסגרת שמאזנת בצורה מוצלחת בין חדשנות ושימוש יעיל בנתונים, תוך שמירה אמיתית על זכויות הפרט. מוצע כי בעת הבחינה והדיון שייערך בנושא בישראל, ייבחן גם ההסדר הבריטי, על הניסיון שייצבר מיישומו.