מדריך GDPR לחוקרי אוניברסיטת תל-אביב

התקנות הכלליות להגנה על מידע (General Data Protection Regulations – GDPR) הן דבר חקיקה החל במישרין בכל אחת מ-28 מדינות האיחוד האירופי. הן קובעות דין זהה החל בכל אחת מהן במישרין. התקנות נכנסו לתוקף במאי 2018 וחוללו מהפכה באופן שבו מידע אישי נאסף, נשמר, מעובד, מועבר ואף מושמד. **מהפכה זו לא פסחה על חוקרי האוניברסיטה: היא משליכה במישרין הן על פעילותם המחקרית, הן על האופן שבו בקשותיהם לקבלת מענקי מחקר מהאיחוד האירופי נבחנות והן על שיתופי פעולה עם גורמי מחקר באקדמיות ברחבי עולם בכלל ובאירופה בפרט.**

ה-GDPR הוא חלק ממכלול של דינים, הידועים כדיני הגנת הפרטיות או הגנת המידע. דינים אלה נהוגים במרבית מדינות תבל, עם זה הם שונים בפרטיהם: חוק הגנת הפרטיות, התשמ"א-1981 הוא המקבילה הישראלית לתקנות האירופאיות. כל מחקר המערב יחידים מישראל חייב להתחשב קודם כל בהוראותיו. לצדו מכיר חוק יסוד: כבוד אדם וחירותו בזכות לפרטיות כזכות חוקתית. חוקים אחרים בישראל עוסקים בנושאים פרטיקולריים של פרטיות ומידע וגם בהם יש להתחשב, כמובן. לדוגמה, חוק זכויות החולה, תשנ"ו-1996 יכול שיגע בנושאים של מחקר רפואי, חוק מידע גנטי, תשס"א-2000 נוגע במידע המתחייב משמו וכיו"ב.

בארצות-הברית, לעומת זאת, המשטר המשפטי שונה לגמרי. אין חוק מקיף המגן על כל מידע אישי באשר הוא, אלא שחוקים פדרליים מגנים על מידע כזה בתחומים מסוימים – לדוגמה, בפיננסים, במוסדות חינוך, בבריאות ועוד. לצד אלה קיימים חוקים במדינות השונות המרכיבות את ארצות-הברית.

בקרב דיני פרטיות והגנה על מידע, ה-GDPR הוא ה'סמן הימני' והוא נחשב המודרני שבדינים. לאחר שהתקבל כבר יש מדינות ברחבי תבל המתאימות את דיניהן לאמות-המידה שלו ומחוקקות GDPR-מקומי. כאלה הן ברזיל, ארגנטינה וויטנאם לדוגמה. אפילו קליפורניה שבארצות-הברית חוקקה חוק, שייכנס לתוקף ב-2020, ושזכה, בצדק או שלא, להיות מתואר כמיני-GDPR.

מדריך קצר זה מיועד לתת מושג ראשוני אודות ה-GDPR. הוא יאפשר לכם להתאים מראש את מתווה המחקר להוראותיו העיקריות, כך שיגדל הסיכוי לתשובה חיובית ומהירה לבקשות למענקי מחקר מאירופה והדרך לשיתופי פעולה מחקריים חוצי-יבשות תהיה קלה יותר.

על מה ה-GDPR חל?

ה-GDPR חל על "עיבוד" של "מידע אישי". שני המונחים מוגדרים בשפה מאד רחבה –

- "עיבוד" הוא כל פעולה המבוצעת על מידע אישי, לא רק באמצעות מחשב, לרבות איסוף המידע, שמירתו, אירגונו, הבנייתו, איחסונו, שינויו או התאמתו, איחזורו, השימוש בו, העברתו הלאה, הפצתו וגם מחיקתו או השמדתו. נכון לומר שאין פעולה שאנו מעלים בדעת באופן אינסטינקטיבי שהיא בגדר "עיבוד" שלא נופלת בתחומי ההגדרה;

- מידע אישי אינו רק מידע על אדם מזוהה (לדוגמה, על ריקרדו גונזלס מרחוב כך וכך מספר זה וזה בעיר קורדובה), אלא גם על מי שאפשר לזהותו. האפשרות לזהות אדם נגזרת ממידע היקפי – לדוגמה, כתובתו או מיקומו, מאפיינים כלכליים, תרבותיים או חברתיים שלו, וכמובן מידע גנטי או ביומטרי. לכן, העובדה שהמחקר שלך אוסף מידע ואינו משייך אותו לשם מוגדר או למזהה מובהק כמו תעודת זהות, אין פירושה של דבר שאינך אוסף ומעבר "מידע אישי".

אני פועל בישראל, מה לי ול-GDPR?

ה-GDPR יכול לחול על מי שיש לו התארגנות (establishment) בתחומי האיחוד האירופי, בקשר עם פעילות עיבוד המידע האישי הקשורים בה, בין אם הם מבוצעים באירופה ובין אם מחוצה לה. לכן, חוקר אירופאי המשתף מידע עם חוקר ישראלי, כפוף להוראות ה-GDPR. מכוחו, עליו לעורר דרישות מסוימות מול עמיתו הישראלי, שביטוין בין השאר בהתקשרות הסכמית נאותה.

אבל, וכאן החידוש, ה-GDPR יכול לחול גם על מי שמחוץ לתחומי האיחוד בכל אחד מהמצבים הבאים –

- אם ארגון שמחוץ לאיחוד האירופי מציע "מוצרים ושירותים" ליחידים בתחומי האיחוד. אכן, זו לשון הפונה קודם כל לפעילותן של חברות מסחריות, אבל מחקרים מסוימים, בפרט בתחומי מדעי החברה, עלולים להחשב כבאים בגדרה;

- אם ארגון שמחוץ לאיחוד האירופי מנטר התנהגות של יחידים בתחומי האיחוד. לשון זו מופנית לניטור מקוון, המאפיין ניסויים מסוימים במדעי החברה, אבל גם לניטור בריאותי ואחר, היכול להיות כרוך במחקרים שבתחומי הרפואה ומדעי החיים. טול לדוגמה מחקר המערב יחידים באירופה ובוחן את האופן שבו תרופות או אוכלוסיית חיידקים משליכים על בריאותם או התנהגותם;

- ה-European Research Council (ה-ERC), המקצה מענקי מחקר מכוח תוכנית Horizon 2020 של האיחוד האירופי, דורשת עמידה בכללי אתיקה. בכללים אלה יש פרק הנוגע לעיבוד מידע אישי, והוא כולל חלק מדרישות ה-GDPR. לכן מי שפונה לקבל מענק מה-ERC צריך להיות מוכן לדרישה לציית להוראות הלקוחות מה-GDPR אפילו מחקרו לא מערב כלל מידע אישי אודות יחידים באירופה;

- כאשר מידע אישי מועבר ממי שמחזיק בו באירופה לגורם אחר (בין אם באירופה ובין אם מחוצה לה), נדרשת התקשרות חוזית מתאימה בין הצדדים. טיבה של ההתקשרות נגזר מהזיקה של כל צד למידע. ההתקשרות מכילה את הוראות ה-GDPR לא במישרין אלא דרך ההסכם;

כל עיבוד מידע מחיל עלי את ה-GDPR?

ה-GDPR מכיר בשתי זיקות למידע אישי. כל אחת מהן גוררת אחריה התחייבויות אחרות –

- Controller – הוא המקבילה הישראלית לבעל מאגר המידע. הקונטרולר הוא מי שקובע מהן המטרות של עיבוד המידע ומהם האמצעים שישמשו לכך. אגב כך הקונרטולר מחליט למי יועבר המידע, כמה זמן יאוחסן, היכן יישמר ויעובד וכו'. כל החובות וההוראות של ה-GDPR חלות על קונטרולר. מוסד אקדמאי האוסף מידע על יחידים באירופה לצרכי מחקר, יכול להיחשב בנסיבות המתאימות לקונטרולר.

- ה-GDPR מכיר במי שהם בעלי השליטה במידע במשותף עם אחרים, Joint Controllers. לדוגמה, אם חוקר אירופאי מעביר לעמיתו הישראלי נתונים אישיים במטרה ששניהם יחקרו אותם, זיקתם המשותפת למידע היא כזו של Joint Controllers.

- Processor – הוא מי שרק מספק שירותי עיבוד מידע, בהתאם להוראות והנחיות ה-Controller. ה-GDPR יכול על פרוסור מכוח הוראות חוזיות של הקונטרולר. הוראות מסוימות ב-GDPR, כמו החובה לאבטח מידע או לשתף פעולה עם הרשויות האירופאיות להגנת הפרטיות, חלות על הפרוסור במישרין. מעבדה המספקת שירותי ניתוח למידע שנאסף באירופה היא באופן מובהק פרוסור.

מה ה-GDPR מחייב אותי לעשות במידע שאספתי למחקר?

ה-GDPR מטיל שורה ארוכה של חיובים על מי שמעבד מידע אישי. אלה העיקריים שבהם –

- עליו לעבד את המידע באופן **חוקי, הוגן ושקוף**. לכל אחד מאלה יש סבר. "חוקי" פירושו שעיבוד המידע מעוגן באחת משש עילות מוכרות ב-GDPR ובהן הסכמת האדם שאודות מעובד המידע ("נושא המידע"), קיום חוזה, מימוש אינטרס חיוני של נושא המידע, אינטרס לגיטימי של הקונטרולר ועוד. "הוגן" פירושו שיינתנו לנושא המידע כל זכויותיו לפי ה-GDPR (לפירוט הזכויות ראו בהמשך) ו"שקוף" פירושו שתימסר לו בלשון פשוטה וברורה הודעה שנושאיה מוכתבים ב-GDPR.

- המידע ייאסף רק ל**מטרה מוגדרת ומפורשת**. כלומר, אי אפשר לאסוף מידע "לכל מטרה חוקית". דוגמה למטרה מוגדרת – "המידע נאסף לצורך מחקר על האינטרקציה בין אדם למכונה בנסיבות האלה והאלה". אגב, בעניינים אלה יש הקלות לעיבוד-נוסף לצרכי מחקר (ראו בהמשך);

- המידע שיאסף יהיה **המינימום החיוני** למטרת עיבוד המידע – במילים אחרות, יש להגדיר מהו מינימום המידע הנחוץ לך, שבלעדיו תסוכל מטרת האיסוף, ואז לאסוף רק אותו;

- המידע יהיה **מדויק** וכשזה הדבר נחוץ יישמר מעודכן;

- המידע יישמר רק ל**משך הזמן המינימלי** הדרוש למימוש הסיבות שלשמן נאסף ולא מעבר לזה. שוב, יש הקלות למחקר (בהמשך...);

- המידע יעובד באופן **מאובטח**. זהו עיקרון חשוב. במילים פשוטות - אי-אפשר לשמור מידע אישי בגיליון אלקטרוני על גבי מחשב אישי לא מאובטח.

מה הזכויות של מי שהמידע אודותם נאסף?

זכויות נושא המידע (data subject) הן בליבת ה-GDPR. הוא מתייחס אליהן בקפדנות גדולה. הא ראיה היא שהקנסות הכבדים ביותר מוטלים בו על מי שלא מכבד את זכויות נושאי המידע – עד 4% ממחזור ההכנסות הגלובלי של האירגון או 20,000,000 אירו, לפי הגבוה מבין השניים!

ואלה הזכויות –

- **זכות הגישה.** כל נושא-מידע זכאי לגשת למידע האישי שמעובד אודותיו. הוא גם זכאי לקבל מידע נוסף כמו מטרות עיבוד המידע, מי מקבל את המידע אודותיו, מהם מקורות המידע ועוד.
- **זכות התיקון**. הזכות לתקן מידע שגוי ולהשלים מידע חסר.
- **הזכות להישכח**. לכל נושא-מידע יש זכות לדרוש כי המידע אודותיו יימחק. למעשה, יש חובה למחוק באופן יזום מידע כאשר הוא אינו דרוש עוד למימוש המטרה שלשמה נאסף מלכתחילה, נושא-המידע חזר בו מהסכמתו לעיבוד המידע ואין עוד בסיס חוקי אחר לעיבודו, המידע עובד באופן בלתי חוקי ועוד. הזכות להישכח אינה מוחלטת. יש לה סייגים, ופירושם שהזכות למחיקת מידע ניגפת מפני הנסיבות הבאות – חופש הביטוי וההבעה (לדוגמה, כלי תקשורת יכול להימנע ממחיקה מכוח עקרון זה), כדי לציית לדרישת החוק באחת ממדינות האיחוד האירופאי (לדוגמה, דינים העוסקים במחקר רפואי יכולים לחייב שמירת מידע אף ל- 35 שנים), בריאות הציבור, שימור המידע לצרכי ארכיונים, מחקר מדעי או היסטורי או סטטיסטיקה וכן לשם התגוננות מפני תביעה משפטית (כך, לדוגמה, אפשר להצדיק שמירת מידע מסוים כל עוד לא חלפה תקופת ההתיישנות בחוק מפני תביעה).
- **הזכות להגבלה**. נושא-המידע זכאי להגביל את עיבוד המידע כשהמידע האישי אינו מדויק, עיבודו הוא בלתי חוקי, הוא אינו דרוש עוד למטרתו ועוד. הגבלה כזו פירושה שהמידע רק יישמר ולא ניתן לעבד אותו הלאה בלא הסכמת נושא-המידע או אם נדרש הדבר להליך משפטי.
- **זכות הניידות**. נושא-המידע רשאי לדרוש שהמידע אודותיו ייוצא לתבנית שגורה בתעשיית המידע כך שאפשר יהיה להעבירו לצד שלישי. זוהי זכות חדשנית שאינה מוכרת, לדוגמה, לפי דיני ישראל.
- **הזכות להתנגד** מסיבות אישיות לעיבוד מידע שבסיסו החוקי נעוץ באינטרס הציבורי או באינטרס הלגיטימי של מעבד המידע או צד שלישי.
- **הזכות להימנע מקבלת החלטות אוטומטיות** שיש להן השלכה משפטית על נושא המידע (לדוגמה, קבלת החלטות המבוססת על יצירת פרופיל לאדם. אבל יצירת פרופיל לצרכי מחקר שאינה משליכה על זכויותיו של אדם לא כפופה לכלל זה).

איזו הודעה עלי לתת על הזכויות הללו?

ה-GDPR מקפיד מאד בדרישה לתת הודעה לנושאי המידע. הוא עושה כן מפני שהוא מבקש לקדם שקיפות והגינות בעיבוד המידע. את ההודעה יש לתת למי שמבקשים ממנו את המידע, כאשר פונים אליו בבקשה לקבל מידע – ולמי שהמידע אודותיו התקבל מצד שלישי, לכל המאוחר בתוך חודש מרגע שהתקבל.
התקנות מפרטות נושאים רבים שיש לכלול בהודעה. את ההודעה יש לתת בשפה תמציתית, פשוטה, ברורה ומובנת. הנה כמה מהנושאים שיש לכלול בה –

- מי אוסף את המידע ומה פרטי הקשר עימו;
- מה פרטי הקשר של הממונה על הגנת המידע (Data Protection Officer), אם מונה כזה לפי דרישות ה-GDPR או באופן וולונטרי;
- לאיזה מטרות ישמש המידע ומה הבסיס החוקי לשימוש בו;
- מי יקבל את המידע, או קטגוריות של צדדים שלישיים שיקבלו את המידע;
- האם המידע יועבר למדינה שלישית, ומה הבסיס החוקי לזה. כפי שנראה, ה-GDPR מגביל העברות מידע כאלה;
- לכמה זמן יישמר המידע;
- זכויות נושאי המידע לפי ה-GDPR, כולל – אם הבסיס החוקי לעיבוד המידע מתבסס על הסכמה – הזכות של נושא המידע לחזור בו מהסכמה כזו;
- הזכות להגיש תלונה בעניין עיבוד המידע לרשות הממונה על הגנת הפרטיות;
- האם מסירת המידע מחויבת לפי חוק או חוזה ומה התוצאות האפשריות של אי-מסירת המידע;
- האם המידע ישמש בתהליכים אוטומטיים לקבלת החלטות העשויים להשפיע על זכויות נושא-המידע;
- אם המידע לא הגיע במישרין מנושא המידע, מה מקור המידע.

יש מידע שאסור לי לעבד?

כן. ה-GDPR קובע כלל מאד קיצוני שיש לו השלכות מובהקות על מחקר אקדמאי: אסור לעבד מידע אישי על מקור אתני, דעות פוליטיות, אמונות דתיות או פילוסופיות, חברות באיגודים מקצועיים. כיוצא בזה אסור לעבד מידע גנטי או ביומטרי כדי לזהות אדם. אסור לעבד מידע בבריאותי או מידע אודות חיי המין או הנטייה המינית של אדם. חד וחלק. כל אלה נחשבים "קטגוריות מיוחדות של מידע".

אבל. ביחד עם זה שהוא קובע שאסור לעבד את המידע מהסוגים הרגישים הללו, ה-GDPR מוסיף ומורה באילו נסיבות אפשר יהיה בכל זאת לאסוף ולעבד מידע כזה. אלה חלק מהנסיבות שיכולות להיות רלבנטיות במיוחד למחקר –

- אם התקבלה הסכמת נושא-המידע – כלומר, אם המשתתף במחקר נתן הסכמתו לאיסוף. ה-GDPR, עוד נראה, מקפיד מאד ביחס לאופן שבו יש לקבל הסכמה. באותה נשימה שהוא מתיר לקבל הסכמה מנושא המחקר, ה-GDPR קובע שהמדינות החברות באיחוד האירופי רשאיות לסייג את ההסכמה.

- המידע המעובד פורסם בפומבי באופן מוצהר. כך, לדוגמה, אפשר לבצע מחקר המסתמך על מידע בפרופילים ציבוריים ברשתות חברתיות, שאינם חסומים רק לחבריו של המפרסם;

- עיבוד המידע נחוץ מסיבות של אינטרסים ציבוריים מהותיים, שהחוק במדינות החברות באיחוד האירופי הכיר בהם. שימו לב שכדי להסתמך על אפשרות זו צריך לוודא, כמובן, מה קובע החוק במדינה הרלבנטית: בהחלט ייתכן שהחוק בצרפת, לדוגמה, יקבע הוראות שונות מהחוק ביוון, למשל;

- עיבוד מידע הנחוץ מסיבות של בריאות הציבור;

- עיבוד מידע לצרכים ארכיוניים שהם בגדר האינטרס הציבורי, מחקר מדעי או היסטורי, העולה בקנה אחד עם הוראות ב-GDPR או בדיני המדינות החברות באיחוד האירופי, הוא פרופורציונלי למטרתו, מכבד את הזכויות להגנה על מידע ונוקט אמצעים לאבטחת זכויותיהם של נושאי המידע והאינטרסים שלהם.

אם אחד הצידוקים הללו מתקיים, די בו. אין צורך למצוא בסיס אחר לעיבוד המידע הרגיש. עם זאת, השאלה אם מתקיים צידוק כזה היא מורכבת. התיאורים שסיפקנו פה להוראות ה-GDPR הם פשטניים במידת מה. לכן, אם המחקר שאתם עורכים מערב אחד מסוגי המידע הרגישים והוא נעשה בזיקה לאירופה, חובה להיוועץ ברשות המחקר או בייעוץ המשפטי של האוניברסיטה כדי להבין אם יש לו בסיס לפי ה-GDPR.

אני יכול לאסוף כל מידע לכל מטרה מחקרית?

בעיקרון, כל עוד מצייתים לאמות המידע שלמעלה – הווה אומר, נמצא בסיס חוקי לאיסוף המידע, העיבוד הוא הוגן ושקוף, המטרה מוגדרת וכיו"ב וכמובן אי איסור על עיבוד המידע – ה-GDPR כשלעצמו לא מגביל מטרות מחקר.

אבל ה-GDPR לא נותן לך כרטיס חופשי לאסוף כל מידע שהוא. הוא דורש להטמיע בתהליכי עיבוד המידע שני עקרונות חשובים. הראשון קרוי "פרטיות כברירת מחדל" (Privacy by Default) והשני "עיצוב לפרטיות" (Privacy by Design) –

- פרטיות כברירת מחדל משמעה שיש לעולם להעדיף את החלופה המגינה על הפרטיות ככל הניתן;
- עיצוב לפרטיות פירושו שעליך להטמיע שיקולים של הגנת פרטיות והגנת המידע כבר משלב התכנון הראשוני של המערכת.

שני העקרונות האלה מתמצים בעקרון אחד – **אסוף את מינימום המידע האישי הדרוש לך למטרתך**.

הנה דוגמה ליישום העקרונות הללו מחיי המעשה: מחקר אוניברסיטאי מבקש לבחון את האופן שבו אינטרקציה עם משתמשי אתר אינטרנט משפיעה על נכונותם למסור מידע אישי. המחקר מחייב אפוא להפנות שאלות אישיות למשתמשי אתר אינטרנט ייעודי. בשלב עיצוב המחקר הבינו החוקרים כי תוכן התשובה לא מעניין אותם כלל ועיקר. מעניינת רק הנכונות להשיב. אשר על כן עיצבו את המערכת כך שלא תעביר אליהם את תשובת המשתמשים אלא רק חיווי אם המשתמש ענה או לא ענה על השאלה האישית.

אין ב-GDPR הקלות למחקר? הרי יש לו חשיבות ציבורית

התקנות האירופאיות מזכות את המחקר המדעי וההיסטורי ביחס של כבוד. הוא זוכה להקלות שונות. אלה הן

- אחד מכללי היסוד ב-GDPR הוא שמידע ייאסף רק למטרה מפורשת, מוגדרת ולגיטימית. אסור לעבד אותו באופן החורג ממטרות אלה. אבל עיבוד מידע לצרכים של מחקר מדעי או היסטורי או למטרות סטטיסטיקה לא ייחשב לבלתי-תואם את המטרה הראשונית שלשמה הוא נאסף. אין פירושו של דבר שעיבוד כזה חופשי מכל שאר הדרישות – לדוגמה, שיימצא לו בסיס חוקי, שינתן בגינו מידע ההולם את דרישת השקיפות ושיכובדו שאר זכויות נושאי המידע – אלא שמהדרישה לתאימות בין מטרת איסוף המידע האישי מלכתחילה לבין מטרות עיבוד המידע, מחקר זוכה להקלה מסוימת.

- בעוד שהכלל הוא שאסור לעבד קטגוריות מיוחדות של מידע, שהן בגדר מידע רגיש, עיבוד מידע כזה לצרכי מחקר מדעי או היסטורי, מותר אם הוא עולה בקנה אחד עם הוראות ב-GDPR או בדיני המדינות החברות באיחוד האירופי, הוא פרופורציונלי למטרתו, מכבד את הזכויות להגנה על מידע ונוקט אמצעים לאבטחת זכויותיהם של נושאי המידע והאינטרסים שלהם.

- על-פי ה-GDPR יש לתת לנושאי-המידע הודעה מאד מפורטת באשר לעיבוד המידע. הודעה כזו מממשת את עקרון השקיפות בתקנות האירופאיות. אולם אם מתן הודעה כזו עלול לסכל או להכביד באופן בלתי סביר על מחקר מדעי או היסטורי, כמו גם על עיבוד מידע לצרכים סטטיסטיים, ה-GDPR מוכן לפטור מחובת ההודעה, בכפוף לנקיטת אמצעים להבטחת זכויותיהם וחירויותיהם של נושאי המידע (ראו בהמשך).

- 'הזכות להישכח', שמכוחה יכול אדם לדרוש כי המידע האישי אודותיו יימחק כליל, לא תחול כשעיבוד המידע נעשה לצרכים ארכיוניים העולים בקנה אחד עם האינטרס הציבורי, לצרכי מחקר מדעי או היסטורי או לצרכי סטטיסטיקה אם מימוש הזכות עלול לסכל או לפגוע במטרות אלה באופן בלתי סביר.

- כאשר מידע מעובד לצרכי מחקר מדעי או היסטורי או לצרכים סטטיסטיים, המדינות החברות באיחוד האירופי רשאיות, בדיניהן הלאומיים, לסייג את זכויות נושאי המידע לגשת למידע, לדרוש את תיקונו, להגביל את עיבודו ולהתנגד לעתים לעיבוד המידע האישי אודותיהם – אם מימוש הזכויות הללו עלול לסכל את מטרות המחקר או לפגוע בהן.

- כיוצא בזה אפשר להגביל אותן זכויות ואף נוספות, כשמידע מעובד לצרכים ארכיוניים.

ויש גם הכבדות על מחקר?

ראשית, ה-GDPR מקנה ליחידים את הזכות להתנגד לעיבוד מידע אישי שלהם לצרכי מחקר מדעי או היסטורי או לצרכים סטטיסטיים. סיבת ההתנגדות צריכה להיות נעוצה במצבם האישי של אותם מתנגדים. והסייג היחיד להתנגדות הוא שאם עיבוד המידע מתבצע למען אינטרסים ציבוריים, ההתנגדות תינגף מפני העניין הכללי.

שנית, וזה העיקר - אם נפתח פתח בדמות הקלות למחקר, ה-GDPR רוצה להבטיח שהן לא ינוצלו לרעה ושהפגיעה בזכויות נושאי המידע לא תהיה גדולה מהנדרש. לכן הוא מציב בפני החוקר את הדרישות הבאות, שמרבית ההקלות מפנות אליהן במפורש –

עיבוד מידע אישי לצורך מחקר מדעי או היסטורי או למטרות סטטיסטיקה, יהיה כפוף להגנה נאותה על זכויותיהם וחירויותיהם של נושאי המידע. לשם כך יש להבטיח קיומם של אמצעים טכניים וארגוניים מתאימים. בפרט, יש למזער את היקף המידע הנאסף (data minimization), להשתמש בפסאודונימיזציה (תהליך שבו לא ניתן עוד לקשר בין אדם לבין המידע אודותיו, אלא באמצעות מידע נוסף שנמצא במקור אחר. לדוגמה, שימוש בשמות בדויים או במספרי זיהוי אקראיים במקום בשמותיהם האמיתיים של נושאי-המידע), וככל שאפשר – לעבד מידע באופן שלגמרי אינו מאפשר את זיהוי נושאי המידע.

עצה מעשית: בכל מחקר המערב יחידים בשר ודם, שאלו את עצמכם האם אתם חייבים לשמור את שמותיהם ומידע מזהה אחר; במידה שכן – האם אתם יכולים להפריד בין המידע המזהה לבין המידע שנאסף במסגרת המחקר ולהסתפק בבסיס-הנתונים המחקרי בזיהוי אקראי כלשהו שאינו מאפשר חזרה אל האדם בשר-ודם שממנו נאסף המידע; בחנו וראו האם כל פריט מידע שאתם אוספים הוא באמת חיוני למחקר או שאתם יכולים לוותר על חלק מהפרטים ואף רובם. כן, אנו יודעים – כיבוד הפרטיות בכלל והוראות ה-GDPR בפרט מחייב שינוי בהרגלים מושרשים היטב והדבר עלול להיתפס כהכבדה: אבל כך מורה החוק, והמטרה, בסופו של דבר, היא רצויה. גם אנו רוצים שיכבדו את פרטיותנו באופן שבו אנו נדרשים לכבד את פרטיותם של אחרים.

מה בעצם ייחשב ל"מחקר"?

ה-GDPR אמנם אינו מגדיר מהו ה"מחקר" הזכאי להקלות הללו, אבל הוא אומר במבוא לו, ש"עיבוד מידע אישי למטרות מחקר מדעי יש לפרש באופן רחב לרבות, לדוגמה... מחקר בסיסי, מחקר יישומי ומחקר במימון פרטי... [וכן] מחקרים שיש בהם עניין ציבורי בתחום הבריאות". גם "מחקר סטטיסטי" הוא מאפיין בהרחבה כ"כל פעולה של איסוף ועיבור מידע אישי שהיא חיונית למחקרים סטטיסטים לצורך הפקת תוצאות סטטיסטיות".

מה עלי לעשות עם המידע בתום המחקר?

עקרון היסוד ב-GDPR אומר שאם חדלה המטרה שלשמה נאסף המידע, אינך יכול עוד לעבד אותו. למעשה, עליך למחוק אותו ביזמתך. במקום מחיקה גמורה, אפשר להפוך את המידע לאנונימי, כך שאי אפשר יהיה עוד לשייך אותו בשום צורה פנים ואופן לאדם מסוים. זו מטלה קשה, בפרט מפני שהנחיות רגולטוריות באירופה מפרשות אותה באופן מחמיר. עם זה, מי שעמד בה נחלץ ממלתעות ה-GDPR. מידע אנונימי לגמרי שוב אינו יכול להיחשב למידע אישי.

שתי הערות של הסתייגות מהכלל הגורף הזה –

- האחת, יש הסדרים שיבקשו כי תפרסם ברבים את המידע הגלמי ששימש למחקר;
- השניה, ראינו קודם שעיבוד מידע למטרות מחקר שהן שונות מהמטרות שלשמן נאסף המידע מלכתחילה, לא ייחשב לבלתי-תואם את המטרה הראשונית שלשמה הוא נאסף. לכן, אם בטרם חדלה המטרה שלשמה נאסף המידע מלכתחילה נמצאה לו מטרה מחקרית אחרת, הרי שבעקרון מותר להמשיך לעבדו לאותה מטרה.

האם אני יכול להעביר את המידע בחופשיות לכל חוקר אחר ברחבי תבל?

לא. ממש לא. ה-GDPR מסייג העברת מידע ממדינות האיחוד האירופי והוא אוסר להעבירו למדינה שאינה מקיימת רמה נאותה של הגנה על מידע אישי. פירושו של דבר שהעברת מידע לחוקרים ומרכזי מחקר באחת ממדינות האיחוד האירופי – מותרת; אבל העברתו מחוץ לתחומי אותן מדינות כפופה לכך שהן הוכרו כתואמות (Adequete) לדרישת התקנות האירופאיות. נכון לתחילת 2019, אלה המדינות שהוכרו כמקיימות רמה נאותה של הגנה על מידע אישי – אנדורה, ארגנטינה, קנדה, איי פארו, גורנסי, האי מאן, ג'רזי, ניו-זילנד, שוויץ, אורוגוואי ו... ישראל. ההכרה בכל המדינות הללו קדמה ל-GDPR אבל היא בתוקף גם כעת. עם זה היא נבחנת מחדש. החלטה צפויה עד 2020.

לארצות-הברית מעמד מיוחד. בגלל ההבדל התהומי בין דיני הגנת המידע באירופה לדינים בארצות הברית (ראו בקצרה במבוא למדריך זה), ארצות-הברית אינה מוכרת כתואמת לאירופה. כיצד יועבר אפוא מידע בין שתי כלכלות-הענק של העולם המערבי? נציבות הסחר הפדרלית בארצות-הברית והנציבות האירופאית גיבשו הסדר הידוע כ-Privacy Shield. הוא מאפשר לחברות להחיל על עצמן באופן וולונטרי את אמות המידע האירופאיות לעיבוד מידע אישי. אלפי חברות – ובהן מפורסמות כמייקרוסופט, גוגל, אמאזון ופייסבוק – הצטרפו להסדר והעברת המידע אליהן מותרת מכוחו. לכן, חוקר המבקש, לדוגמה, לאחסן מידע בשירותי ענן של חברה אמריקאית, ייטיב לעשות תחילה אם יבדוק באתר האינטרנט של ה-Privacy Shield האם אותה חברה קיבלה על עצמה את הוראות ההסדר. אם לאו, יימנע מהעברת מידע לשרתיה שבארצות-הברית.

ומה אם אני רוצה להעביר מידע למדינה מחוץ לאיחוד האירופי שלא הוכרה כתואמת?

יש דרכים לעשות זאת. הן מורכבות יותר. חלקן מחייבות התקשרות בהסכמים מיוחדים עם מקבל המידע. אחרות נשענות על היתרים פרטיקולריים ב-GDPR. חסרונם העיקרי שאי אפשר להסתמך על היתרים אלה באופן גורף ושיטתי. בכל מקרה שרצונך לשתף חוקר ממדינה אחרת במידע אישי שאספת במחקרך והוא כפוף ל-GDPR, פנה לרשות המחקר באוניברסיטה לקבלת ייעוץ והכוונה.

מה זו 'אבטחת מידע' ולמה אני צריך לטרוח בה?

אחת משש החובות העיקריות לפי ה-GDPR היא החובה לאבטח מידע אישי. היא כה חשובה, החובה הזו, שהיא חלה גם על Controller וגם על Processor. היינו שמחים לתאר רשימה מוגדרת של דרישות שה-GDPR קובע, אבל הוא חכם מזה. ה-GDPR יודע שהטכנולוגיה והאמצעים לאבטחת מידע משתנים במהירות שבה מתפתחים האיומים על מידע אישי. לכן דרישותיו לאבטחה הן מעורפלות – בהתחשב בטכנולוגיות החדשניות, בהוצאות היישום, בהיקף עיבוד המידע ובסיכונים הנובעים ממנו לחירויותיהם של נושאי המידע, על הקונטרולר וגם על הפרוססור לנקוט אמצעי אבטחה הולמים. באופן פרטני, ה-GDPR מזכיר פסאודונימיזציה והצפנה של מידע אישי, אבטחת המשכיות עיבוד המידע (לדוגמה, היכולת להתמודד מפני התקפות מבחוץ או תקלות מבפנים), שיחזור זמינותו של המידע במקרה של כשל טכני או פיזי ובדיקה מתמדת של יעילות מערכות ההגנה.

הדרישות הללו הן מעבר למה שאפשר מחוקר בודד ליישם. אבל נגזר מהן שחוקר לא יכול עוד להסתמך במחקר המערב מידע אישי על מחשב פרטי, Laptop, שבו הוא מחזיק מידע לא מוגן, לדוגמה בגיליונות אלקטרוניים. אנו באוניברסיטה מקיימים מערכות מתוחכמות שתפקידן לאפשר לחוקר לעבד את המידע הדרוש לו ולשמור עליו באופן מאובטח. לפרטים פנה [לממונה על אבטחת מידע](#).

מה לעשות אם פרצו לי למידע?

לא רק פריצה, כל שימוש בלתי מורשה במידע או ארוע אבטחה אחר – לדוגמה, אם מי שאינו בעל הרשאת גישה למידע צפה בו, או אם שיגרת את מאגר הנתונים בטעות למי שאינו אמור לקבל אותו, או אם מדיה המחזיקה את המאגר אבדה או הושמדה וכמובן אם האקר חדר למאגר והעתיק אותו – כל אלה עלולים לחייב בדיווח על פי ה-GDPR או על פי הדין בישראל. במקרה שנודע לך על אירוע מסוג זה, פנה בדחיפות לגורמים הבאים, מסור את כל המידע הנוגע בדבר ופעל לפי ההנחיות שתקבל.

- [ממונה הגנת הפרטיות](#) (DPO)
- [רשות המחקר – אייל שכטר](#)
- [מנהל תחום אבטחת מידע באוניברסיטה](#)

ואם לא אציית ל-GDPR, מה כבר יעשו לי?

ה-GDPR בא עם שוט משמעותי. יש בו מנגנון קנסות כבד. אלה עלולים להגיע ל- 4% מהמחזור השנתי של הגוף שנתפס בהפרה או 20,000,000 אירו, לפי הגבוה מבין השניים. נכון לשלהי 2018, עוד לא נצבר ניסיון מעשי עם קנסות אלה. בעוד שידם של הרגולטורים לא קלה על ההדק, הם ימצאו את המקרה המתאים להטיל בו קנסות. סכומם המדויק ייקבע משיקולים כדוגמת היקף ההפרה, עד כמה הם סבורים שהיתה התעלמות מכוונת מהוראות ה-GDPR, האם הקונטרולר או הפרוססור שיתפו פעולה עם רשויות הגנת הפרטיות ועוד.

אם אפנה לקבל מענק מחקר מהאיחוד האירופי, אילו מהוראות ה-GDPR יחולו עלי מכח כללי האתיקה של האיחוד?

גם בהעדר תחולה ישירה של ה- GDPR, יחולו עליך חלק מהוראות ה GDPR כפי שהן משתקפות בכללי האתיקה של האיחוד האירופי. כללי האתיקה חולקים את העקרונות הבסיסיים של ה-GDPR. אלה ההוראות המרכזיות של כללי האתיקה בהקשר זה:

- פרטיות כברירית מחדל ועיצוב לפרטיות.
- מזעור המידע הנאסף והעדפה של אנונימיזציה ופסאודונימיזציה של מידע כברירת מחדל.
- קבלת הסכמה מדעת כבסיס חוקי לאיסוף ועיבוד המידע
- אבטחת מידע
- התייחסות מיוחדת לכל אחד מאלה –

1. עיבוד "קטגוריות מיוחדות" של מידע (בין השאר, מידע על זהות אתנית, נטיה מינית, בריאות, ביומטריה וגנטיקה).
2. עיבוד מידע על ילדים.
3. העברת מידע אל מחוץ לאיחוד האירופי.
4. Profiling (מאפיין מחקרים במדעי החברה), ניטור שיטתי של יחידים בהיקף גדול ושיטות איסוף ועיבוד מידע פולשניות.

- מינוי DPO ועריכת DPIA (Data Protection Impact assessment) כאשר הדבר מתחייב על פי הוראות ה-GDPR, או לחילופין - כאשר אין חובה לפי ה-GDPR - מינוי מומחה/יועץ להגנת מידע ועריכת סקר סיכונים במקרים שבהם המחקר מעלה שאלות אתיות משמעותיות.

... וזה הכל?

לא. ממש לא. ה-GDPR הוא דבר חקיקה ארוך ומפורט. הוא מגובה בהנחיות של גופי הרגולציה באירופה וביחד כל אלה מחזיקים מאות רבות של עמודים. מה שסיפקנו פה זו רק טעימה, המיועדת להבהיר כמה מהסוגיות שאתם עשויים להתקל בהן במחקר ולאפשר לכם להיערך אליהן מראש.

למחקר המערב מידע אישי, שמראש שוקל שיקולים של הגנת המידע ולוקח בחשבון את ה-GDPR, יש יתרונות רבים: ביבוד החוק וזכויות משתתפי המחקר מעודד השתתפות כזו; הסיכויים לקבל מענקי מחקר אירופאים במהירות רבה יותר, משתפרים; הבירוקרטיה הבלתי נמנעת של עיסוק בהגנה על מידע אישי, מוסדרת ומובנת מלכתחילה ולפיכך דורשת משאבים פחותים-יותר ומפנה זמן לעריכת המחקר עצמו.

בכל מקרה של ספק או שאלה, פנו לאייל שכטר ברשות המחקר.