

מדריך הגנת הפרטיות לחוקרי אוניברסיטת תל-אביב –

החקיקה הישראלית

כל מחקר באוניברסיטה המערב איסוף ועיבוד מידע אישי כפוף בראש ובראשונה לחוק הישראלי. מעבר לדרישות החוק הישראלי, המחקר שלכם עשוי להיות כפוף גם לדינים נוספים. למשל, אם משתתפים במחקר תושבי מדינות אחרות, אם הוא כרוך בשיתוף פעולה עם חוקרים מחוץ לישראל, או מקבל מימון מגופים בינלאומיים כגון האיחוד האירופי. ראו בהקשר

זה [מדריך GDPR לחוקרי אוניברסיטת תל אביב](#).

חשוב לציין כי בנוסף לדרישות החוק (הישראלי, והזר במידה וחל), כל מחקר באוניברסיטה כפוף גם לכללי האתיקה ולנהלי האוניברסיטה, וחייב לקבל את אישורי האתיקה הנדרשים.

מדריך זה מיועד לתת לכם מושג כללי לגבי החוק בישראל בנוגע להגנה על פרטיות מידע אישי. הוא יאפשר לכם להתאים מראש את מתווה המחקר שלכם לדרישות החוק.

איך מוגנת הפרטיות בישראל?

הזכות לפרטיות מעוגנת בחוק יסוד: כבוד האדם וחירותו כזכות חוקתית. היא הוכרה בפסיקה כאחת מזכויות האדם המרכזיות. הזכות לפרטיות חלה על מידע אישי.

חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "החוק") והתקנות שנחקקו מכוחו מהווים את המסגרת הכללית המחייבת בכל הקשור להגנה על מידע אישי.

בנוסף, קיימים חוקים נוספים העוסקים בהגנת הפרטיות בתחומים פרטיקולריים, כגון חוק זכויות החולה, תשנ"ו-1996 וחוק מידע גנטי, תשס"א-2000. מחקרים המערבים איסוף מידע רפואי או גנטי יהיו כפופים גם לחוקים אלה.

רגע, אנחנו מדברים על הגנה על פרטיות או הגנה על מידע?

חוק הגנת הפרטיות עלול לבלבל מעט. הוא מתייחס הן להגנה על פרטיות קלאסית – והן להגנה על מידע אישי בסביבה ממוחשבת. והכי מטעה זה שפרטיות קלאסית מתקיימת גם בסביבה ממוחשבת ולכן צריך להתחשב בה גם שם.

הגנה על פרטיות קלאסית כוללת הוראות כגון איסור על התחקות אחרי אדם העלולה להטרידו, איסור על צילום ברשות היחיד או פרסום צילום ברבים בנסיבות העלולות להשפילו, שימוש בלתי מורשה בתוכן של כתב (כולל מסמכים אלקטרוניים), הפרה של חובות סודיות ועוד. כמובן שנסיבות כאלה יכולות בהחלט לגעת למחקרים. לדוגמה, מעקב אלקטרוני אחרי אדם הרווח במחקרים בתחומי מדעי החברה יכול להיחשב ל"התחקות אחרי אדם העלולה להטרידו"; שימוש

במידע שמסר אדם לצורך אחד (לדוגמה, למחקר שעניינו רפואי) למטרה שונה מזו המקורית (למחקר סוציולוגי או אנתרופולוגי), עלול להיחשב ל"שימוש בידעה על ענייני הפרטיים של אדם שלא למטרה שלשמה נמסרה" ועוד.

ההגנה על הפרטיות בסביבה ממוחשבת מתבטאת בחוק הגנת הפרטיות בשורה של הוראות המחייבות לרשום מאגרי מידע, לאבטח את המידע שבהם, לאפשר לנושאי המידע (מי שהמידע אודותם נשמר במאגר) לעיין במידע ולתקן אותו ועוד.

מה זה מידע אישי?

החוק מגדיר "מידע" כ- "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו". כלומר, לא כל "מידע" על אדם ייחשב כמידע אישי לצורך חוק הגנת הפרטיות.

החוק אף מגדיר "מידע רגיש" כ- "נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו", וכן מידע ששר המשפטים קבע בצו שהוא מידע רגיש. מעניין לשים לב מה קורה כשהגדרה של "מידע" ו"מידע רגיש" היא סגורה. מידעים מאד אינטימיים – לדוגמה, מידע ביומטרי או נתוני מיקום של אדם – לא ייחשבו כלל כ"מידע" לצרכי חוק הגנת הפרטיות בישראל. זה מאד שונה מהסדרים משפטיים מתקדמים יותר, כמו ה-GDPR באירופה, שבהם "מידע אישי" הוא כל מידע שאפשר לייחס לאדם מזוהה או בר-זיהוי.

כשהחוק מגן על מאגרי מידע – הוא מתכוון למאגרים שיש בהם "מידע" מהסוג הזה.

אבל כשהוא מגן על "פרטיות", מוטת הכנפיים שלו רחבה לאין ערוך. או אז החוק אינו עוצר בהגדרת "מידע". הוא מגדיר באופן כללי יותר פגיעה בפרטיות כשימוש בידיעה על ענייני הפרטיים של אדם או מסירתה לאחר, שלא למטרה לשמה נמסרה. הפסיקה פירשה את המונח "ידיעה על ענייני הפרטיים של אדם" בהרחבה וכללה בו כל מידע הקשור לחיי הפרטיים של אדם, לרבות פרטים טריוויאליים לגמרי כגון כתובת, מס' טלפון, מס' ת.ז., פרטי חשבון בנק וכן כתובת IP.

פועל יוצא מזה הוא ששימוש במידע מחקרי לצרכי מחקר-המשך, מחייב זהירות ושיקול דעת. כתב ההסכמה של משתתפים במחקר יכול להתיר זאת, אבל לא באופן בלתי מוגבל. משפט כדוגמת "מותר לכם להשתמש במידע אודותי לכל מטרה אחרת שתמצאו לנכון" עלול להיחשב לא תקף.

מתי מותר לי לאסוף מידע אישי למחקר?

החוק קובע עיקרון ברור: אין פוגעים בפרטיותו של אדם ללא הסכמתו. מכאן, שכאשר מבצעים פעולה שעלולה לפגוע בפרטיות, אפשר לבסס אותה רק על הסכמה (או על היתר בחוק אחר).

בהמשך לזה קובע החוק כי כאשר פונים לאדם בבקשה לכלול את פרטיו במאגר מידע, יש לתת לו הודעה האומרת אם הוא חייב למסור את המידע לפי חוק או שמסירתו תלויה בהסכמתו, מהן מטרות איסוף המידע ולמי המידע יועבר.

אז כיצד עלי לקבל הסכמה של משתתפי מחקר?

חוק הגנת הפרטיות דורש שההסכמה לפגיעה בפרטיות תהיה "הסכמה מדעת". הסכמה מדעת היא זו שניתנת לאחר שנמסרו לאדם כל הפרטים הדרושים לו באופן סביר כדי להחליט אם הוא מסכים לפגיעה או לא. ההסכמה לא צריכה להיות בכתב. לפי לשון החוק היא יכולה להיות גם משתמעת מהנסיבות. אבל הוודאות מחייבת לקבל הסכמה בכתב ובחתימת הנחקר. יהיה קשה להוכיח אחרת הסכמה מדעת, ולכן אנחנו ממליצים בכל פה להסתמך רק על הסכמה מתועדת וחתומה. הסכמה כזו צריך לנסח בשפה פשוטה וברורה. היא לא יכולה לכלול כל מיני "ו/או", ניסוחים מסורבלים או ביטויים עמומים אחרים.

פשוטה, ברורה ומוגדרת היטב. חשוב לזכור את זה.

מה הפרטים שעלי למסור לאדם כדי שייחשב כמי שהסכים מדעת לפגיעה בפרטיות?

הפרטים האלה כוללים בדרך כלל תשובות לכל אחת מהשאלות הבאות –

- מה המידע שתאספו?
- איך תאספו את המידע הזה? לדוגמה: האם כל המידע יימסר באופן פעיל על ידי המשתתף, למשל באמצעות שאלונים, או שחלק מהמידע ייאסף באופן סביל, למשל דרך נתונים שתפיקו ממערכות מחשב שהמשתתף משתמש בהן או תסיקו מניתוח מידע-עתק (Big Data Analysis)
- איך תשתמשו בפרטים הללו ולא יזו מטרות?
- למי תעבירו את הפרטים הללו, ומי ייחשף להם?
- כמה זמן תשמרו על המידע?
- האם הוא יישמר בישראל או במדינה אחרת? זו נקודה חשובה מפני שיש תקנות מכוח חוק הגנת הפרטיות שמגבילות העברת מידע אל מחוץ לתחומי המדינה. אחד החריגים להגבלה הזו מתקיים אם נושא המידע, מי שהמידע אודותיו נאסף, נתן את הסכמתו להעברה לחו"ל.
- מה הזכויות שיש לאדם בקשר לפרטים האלה?

וברגע שאדם הסכים, זה סופי?

כן ולא. כן, מפני שההסכמה מאפשרת גם לבצע מעשים שעלולים להיחשב לפגיעה בפרטיות – ולא, מפני שבתחום הגנת הפרטיות אדם יכול לחזור בו מהסכמתו בכל רגע. אם ביטל את ההסכמה, זה לא יהפוך את השימוש שכבר ביצעתם במידע לבלתי-חוקי, אבל אסור יהיה לכם להמשיך להשתמש בו באופן מזהה.

האם אוכל להשתמש במידע אם אהפוך אותו לאנונימי?

כן. אין פגיעה בפרטיות אם אי אפשר לשייך את המידע לאדם בשר ודם. לכן אם הצלחת 'להפשיט' את המידע מכל מה שיכול לקשר אותו לאדם, אתה חופשי להשתמש בו בלא המגבלות של חוק הגנת הפרטיות. אבל להסיר מהמידע כל נתון שיכול לקשר לאדם – זה מאד לא פשוט. אין צורך בשם ובכתובת כדי שאפשר יהיה לשייך מידע לאדם מסוים. לדוגמה, במדינת וושינגטון בארה"ב מתפרסמות רשומות רפואיות בלא פרטיות של החולים. חוקרים הצליחו לשייך את המידע לחולים מזוהים באמצעים פשוטים, כמו הצלבה בין הרשומות שפורסמו לידיעות בתקשורת על תאונות שהתרחשו. במקרה אחר, חוקרי אבטחה הצליחו לזהות משתמשים בבסיס נתונים אנונימי-כביכול שפרסמה נטפליקס, דרך הצלבתו עם ביקורות שפרסמו גולשים באתר הסרטים הידוע IMDB – ודרך המידע הזה גם חשפו נטיה פוליטית ומינית...

הנה דוגמה למידע אנונימי: במחקר אחד שאנו עורכים באוניברסיטת תל-אביב, מתבקשים נחקרים להשיב על שאלות מקוונות. את הנחקרים מגייסת החוקרת באמצעות שירות כדוגמת Amazon Turk המאפשר לאנשים לבצע מטלות פשוטות בתמורה זעומה. החוקרת הבינה מלכתחילה שלמחקר המסוים הזה אינה צריכה לדעת את פרטי המשתמשים וגם לא את תוכן תשובותיהם, אלא רק אם השיבו לשאלות. לכן היא שומרת אך ורק מספר אקראי של כל משתמש וחיווי ב"כן/לא" המסמל אם השיב לשאלות המחקר או לא. מידע כזה הוא אנונימי.

ובמידע אנונימי – אבל באמת אנונימי! – אפשר לעשות הכל, בלי הגבלה.

אם אני אוסף מידע שאינו פוגע בפרטיות, אני לא צריך לקבל

הסכמה?

החוק מחייב כל מבקש מידע לתת הודעה למי שהמידע אודותיו נאסף, כאשר פונים אליו בבקשה לקבלת מידע. המשמעות היא שגם אם המידע שאתה אוסף הוא טריוויאלי ואין בו פגיעה בפרטיות, כל עוד הוא "מידע" בהגדרתו בחוק – אתה נדרש למסור למשתתף במחקר הודעה מתאימה על איסופו.

ההודעה צריכה לכלול את הנושאים הבאים:

1. המטרה לשמה נאסף המידע.
2. למי יימסר המידע ומטרות המסירה.
3. האם חלה על אותו אדם חובה חוקית למסור את המידע או שמסירת המידע תלויה ברצונו ובהסכמתו.

החוק לא דורש הסכמה לאחר ההודעה. הוא מניח שאם מסרת הודעה והאדם נתן לך את המידע לאחריה, הוא הסכים במשתמע לתוכן ההודעה. אבל כמו במקרה של הסכמה מדעת, ההודעה צריכה להיות מנוסחת בשפה ברורה ומובנת לכל.

מה הזכויות של מי שהמידע אודותיו נאסף?

זכות העיון - כל אדם זכאי לעיין במידע שנאסף עליו.

כל משתתף במחקר יכול לפנות אליך בבקשה לממש את זכותו לעיין במידע שנאסף אודותיו ועליך לאפשר לו עיון במידע. בתקנות המסדירות את התנאים לעיון במידע נקבע כי העיון ייערך במקום שבו נמצא המאגר, אך בהנחיה שפרסמה הרשות להגנת הפרטיות נקבע כי במציאות הטכנולוגית של ימינו, ככל שמדובר במידע ששמור באמצעים דיגיטליים, יש לאפשר את זכות העיון באמצעות משלוח קובץ דיגיטלי הניתן לקריאה, שמיעה או צפייה, בהתאם לאופן שמירת המידע במקור. יש להקפיד כי מתן זכות העיון בדרך זו ייעשה תוך נקיטת אמצעים נאותים לזיהוי המבקש ולאבטחת המידע.

ההנחיה אף מבהירה כי זכות העיון במידע חלה גם כאשר המידע אינו שמור מלכתחילה באופן המקושר לאותו משתתף, אולם ניתן, במאמץ סביר, לקשר בין המידע לאותו משתתף. החוק מגדיר מספר חריגים לזכות העיון. אחד החריגים, שעשוי להיות רלוונטי גם למידע הנאסף במסגרת מחקר, מתייחס למידע רפואי או נפשי, אם לדעת בעל המאגר המידע עלול לגרום נזק חמור לבריאותו הגופנית או הנפשית של המבקש או לסכן את חייו. במקרה כזה המידע יימסר לרופא או לפסיכולוג מטעם המבקש.

זכות לתיקון ומחיקה – כל אדם זכאי לבקש לתקן או אף למחוק את המידע שנאסף עליו אם הוא שגוי, לא ברור או לא מעודכן. אם מידע תוקן או נמחק בעקבות בקשה של משתתף במחקר, עליך להודיע על התיקון או המחיקה לכל מי שקיבל ממך את המידע בשלוש השנים שקדמו לתיקון או למחיקה.

כבעל מאגר מידע, מה החובות שחלות עליך?

חובת רישום

החוק קובע כי יש לרשום מאגרי מידע במרשם מאגרי המידע. לא כל מאגר מידע חייב ברישום והחוק קובע אלו מאגרים חייבים ברישום.

מאגר שנתקיים לגביו אחד התנאים הבאים חייב ברישום:

1. המאגר כולל מידע על למעלה מ-10,000 אנשים.
2. המאגר מכיל מידע רגיש.
3. המאגר כולל מידע על אנשים והמידע לא נמסר על ידם, מטעמם או בהסכמתם.
4. המאגר הוא של גוף ציבורי.
5. המאגר משמש לשירותי דיוור ישיר כהגדרתם בחוק.

חובת סודיות

החוק קובע כי אדם שנחשף למידע אישי בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, לא יגלה מידע זה אלא לצורך ביצוע עבודתו, או אם נדרש לכך על פי צו בית משפט. חובת הסודיות חלה על כל מי שנחשף למידע האישי שנאסף במסגרת המחקר, מתוקף תפקידו.

חובת אבטחת מידע

בעל מאגר מידע אחראי לאבטחת המידע במאגר המידע.

כיצד עלי לאבטח את המידע?

תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, שנכנסו לתוקף בשנת 2018, מטילות חובות מפורטות באשר לנהלי אבטחת מידע במאגרי מידע. התקנות חלות על כל הבעלים, המנהלים והמחזיקים של מאגרי מידע בישראל.

"מאגר מידע" מוגדר בחוק כ-"אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט –

- אוסף לשימוש אישי שאינו למטרות עסק
- אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף.

המידע האישי הנאסף במסגרת מחקר מהווה מאגר מידע וחלות עליו כל החובות המפורטות בתקנות. הדרישות הללו הן מעבר למה שאפשר לדרוש 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.

למידע נוסף בעניין זה אנא פנה [למנהל תחום אבטחת מידע](#).

מה לעשות אם פרצו לי למידע?

לא רק פריצה, כל שימוש בלתי מורשה במידע או אירוע 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 הדין בישראל. השאלה אם יש או אין חובה כזו, מוכרעת לפי רמת אבטחת המידע שהמאגר חייב בה.

אם נודע לך על אירוע מסוג זה, פנה בדחיפות [למנהל תחום אבטחת מידע](#), מסור לו את כל המידע הנוגע בדבר ופעל לפי הנחיותיו.

האם אני יכול להעביר את המידע בחופשיות לכל חוקר אחר מחוץ לישראל?

לא.

תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה) תשס"א – 2001, אוסרות על העברת מידע ממאגר מידע בישראל למדינה אחרת, אלא אם כן המדינה שאליה מועבר המידע מבטיחה רמת הגנה על מידע שאינה נופלת מרמת ההגנה בישראל, ובמיוחד מקיימת את העקרונות הבאים:

1. מידע ייאסף ויעובד רק באופן חוקי והוגן.
 2. ייעשה שימוש במידע רק למטרה שלשמה נתקבל.
 3. מידע שייאסף יהיה מדויק ומעודכן.
 4. הבטחת הזכות לעיון ולתיקון למי שהמידע עליו נאסף.
 5. נקיטת אמצעים נאותים של אבטחת מידע.
- התקנות מאפשרות חריגים לאיסור, בתנאים מסוימים. מבין התנאים המפורטים בתקנות, הרלוונטיים ביותר להעברת מידע במסגרת מחקר הם:
1. אם ניתנה הסכמה של האדם אודותיו נאסף המידע. לכן, אם אתה יודע מראש שתצטרך להעביר את המידע, עליך לכלול הסכמה כזו בטופס שמאשר כל משתתף בחתימתו.
 2. אם בעל מאגר המידע במדינה שאליה מועבר המידע התחייב בהסכם לקיים את התנאים החלים על מאגר מידע בישראל.
 3. המידע מועבר למדינה שהיא צד לאמנה האירופית להגנת הפרט בקשר לעיבוד אוטומטי של מידע רגיש. קישור לרשימת המדינות ניתן למצוא כאן.
 4. המידע מועבר למדינה בה קיים הסדר המאפשר קבלת מידע ממדינות האיחוד האירופי. למשל, בארה"ב, בה דיני הגנת המידע שונים לחלוטין מהדין האירופי, 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, אמזון ופייסבוק – הצטרפו להסדר והעברת המידע אליהן מותרת מכוחו.
- בנוסף, התקנות מתנות העברת מידע מחוץ לישראל בהתחייבות בכתב של מקבל המידע כי הוא נוקט אמצעים מספיקים להבטחת פרטיותם של מי שהמידע עליהם הועבר, וכי לא יעביר את המידע לצד שלישי.

האם חלות הוראות מיוחדות על איסוף מידע רפואי או מידע גנטי במסגרת מחקר?

כן. **חוק זכויות החולה, תשנ"ו-1996**, קובע הוראות באשר למסירת מידע רפואי:

"מידע רפואי" הוא מידע המתייחס באופן ישיר למצב בריאותו הגופני או הנפשי של מטופל או לטיפול הרפואי בו.

"מטופל" הוא חולה וכל המבקש או המקבל טיפול רפואי.

החוק מתנה העברת מידע רפואי לאחר בהסכמת המטופל למסירת המידע הרפואי אודותיו.

לצד זה החוק מפרט מספר מקרים בהם מסירת מידע מותרת ללא הסכמת המטופל. אחד המקרים מתייחס למסירת מידע למטרות פרסום בביטאון מדעי, למטרות מחקר או הוראה. החוק מתנה את מסירת המידע בכך שלא נחשפו בו פרטים מזהים של המטופל.

לכן, ככלל, מחקר קליני המערב איסוף מידע רפואי ממטופלים, מחייב הסכמה מפורשת של המטופל להעברת המידע לחוקר. החריג לכלל זה הוא מחקר שבו נאסף מידע רפואי אנונימי, כזה שלא ניתן לייחסו למטופל מסוים. בהקשר זה חשוב להבין שאם קיימת אפשרות לייחס את המידע למטופל מסוים באמצעות מידע אחר (למשל: רשימת קודים ולצדה פרטים אישיים), אין מדובר במידע אנונימי כי אם במידע מזהה הכפוף לדרישת ההסכמה.

חוק מידע גנטי, תשס"א-2000, מתנה איסוף דגימה גנטית למטרת מחקר בקבלת הסכמה מדעת, בכתב, לאחר מתן הסבר מפורט לנבדק. ההסבר יכלול גם פירוט של זכויות הנבדק:

- הזכות לקבל מידע על אופן ביצוע הבדיקה ומשמעות תוצאותיה לגבי הנבדק וקרובי משפחתו.
- הזכות להורות בכתב על מחיקת פרטים מזהים מהדגימה או מתוצאות הבדיקה.

מחקר שעושה שימוש בדגימות גנטיות בלתי מזהות פטור מהדרישות הללו. על פי החוק, דגימות גנטיות בלתי מזהות הן דגימות שלא מופיעות עליהן פרטים מזהים של הנבדק, או דגימות שהפרטים המזהים הופרדו מהן באופן שלא ניתן לחזור אליהם.

החוק מתיר למי שמחזיק במידע גנטי להעביר את המידע למטרת מחקר בתנאי שניתנה הסכמה מפורשת בכתב של הנבדק להעברת המידע. העברת מידע גנטי ללא כל פרט מזהה מותרת גם ללא הסכמה.

מידע רפואי ומידע גנטי מוגדרים כ"מידע רגיש", ומחקר העוסק באיסוף מידע כזה, כפוף לדרישות מחמירות יותר, הן באשר לאפשרות ולאופן איסוף המידע, והן באשר לרמת אבטחת המידע. לפיכך, בכל מחקר המערב איסוף מידע מסוג זה אנו ממליצים לפנות מראש [לאייל שכתר](#) ברשות המחקר על מנת לוודא כי המחקר עומד בכל דרישות החוק.

ואם לא אציית לחוק, מה יעשו לי?

חוק הגנת הפרטיות קובע כי פגיעה בפרטיות היא עוולה אזרחית - כלומר לנפגע תהיה עילת תביעה לפי פקודת הנזיקין. בנוסף, החוק מגדיר נסיבות מסוימות בהן פגיעה בפרטיות מהווה גם עבירה פלילית.

חשוב לדעת כי החוק מאפשר פסיקת פיצויים בסכום משמעותי גם ללא הוכחת נזק (עד כ-60,000 ₪ ואף כפול מכך, אם הוכח כי הפגיעה בפרטיות נעשתה בכוונה לפגוע. סכומים אלה מעודכנים בהתאם לעליית מדד המחירים לצרכן). בנוסף, לרשות להגנת הפרטיות יש סמכות להטיל קנסות מנהליים בסכום של בין 2,000 ל-5,000 ₪ בשל עבירות על חלק מסעיפי החוק (כגון: הפרת חובת רישום מאגר, שימוש במידע שלא למטרה לשמה נאסף, הפרת זכות העיון ועוד).

ולסיכום, עצה מעשית:

בכל מחקר המערב יחידים בשר ודם, שאלו את עצמכם האם אתם חייבים לשמור את שמוותיהם 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 מחייב שינוי בהרגלים מושרשים היטב והדבר עלול להיתפס כהכבדה: אבל כך מתחייב מהוראות החוק, והמטרה, בסופו של דבר, היא רצויה. גם אנו רוצים שיכבדו את פרטיותנו באופן שבו אנו נדרשים לכבד את פרטיותם של אחרים.

המידע המובא במדריך זה הינו כללי ואיננו ממצה. בכל מקרה של ספק או שאלה, פנו [לאייל שכטר](#) ברשות המחקר.