

תקנות העברת מידע לישראל

אייל שגיא | 7.5.23

AYR

Amar Reiter Jeanne Shochatovitch & Co

המצגת הינה כללית ולא מהווה תחליף
לייעוץ משפטי

רקע

- בחינה מחודשת של החלטת ה-adequacy לישראל
 - חוק מ 1981
 - תיקון 14 לא הספיק לעבור
 - תיקון 15 אפילו לא פורסם
- תקנות
 - שר המשפטים מתקין, וועדת חוקה מאשרת
 - ב-29.11.22 פורסמו להערות
 - ב-23.4.23 אושרו בוועדת חוקה, חוק ומשפט
- הועדה ביקשה תיקונים
 - בעיקר: תחולה על כל המידע במאגר, גם כזה שלא הגיע מאירופה
 - נוסח סופי עוד לא פורסם

טריגר תחולה

• "תקנות אלה יחולו על מידע המצוי במאגר מידע בישראל אשר הועבר מהאזור הכלכלי האירופי, ולמעט מידע שהעביר במישרין אדם על אודות עצמו"

• תחולה עצמאית מה-GDPR

• צריך לבדוק תחולה של כל דין בנפרד

• העברה למדינה adequate לא אומרת שה-GDPR לא חל

• רק שההעברה קלה

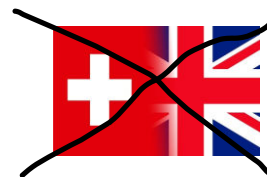
• חל גם על מידע של ישראלים

• "אזור כלכלי אירופי"

• EEA – כל ה-EU + נורבגיה, ליכטנשטיין ואיסלנד

• אבל לא שווייץ

• ולא בריטניה



העברות מאירופה לישראל

- מקונטרולר אירופי לבעל מאגר ישראלי
- סוכנות נסיעות אירופאית מעבירה הזמנות למלון ישראלי
- חברה בת אירופאית מעבירה מידע לחברה האם הישראלית
- למשל מידע על עובדים של חברה בת אירופית שעובר לחברה האם הישראלית
- מגיע מגוף אירופאי למחזיק (processor) ישראלי
- אין כמעט משמעות כי כל התקנות חלות על "בעל מאגר" ולא על מחזיק
- חוץ מתקנה 7 (התוספת למידע רגיש)
- קיום מידע רגיש במאגר מחייב רישום
- אבל מחזיקים לא רושמים

העברות מישראל לעיבוד באירופה ובחזרה

- מצד אחד, מלשון התקנות ומהדיון עולה שכן תהיה תחולה של התקנות במקרה כזה
- מצד שני, מידע זה פחות מעניין אירופאים:
- לפי ה EDPB שמידע שמגיע לעיבוד באירופה לא "נדבק" ב GDPR
- בלי adequacy, המידע חוזר למדינת המוצא תחת המודול הרביעי של ה SCC, שלעומת שאר המודולים:
- אינו מצריך בחינת TIA ו/או החלת safeguards נוספים על המידע
- מצריך חתימה על הסעיפים הכלליים של ה-SCC בלבד
- הדין החל יכול להיות לא אירופאי
- סעיף 15 ל SCC, שמדבר על הודעה למייצא המידע אודות בקשת גישה של רשויות למידע לא יחול גם כן

מידע שהעביר במישרין אדם על אודות עצמו

- לא נחשב מידע שמגיע מאירופה
- לדוגמא: לקוח ישראלי בטיול באירופה משתמש באפליקציה להזמין תור לרופא
- מידע שמועבר באמצעות מתווכים / רשתות
- אם הם controller התקנות כנראה חלות

אם חל, מתי חל ועל מה?

- מידע חדש מאירופה
- תוך שלושה חודשים
- מידע מאירופה שקיים במאגר לפני כניסת התקנות לתוקף
- תוך שנה
- מידע באותו מאגר עם מידע מאירופה
- החל מה 1.1.2025
- אפשר להפריד את המאגרים
- לא תמיד אפשרי מבחינה טכנית
- נושאי מידע ידרשו את הזכויות בכל מקרה
- תיקונים 14 ו 15 ידרשו אותו הדבר

מה הדרישות המהותיות?

- מוצא וחברות בארגון עובדים הם "מידע רגיש" (תקנה 7)
- אין משמעות למעט חובת רישום
- חובת דיוק (תקנה 5)
- **בעל מאגר** מידע יפעיל מנגנון ארגוני, טכנולוגי או אחר שמטרתו להבטיח כי המידע שבמאגר המידע נכון, שלם, ברור ומעודכן
 - נוהל זה מנגנון ארגוני
 - אם יש מידע לא נכון, שלם, ברור או מעודכן – יש לתקן או למחוק
 - מקביל לסעיף 14 לחוק (בלי חובה ליזום בדיקה עצמאית)
 - יש חובות סקטוריאליות מקבילות

יידוע (תקנה 6)

- **בעל מאגר** מידע שקיבל מידע אודות אדם (+ להעביר את המידע שקיבל לצד שלישי), יודיע לו, במישרין או בעקיפין באמצעות הגורם שממנו הועבר המידע מהאזור הכלכלי האירופי... תוך חודש ממועד קבלת המידע:
- זהות בעל מאגר המידע ומנהל המאגר, מענם ודרכי ההתקשרות עמם
- במקרה של העברה לצד שלישי: זהות ופרטי ההתקשרות של הצד שלישי או סוג הגורמים השלישיים אליהם יועבר המידע
- מטרת העברת המידע, סוג המידע שהועבר
- קיומן של זכויות: מחיקה (לפי תקנה 2), עיון (לפי סעיף 13 לחוק) וזכות לתיקון (לפי סעיף 14)
- לעומת סעיף 11 לחוק:
- הרחבת סוגי נושאי המידע שיש ליידע: מי שמסר מידע באופן ישיר + כל מי שהגיע אודותיו מידע
- הרחבת תחומי היידוע: חובה חוקית, מטרות, מסירה לאחר ולאיזה מטרות + מנהל מאגר ופרטי התקשרות (בGDPR: DPO), יידוע על זכות מחיקה, עיון ותיקון, וסוג המידע
- חריגים
- נושא המידע כבר יודע, הכבדה, סודיות, דין ספציפי אחר שמסדיר, פגיעה בגוף, בזכויות, בעיתונאות
- יישום
- במישרין (מדיניות פרטיות(?)) או בעקיפין דרך הגורם המעביר (הרבה פעמים חלק מהDPA)

הגבלת החזקת מידע עודף (תקנה 4)

- **בעל מאגר** מידע יפעיל מנגנון ארגוני, טכנולוגי או אחר, שמטרתו להבטיח כי במאגר המידע לא מוחזק מידע שאינו נחוץ עוד למטרה שלשמה נאסף או הוחזק או למטרה אחרת שלשמה מותר להחזיקו לפי כל דין... ימחק את המידע שאינו נחוץ במועד המוקדם האפשרי בנסיבות העניין
- תקנות אבטחת מידע 2(ג): "בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר"
- לא דורש מחיקה אבל תקנה 19(ב) דורשת לתעד את הבדיקה
- המשמעות היא תיעוד של הפרת התקנות
- למעשה דורש איתור בסיס חוקי כי בלעדיו המידע עודף
- גם לשמירה ארוכת טווח
- מנגנון
- ארגוני - נוהל
- לא פעם בשנה כמו ב 2(ג), אלא רציף
- טכנולוגי - למשל מערכות data life cycle management

חריגים למחיקה

- נותנים אינדיקציה גם לתקנה 2(ג) לתקנות אבטחת מידע
- התממה
- "יבצע פעולות המבטיחות שלא יתאפשר, באמצעים סבירים, לזהות את נושא המידע"
- צידוקים
- אם השימוש במידע הוא לצורך אחד מאלה, וזאת **בהיקף הנחוץ והמידתי** לאותו צורך
 - מימוש חופש הביטוי או זכות הציבור לדעת, הסכם בין-לאומי שישראל צד לו
 - ניהול הליך משפטי או גביית חובות
 - מניעת הונאה, גניבה, או מניעת פעולות אחרות שעלולות להשפיע על דיוק המידע או מהימנותו
 - להגנה על עניין ציבורי, **לרבות** למטרות ארכוב, מחקר מדעי או **מחקר** סטטיסטי...
- GDPR 17(3)(d): for archiving purposes in the public interest, scientific or **historical** research purposes or statistical purposes...

מחיקת מידע לפי דרישה (תקנה 3)

- **בעל מאגר** מידע ימחק מידע לבקשתו הכתובה של נושא המידע בהתקיים אחד מאלה:
 - המידע נוצר, נתקבל, נצבר או נאסף בניגוד להוראות כל דין, או שהמשך השימוש בו מנוגד להוראות דין
 - המידע אינו נחוץ עוד למטרות שלשמן נוצר, נתקבל, נצבר או נאסף
 - תיאורטית מי שעובד נכון בתקנה 4 לא יגיע לתקנה 3
 - למעט למטרות שיווק
 - מחיקה על בסיס בקשה כתובה קיים בחוק בסעיף 14 (מידע לא נכון שמסרבים לתקן) ובסעיף 17 (מידע המשמש לדיוור ישיר – ר' הנחיית דיוור ישיר 2/2017)
- בעל מאגר מידע יודיע בכתב לנושא המידע על החלטתו בבקשה, במועד המוקדם האפשרי בנסיבות העניין
- אין חובת הנמקה ("...על החלטתו...") אבל...

מסקנות והמלצות

- עיקר ההתעסקות תהיה כנראה סביב תקנה 3, שנותנת כלים לנושאי המידע
 - להתחיל data life cycle management ברצינות, תקנה 2(ג) ברצינות
 - ייעול מחיקה בהקשרים שיווקיים
 - מדיניות פרטיות שכוללת התייחסות למידע שלא הגיע ישירות מנושא המידע
 - שפות נוספות?
 - סנקציה:
 - כרגע עוולה אזרחית; אולי ישתנה עם תיקון 14
 - אכיפה של הרשות
 - פרסום הליך האכיפה / ההפרה באתר הרשות
 - מי שפועל היום לפי GDPR – מוכן
 - מי שפועל היום לפי הדין הישראלי (כלומר מקיים את 2(ג) בהשתדלות יתרה) – כמעט מוכן

THANK YOU

The logo for AYR, featuring a small orange square above the letters 'AYR' in a bold, white, sans-serif font.

Amar Reiter Jeanne Shochatovitch & Co



אור רוטר הפילוני
ראש צוות פרטיות בינ"ל,
מח' משפט וטכנולוגיה
OrR@ayr.co.il



שיר שושני-כץ
מנהלת מחלקת
משפט וטכנולוגיה
ShirS@ayr.co.il



אייל שגיא
ראש מחלקת
משפט וטכנולוגיה
EyalS@ayr.co.il