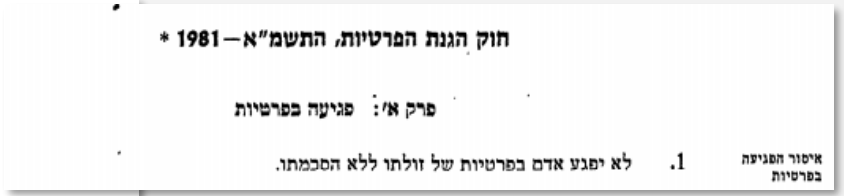
AYR

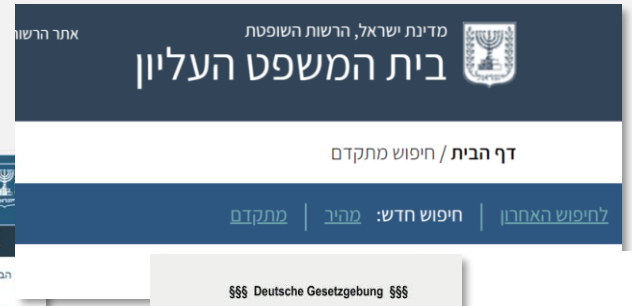
עמר רייטר ז'אן שוכטוביץ ושות'

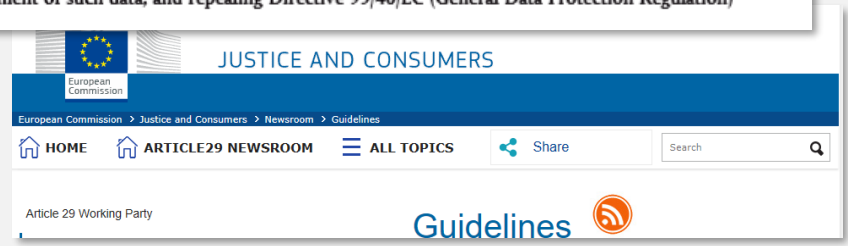
חוק הגנת הפרטיות בהשוואה ל GDPR

אייל שגיא, עו"ד

מסגרת חוקית לחברה ישראלית







תורת ההגנה בסייבר לארגון

Data Processing Agreement

AYR

עקרונות בסיס

- עיבוד חוקי והוגן
- למטרה מוגבלת
- דיוק ועדכניות
- זכות עיון ותיקון
- אבטחת מידע
- מינימליות (אי שמירת מידע עודף)
- שקיפות
- סודיות
- אחריותיות
  - בישראל: בקשר לאבטחת מידע, מיקור חוץ, PIA...

מהו מידע

ישראל

- מידע בסעיף 7
- וכל ענייניו האישיים של אדם
- וכל סוגי המידע שמופיעים בתקנות אבטחת מידע
- וכל מה שאפשר לגלות בהצלבה:
  - "כאשר פרטי מידע אינם עונים להגדרה, אך ניתן להצליבם עם מידע נוסף בשים לב ליכולות העיבוד וההצלבה הקיימות בעידן הדיגיטלי הנוכחי, המאפשר להפוך נתונים חסרי חשיבות כשלעצמם למידע פרטי, הנתונים יחשבו כמידע."

GDPR

- כל מידע מזוהה או ניתן לזיהוי

מידע מסתתר

- מערכת שכר
- דגם מכשיר נייד
- הזמנת ארוחה בטיסה
- כתובת IP
- מצב סוללה

מתי מותר לעבד מידע

ישראל

- בהסכמה מדעת מפורשת
  - מרצון חופשי
  - סבירות, קיפוח
- בהסכמה מדעת משתמעת
  - ביצוע חוזה עם נושא המידע
- כשיש הגנה
  - קיום חובות משפטיות
  - אינטרסים לגיטימיים של "הפוגע"
  - אינטרס ציבורי

GDPR

- בהסכמה מדעת מפורשת
  - מרצון חופשי
  - כללי סבירות והוגנות
- כשהעיבוד נדרש
  - לביצוע חוזה עם נושא המידע
  - לקיום חובות משפטיות
  - לצורך אינטרסים לגיטימיים של המעבד
  - לאינטרס ציבורי

ניהול מערך ניהול הסכמות

ישראל

- כמה סוגי הסכמות
  - Opt-in (מפורשת)
  - Opt-out (משתמעת)
  - יידוע (משתמעת)
- אפשר לחזור מהסכמה
  - אם לא נשאר בסיס אחר לעיבוד – יש להפסיק
- ניהול הסכמות שיווק (חוק הספאם)
  - גם לדיוור ישיר / profiling (חוק הגנת הפרטיות)

GDPR

- רק סוג הסכמה אחד
  - הסכמה מפורשת
  - אבל יש עיבוד ללא הסכמה עם זכות להתנגד
  - ולפעמים אין
- אפשר לחזור מהסכמה
  - אם לא נשאר בסיס אחר לעיבוד – יש להפסיק
- ניהול הסכמות שיווק (e-privacy)
  - גם לדיוור ישיר / profiling (GDPR)

הזכות להתנגד

ישראל

- לא קיימת בשם זה
  - אבל בעיבוד מבוסס הסכמה משתמעת (כמו אינטרס לגיטימי) יש opt out
    - אלא אם יש אינטרס גובר או צרכים משפטיים ואז מספיק יידוע
- אין התייחסות להחלטות אוטומטיות
  - שימו לב לחוק נתוני אשראי
- אם בסיס העיבוד הוא הסכמה – אפשר למשוך

GDPR

- קיימת
  - חלה אם הבסיס לעיבוד הוא אינטרס ציבורי או אינטרס לגיטימי
    - אלא אם מוכח אינטרס גובר, או לצרכים משפטיים
- קיימת לגבי החלטות משמעותיות אוטומטיות
  - למעט ההחלטה אם להתקשר בחוזה
- אם בסיס העיבוד הוא הסכמה – אפשר למשוך

חובת מיפוי מידע ועיבוד

ישראל

- לצורך אבטחת מידע
  - אבטחת מידע זה לא רק עניינים טכניים וניירת
  - תקנה 2(ג) מחייבת דיון שנתי במידע עודף
  - שמחייב בדיקה של נושאים שבליבת דיני הפרטיות
  - אי מחיקה = הפרה של 17 לחוק

GDPR

- לצורך זיהוי הבסיס החוקי לעיבוד כדי שיבהיר מהן הזכויות הקמות לנושא המידע

הזכות להישכח / לדרוש מחיקה

ישראל

- זכות מפורשת רק לגבי מידע שיווקי מאפיין
  - אבל בעל המאגר חייב למחוק מיוזמתו
  - כשהמידע לא נדרש עוד לטובת המטרות שלשמן נאסף
  - אם המידע עובד באופן לא חוקי
- מחייב יכולת טכנית למחיקה חלקית
  - מותר להמשיך לשמור מידע נדרש לתפעול, צורך משפטי
- מעבדי מידע אחרים (מנועי חיפוש) – אין חובת מחיקה

GDPR

- זכות מפורשת
  - כשהמידע לא נדרש עוד לטובת המטרות שלשמן נאסף
  - אין עילה המאפשרת שמירה
  - המידע עובד באופן בלתי חוקי
- מחייב יכולת טכנית למחיקה חלקית
  - מותר להמשיך לשמור מידע נדרש לתפעול, צורך משפטי
- לגבי מעבדי מידע אחרים (מנועי חיפוש) – חובת מחיקה

AYR

זכות לניידות המידע

ישראל

- אין (בשם הזה)
- הנחיית העיון מעניקה זכויות דומות

GDPR

- יש
- במגבלות טכניות
- למידע שנושא המידע בעצמו מסר
- כשהבסיס החוקי הוא הסכמה או חוזה
- וגם זכות עיון
- שימו לב להנחיה בעניין ניידות

תנאים למיקור חוץ

ישראל

- ניתוח סיכונים
- הסכם כתוב בין בעל המאגר למחזיק / קבלן
- הגדרת משך ההתקשרות והגבלת שמירת המידע בסוף ההתקשרות
- הגבלת מטרה, הגדרות העיבוד
- אבטחת מידע
- מעקב ובקרה, דיווחים על אירועים
- תיעוד קבלת ההחלטות שקשורות במיקור חוץ
- נהלים למימוש זכויות נושאי המידע
- איסור על העברת מידע ועל שימוש אחר בלי הסכמה
- שיתוף פעולה עם בעל המאגר

GDPR

- ניתוח סיכונים
- הסכם כתוב בין ה controller ל processor
- הגדרת משך העיבוד, מחיקת מידע או החזרתו בסיום ההתקשרות
- הגבלת מטרה, סוגי מידע
- אבטחת מידע
- מעקב ובקרה, דיווחים על אירועים
- שמירת תיעוד תהליכי העיבוד
- נהלים למימוש זכויות נושאי המידע
- איסור העברה למעבד משנה בלי הסכמה
- עזרה ל controller לקיים את חובותיו, דיווח ל controller על פעולה שמפרה את הרגולציה

ייצוא מידע

ישראל

- תקנות העברת מידע למאגרי מידע מחוץ לגבולות המדינה
  - למדינה שרמת ההגנה בה הולמת / adequate
  - לפי הסכם להחיל את דיני ישראל "בשינויים המחוייבים"
  - בהסכמת נושא המידע
  - למדינות החתומות על האמנה האירופית / למדינות האיחוד האירופי
  - למדינות המקבלות מידע מהאיחוד האירופי "לפי אותם תנאי קבלה"
    - ~~Safe Harbour~~ / Privacy Shield?
  - איסור העברה הלאה / למדינה אחרת
  - = מיקור חוץ

GDPR

- מנגנון קביעת Adequacy
- The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country **without any further safeguard being necessary**. In others words, transfers to the country in question will be assimilated to intra-EU transmissions of data.
  - Privacy Shield להעברות לארה"ב
- מערך הסכמי
  - Standard Contractual Clauses
  - Binding Corporate Rules
- + מיקור חוץ

AYR

אבטחת מידע

ישראל

- מיפוי מאגרים
- מיון עובדים / בדיקות רקע
- הצפנה
- אמצעים טכניים הולמים
- בדיקות ובקרות
- זמינות ועמידות גבוהה
- יכולות שיקום ושחזור נתונים לאחר אירוע אבטחה
- בדיקה והערכה שוטפת של רמת ההגנה על המידע
- ניהול הרשאות גישה
- חובת דיווח על אירועי אבטחה

GDPR

- פסאודונימיזציה
- הצפנה
- אמצעים טכניים הולמים
- בדיקות ובקרות
- זמינות ועמידות גבוהה
- יכולות שיקום ושחזור נתונים לאחר אירוע אבטחה
- בדיקה והערכה שוטפת של רמת ההגנה על המידע
- ניהול הרשאות גישה
- חובת דיווח על אירועי אבטחה

דיווח על אירועי אבטחה

ישראל

- קיימת רק במאגרים ברמת אבטחה בינונית או גבוהה
  - (חשש מבוסס ל)שימוש בלא הרשאה או בחריגה מהרשאה או פגיעה בשלמות
  - אלא אם בחלק לא מהותי במאגר ברמה בינונית
  - דיווח גם לנושאי המידע לפי החלטת הרשם / ראש רשות הסייבר
  - אי זמינות כאירוע אבטחה
  - אם נפגעה שלמות המידע
- דיווח "מיד"
  - תוך 24 ולא יאוחר מ-72 שעות מאותו מועד, "ככלל"

GDPR

- קיימת בכל מאגר
  - (חשש מבוסס ל)גישה או עיבוד לא מורשה של מידע, או פגיעה בשלמות
  - אלא אם לא קיים חשש לפגיעה בנושאי המידע
  - דיווח גם לנושאי המידע – אם יש חשש גבוה לפגיעה בזכויותיהם
  - אי זמינות כאירוע אבטחה
  - אם קיים חשש לפגיעה בנושאי המידע
- דיווח "ללא דיחוי"
  - אך לא יותר מ72 שעות "במידת האפשר"

AYR

הצהרת פרטיות

ישראל

- נדרש (סעיף 11)
  - "מדעת" (ברור, שקוף, נגיש)
- כולל:
  - אם חלה על אותו אדם חובה חוקית למסור את המידע או לא
  - למי יימסר המידע ומטרות המסירה
  - המטרה אשר לשמה מבוקש המידע

GDPR

- נדרש
  - רב שכבתי
- כולל:
  - האם חלה חובה חוקית למסור את המידע או לא
  - סוגי מידע, מקור המידע, מקבלי המידע, העברה למדינה שלישית
  - מטרת העיבוד, הבסיס החוקי, האינטרס הלגיטימי (אם קיים), החלטות אוטומטיות
  - משך שמירת המידע או הקריטריונים שיקבעו אותה
  - קיומן של זכויות נושא המידע והזכות למשוך הסכמה בנסיבות מסוימות
  - הזכות להתלונן לרשות הרלוונטית, פרטי DPO
  - ההשלכות של אי מסירת המידע

AYR

DPIA

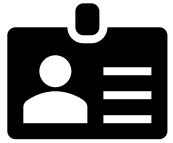
ישראל

- מומלץ לבצע בכל העיבודים שכרוכים בהיבטי פרטיות משמעותיים
  - אי ביצוע הוא בעל פוטנציאל להשפעה שלילית
    - המלצה שאי אפשר לסרב לה?
- מיקור חוץ

GDPR

- חובה לבצע כשהעיבוד מוביל לסיכון גבוה לזכויות וחירויות של נושא המידע
- מיקור חוץ

נושאי תפקידים



ישראל

- מנהל המאגר
  - יש תמיד (אם לא מונה – המנכ"ל הוא המנהל)
  - אחראי על אבטחת מידע וסודיות
  - תקנה 24 לתקנות החדשות ביטלה את תקנה 3 לתקנות תנאי החזקת מידע ושמירתו
  - עובד של הארגון
  - יכול לחוב אישית
  - פועל באופן עצמאי, איסור ניגוד עניינים, בכיר
- ממונה אבטחת מידע
  - נדרש אצל מחזיק בחמישה מאגרים, בנקים וכו' אבל אפשר גם וולנטרי
  - איסור ניגוד עניינים (לא יכול להיות גם מנהל מאגר)
  - מקבל משאבים
  - יכול לחוב אישית
  - יכול לפעול לפי ההוראות של בעל המאגר
  - לא חייב להיות עובד הארגון

GDPR

- DPO
  - נדרש אם ליבת פעולת העיבוד היא עיבוד נרחב ושיטתי
  - ליווי כל הנושאים שקשורים להגנת המידע, ייעוץ, פיקוח על קיום הוראות GDPR, סיוע ב DPIA, תיעדוף פעילויות בהתאם לרמת הסיכון
  - איש קשר מול הרשויות ומול נושאי המידע
  - לא חייב להיות עובד הארגון
  - שמירת נתוני הגיבוי שיש לתעד
  - פועל באופן עצמאי, מוגן מסנקציות ארגוניות, מקבל משאבים, איסור ניגוד עניינים, בכיר
- נציג באירופה
  - לחברות שאינן באירופה (אלא אם העיבוד הוא occasional)
  - אחראי לציות, תיעוד, קשר מול רשויות ונושאי המידע
  - נציג יכול להיתבע ולחוב באופן אישי בקנסות
  - פועל לפי ההוראות של ה controller או ה processor ולכן לא עצמאי
  - לא חייב להיות עובד הארגון

AYR

סנקציות

ישראל

- פלילי
- מחיקת הרישום (!)
- מנהלי
  - צנוע אבל מצטבר
  - + תיקון 13 (!)
- אזרחי
  - פיצוי ללא הוכחת נזק
  - ייצוגיות (!)

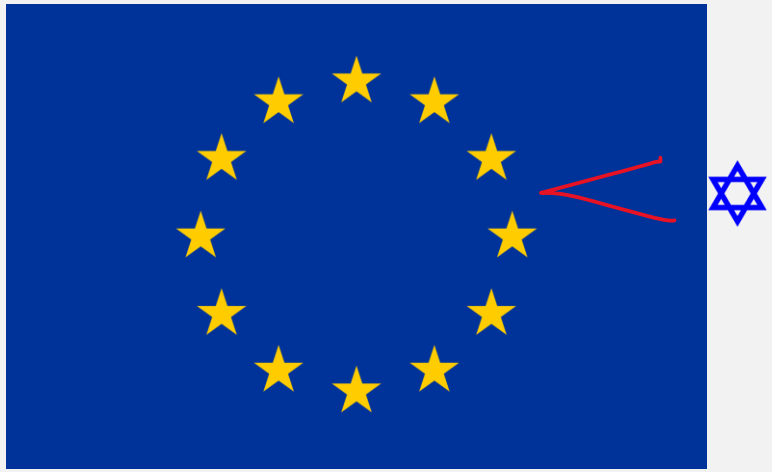
GDPR

- קנסות מנהליים עד 4% מהמחזור העולמי השנתי או 20 מיליון אירו
  - הפרת עקרונות הגנת המידע
  - הפרת זכויות נושאי המידע
  - הפרת הוראות בעניין העברת המידע מחוץ לגבולות האיחוד
- חצי קנס:
  - הסכם מיקור חוץ לא תקין
  - חוסר יישום במערכות של אמצעים טכנולוגיים (PBD) ואי יישום DPIA
  - חוסר יישום של אמצעים לאבטחת מידע, אי דיווח על פריצות למידע
  - אי מינוי קצין הגנת מידע
- הליכים אזרחיים

AYR

מסקנות

- דיני הפרטיות בישראל זה לא מה שהיה פעם
- אין הבדלים גדולים בין דיני הפרטיות בישראל לדיני הפרטיות באירופה
  - יש פערי ציות (אבל גם באירופה)
  - גם בישראל סנקציות כואבות
- כדאי לנצל את ההזדמנות ולישר קו עם הדין הישראלי
  - ולהרוויח גם ציות לרוב GDPR
  - ממילא יפרשו את הדין בישראל בהשפעת ה GDPR



PANIC MODE

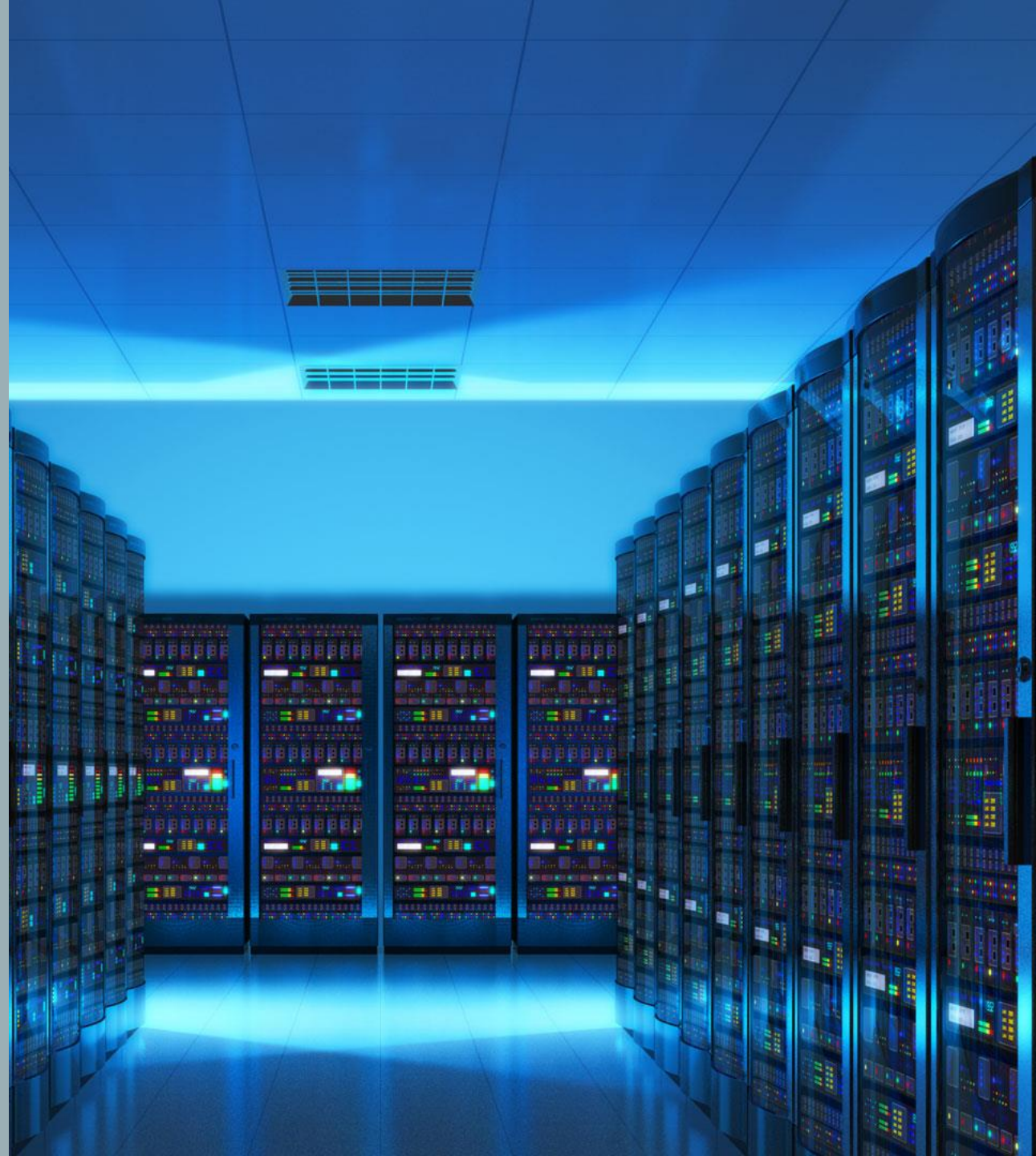
- Don’t Panic
- מאי 2018 הוא אבן דרך – לא סוף הדרך
  - תהליך ארוך טווח ותמידי
- תיעדוף:
  - מיפוי, מיפוי, מיפוי
    - נהלים
    - עדכון מדיניות והצהרות פרטיות, טפסים
    - עדכון הסכמי ספקים
    - התנעת תהליכי DPIA
- DPO / מנהל מאגר / ממונה אבטחת מידע: פרגמטי > נודניק

AYR

עמר רייטר ז'אן שוכטוביץ ושות'

תודה רבה

http://www.ayr.co.il/practice-areas/פרטיות-ועיבוד-נתונים

eyals@ayr.co.il

המצגת היא כללית ואינה תחליף לייעוץ משפטי