
AYR
עולים לענן מבלי להירטב –
עמידה ברגולציה הישראלית צעד אחר צעד
Webinar in collaboration with the ACC Association of Corporate Counsel
13.09.2020 | יום ראשון | 11:00
הנחיות למיקור חוץ, תקנות אבטחת מידע,
שימוש בטכנולוגיית "ענן" - ומה שביניהם.
בהובלת עו"ד אייל שגיא, שותף וראש מחלקת משפט וטכנולוגיה

AYR

מה זה ענן?

AYR

ענן = מיקור חוץ

- חוק הגנת הפרטיות, סעיף 3:
  - "מחזיק, לעניין מאגר מידע" - ~~מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש~~;
- הרשות:
  - "בעל מאגר רשאי בדרך כלל להסתייע בקבלן חיצוני ("מחזיק") לשם אחסון המידע או עיבודו"...
  - מחזיק הוא "הישות אשר מעבדת את המידע עבור בעל המאגר, קרי ספק מיקור חוץ"
  - "במקרה של שירותי ענן, בהם הספק החיצוני ייחשב למחזיק לפי תקנות הגנת הפרטיות, ...יש לוודא בהסכם כי הספק החיצוני מקיים את חובותיו לפי תקנות הגנת הפרטיות, ובפרט תקנה 2 ו15(א) לתקנות הגנת הפרטיות"
- תקנה 15 לתקנות אבטחת מידע
  - "בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע"
  - תקנה 15(א)(2)(ה): "אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה"
- תזכיר חוק הגנת הפרטיות (הגדרות וצמצום חובת הרישום)
  - מחזיק - מי שבמסגרת התקשרות עם בעל המאגר למתן שירות לבעל המאגר או בשמו, קיבל ממנו הרשאה לעשות שימוש במידע במאגר המידע לשם כך.
  - שימוש - לרבות אחסון, עיון, ארגון, תיקון, השלמה, אחזור, מחיקה.

AYR

לא לשכוח את...

- סעיף 11
- "... הודעה שיצויינו בה... למי יימסר המידע ומטרות המסירה"
- צריך לפחות יידוע
- אם לא עומדים בתקנה 15 ייתכן שצריך גם הסכמה מפורשת
- כי מסירת מידע לצד שלישי למטרותיו חורגת מסעיף 2(9) ("צמידות מטרה")
- כל הסכמי הענן מתירים לספק הענן להשתמש במידע למטרות כמו שיפור השירות ואבטחה
- הספק הוא אומנם controller במקרה זה אבל המידע משמש באופן אגרגטיבי
- תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001

תנאים למיקור חוץ

ישראל

- ניתוח סיכונים
- הסכם 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

גופים מפוקחים לא בהכרח פטורים מתקנה 15

- נב"ת A359 מגדיר "מיקור חוץ" באופן צר:
  - "השימוש של תאגיד בנקאי בצד ג' על מנת לבצע, על בסיס מתמשך, פעילויות מהותיות הכלולות ברשימת עיסוקיו של התאגיד הבנקאי המפורטים בסעיף 10 לחוק הבנקאות (רישוי)... בשמו או עבורו."
- פעולה אחרת ע"י קבלן, אינה מיקור חוץ לפי הנב"ת – אבל יכולה להיות מיקור חוץ לפי תקנות אבט"מ (אפילו שהפטור מתקנה 15 בהנחייה 1/2018 כנראה לא הוארך בשל נסיבות ולא משום סיבה מהותית).
- המלצה – להחיל את תקנה 15.

תקנה 15(א)(1)

- "15. (א) בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע –
  - (1) יבחן, לפני ביצוע ההתקשרות עם הגורם החיצוני המסוים כאמור, את סיכוני אבטחת המידע הכרוכים בהתקשרות"
- שימו לב לתקנה 19(ב):
  - "מי שמוטלת עליו בתקנות אלה חובה או אחריות לביצוע פעולה שאינה יצירת מסמך, נדרש לתעד באופן סביר את אופן ביצוע הפעולה לפי העניין"

תקנה 15(א)(2)

- "יקבע במפורש בהסכם עם הגורם החיצוני (בתקנה זו – ההסכם) את כל אלה:"
- הסכם עם ספק ענן:
  - באתר או ב PDF
  - מורכב מעשרות מסמכים
    - SLA
    - הצהרות עמידה בתקנים
    - נהלי אבטחה, white papers ,trust centre, transparency centre, compliance centre
    - נספחים
- הכל ביחד = "ההסכם"
  - אין מנוס, צריך לחפש בערימת הנייר והלינקים מענה לכל הדרישות
  - או לבקש מהספק להתייחס
  - אין דרישת כתב (אבל שימו לב לתקנות הייצוא)

תקנה 15(א)(2)(א)

- "יקבע במפורש... בהסכם... המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות;"
  - הסכמי ענן (לפחות בגירסה האירופית) כוללים סעיף שקובע שספק הענן רשאי לעבד את המידע שהלקוח מעביר, ושהספק לא ישתמש במידע לשום מטרה חוץ מאשר אספקת השירות*
    - זה לא מקרי
  - GDPR סעיף 28 מתייחס להסכם מיקור חוץ וכולל דרישות די דומות לדרישות הישראליות
    - הסכמי מיקור חוץ "אירופאיים" יחסית קלים לשימוש שעומד בדין הישראלי
- * חוץ מאשר מטה-דאטה, מידע תקשורת, לוגים שקשורים לתשתית, מידע נדרש לחיוב...

תקנה 15(א)(2)(ב)

- "יקבע במפורש... בהסכם... מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן"
- לא רלוונטי בדרך כלל

תקנה 15(א)(2)(ג)

- "יקבע במפורש... בהסכם... סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות"
  - החוזה יגביל את המטרות לספק שירות לפי ההגדרות ולפי הפעולות שהלקוח מזמין
  - במילים אחרות, סוג העיבוד יהיה קבוע בהסכם, אבל מי שקבע את זה בעצם זה ספק הענן
  - העיקר שזה נקבע

תקנה 15(א)(2)(ד)

- "יקבע במפורש... בהסכם... משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע"
- יהיה בכל הסכם שעומד ב-GDPR

תקנה 15(א)(2)(ה)

- "יקבע במפורש... בהסכם... אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע"
- עכשיו הדברים מסתבכים
- אומנם סעיף 32 ל GDPR קובע חובות אבטחת מידע לא מאוד שונות מדרישות התקנות
- אבל התקנות הרבה יותר מפורטות, ולפעמים יש דרישות יוצאות דופן
- נגיע לזה

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

AYR

תקנה 15(א)(2)(ו)

- "יקבע במפורש... בהסכם... חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור בפסקת משנה (ה)"
  - יופיע איפשהו במסמכים עקב GDPR סעיף 28(3)(b)
  - "The processor… ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality"
  - ביחד עם GDPR 32(4):
  - "The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller"

תקנה 15(א)(2)(ז)

- "יקבע במפורש... בהסכם... התיר בעל מאגר מידע לגורם החיצוני לתת את השירות באמצעות גורם נוסף – חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו"
  - יופיע איפשהו במסמכים עקב GDPR סעיף 28(2), אבל בצורה "הפוכה":
  - “The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.”

תקנה 15(א)(2)(ח)

- "יקבע במפורש... בהסכם... חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה"
  - יידוע על אירוע אבטחה יופיע איפשהו במסמכים עקב GDPR, אבל
  - יש כמה פערים בין הגדרת אירוע אבטחה בישראל ל GDPR
    - מצד שני, הספק לא יכול להיות בטוח לגבי ההגדרות שחלות על המידע הספציפי, ולכן צפוי "עודף דיווח"
  - לגבי "דיווח פעם בשנה", למעשה יש התחייבויות לעמוד ב GDPR, יש דפים עם ריכוז מידע שוטף, וכו', לאור דרישת GDPR 28(3)(h)
  - במקום דיווח פעם בשנה, יש דיווח כל הזמן

תקנה 15(א)(3)

- "יפרט בנוהל האבטחה של המאגר גם את העניינים המנויים בפסקה (2)(א) עד (ה), וכן יפנה בו במפורש להסכם עם הגורם החיצוני ולנוהל האבטחה שלו"
- שוב חוזר נושא התיעוד

תקנה 15(א)(4)

- " ינקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש בשים לב לסיכונים האמורים בפסקה (1)"
- הספק מספק את הכלים, כי זה נדרש ב GDPR סעיף 28

עמידת מחזיק בתקנות אבטחת מידע

- צריך לעשות את תהליך איתור ההתחייבויות לגבי כל התקנות
  - חוץ מאשר 2 ו 15(א) (שתקנה 19(א) פוטרת לגבי "מחזיק"), והכל "בשינויים המחויבים ולפי העניין"
    - יש כנראה דרך קיצור, אם הספק מתחייב ל GDPR
    - הגדרת מחזיק באתר רשות הגנת הפרטיות היא לא ההגדרה שבחוק, אלא processor
- התשובות לעמידה בתקנות יכולות להיות ב...
  - הסכם עצמו
  - נוהל אבטחת מידע שהספק מפרסם
  - נובעות מהתחייבות הספק לעמוד בתקן שכולל דרישה מקבילה לדרישה בתקנות
  - White paper
  - צריך לחפור

התייחסויות חסרות

- לא תמיד אפשר למצוא מענה לכל דרישה בתקנות אבטחת מידע
  - לפי תקנה 19(א), התקנות חלו על מחזיקים "בשינויים המחויבים ולפי העניין"
    - שינוי מחוייב אפשרי – הספק לא בארץ!
    - להתייעץ עם מחלקת אבטחת מידע אם אפשר לוותר – ולתעד את ההחלטה
- דוגמאות
  - לחובה לשמור לוגים לשנתיים (תקנה 17(א)) אין מקבילה ב GDPR, להיפך, מוחקים
    - פתרון – הורדת הלוגים למערכות SIEM שלכם

הנחיית מיקור חוץ

- בחינה מקדמית - מגבלה חוקית או אתית להעברת המידע.
- הגדרת אופן מתן השירות על ידי הקבלן, תוך עדיפות לדרך של הרשאות גישה (ולא העברת מאגר מידע).
- בחירת הקבלן - ניסיון קודם, מוניטין, חשש לניגוד עניינים.
- אם הקבלן אוסף מידע עבור בעל המאגר - הקבלן יקיים את סעיף 11.
- איסור על הקבלן לאסוף מידע בדרך לא חוקית או להשתמש במאגרים לא חוקיים.
- בטוחות, סעדים וכלי בקרה על הקבלן.
- ייחוד עיסוק והפרדה מבנית אצל הקבלן במידת הצורך.
- קיום חובת הדיווח השנתית של מחזיק במעל חמישה מאגרים.
- קביעת הוראות בהסכם לגבי מימוש זכויות העיון והתיקון של נושאי המידע.
- הטמעת הוראות ההסכם אצל עובדי הקבלן וקביעת אנשי קשר לצורך כך.
- תיעוד קבלת החלטות לגבי מיקור החוץ.

ייצוא מידע מישראל והקשר לאירופה

- תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001
  - "אף אם החוק הישראלי עומד כשלעצמו בסטנדרטים האירופאים, כל עוד אין הוא חוסם אפשרות להעביר מידע למאגרים במדינות שאינן עומדות בסטנדרטים אלה, אוסרת הדירקטיבה האירופאית להעביר מידע למאגרים בישראל"
  - "התקנות נחקקו על מנת שמדינת ישראל תעמוד בסטנדרטים אותם הציב האיחוד האירופאי בדירקטיבה... אי התאמת המצב המשפטי בישראל למצב הרצוי על פי הסטנדרטים האירופאים הייתה מבודדת את המאגרים הנמצאים בישראל ממידע שמקורו במדינות האיחוד האירופאי"

ייצוא למדינות תואמות 1

- תקנה 1: ההעברה מותרת אם דין המדינה שאליה מועבר המידע, מבטיח רמת הגנה על מידע שאינה פחותה, בשינויים המחויבים, מרמת ההגנה על מידע הקבועה בדין הישראלי, ובכלל זה קובע עקרונות אלה:
  - חוקיות והוגנות העיבוד, עדכניות, צמידות מטרה, עיון ותיקון, אבטחת מידע
  - (הרשימה המסודרת היחידה בחקיקה של עקרונות עיבוד המידע בישראל, מוצע בתזכיר)
  - הרשות: מדינה בה חל ה GDPR או שתקיים את ה GDPR (=בריטניה) עונה על תקנה 1
  - האם ישראל תמשיך להעביר מידע לבריטניה על בסיס ה GDPR אפילו אם האיחוד לא ייתן לה adequacy (השאלה השוויצרית)?
- תקנה 2(8)(1): ההעברה מותרת למאגר במדינה החתומה על אמנה 108
  - כל מדינות האיחוד האירופי, בריטניה, שווייץ, אבל גם רוסיה ואוקראינה
  - החלטת הרשות לגבי בריטניה הוסיפה טריטוריות בריטיות שלא מכוסות באמנה

AYR

ייצוא למדינות תואמות 2

- תקנה 2(8)(2): העברה למדינות המקבלות מידע מהאיחוד האירופי לפי אותם תנאי קבלה
  - ~~Safe Harbour~~
    - "נחסמה האפשרות החוקית להעביר מידע ממאגר בישראל לארה"ב בהתבסס על תקנה 2(8)(2) לתקנות"
    - פעם ראשונה ואחרונה שהרשות הודיעה פורמלית שאפשר היה להעביר לפי SB
  - ~~Privacy Shield~~
    - לא היה redress לישראלים (האם מטרת התקנות להגן על מידע ישראלי או על מידע אירופאי?)
    - יש Adequacy אירופאי

ייצוא לפי בסיסים אחרים

- תקנה 2(1): האדם שעליו המידע הסכים להעברה
  - מדעת
  - מרצון חופשי?
    - עמדת הרשות לגבי העברת מידע לרשות ני"ע האמריקאית (SEC) - סעיף ויתור סודיות ברור בהסכם עם נושא המידע מהווה הסכמה לפי תקנה 2(1)
- תקנה 2(3): מחברה ישראלית לחברה בת זרה שלה שמתחייבת להגן על הפרטיות
  - לא להיפך
- תקנה 2(6): העברת המידע הכרחית לשם הגנה על שלום הציבור או ביטחונו
  - הכרחית = strictly necessary

AYR

ייצוא לפי התחייבות חוזית

- תקנה 2(4): העברה "למי שהתחייב בהסכם עם בעל מאגר המידע שממנו מועבר המידע, לקיים את התנאים לאחזקת מידע ולשימוש בו החלים על מאגר מידע בישראל, בשינויים המחויבים"
  - זו לא בהכרח התחייבות לקיים את דין ישראל, אלא הסכם שכולל את "התנאים לאחזקת מידע ולשימוש בו החלים בישראל" (בערך מה שה-SCC עושים)
- לפי תקנה 2(8)(2): העברה "למאגר במדינה המקבלת מידע ממדינות החברות בקהיליה האירופית, לפי אותם תנאי קבלה"
  - זאת אומרת שאפשר להחיל את ה SCC על ההעברה מישראל למדינה השלישית
  - אבל...

AYR

העברה מישראל לפי SCC

- האם התחייבות חוזית אזרחית מתירה את הייצוא לאור הביטוי "מאגר במדינה" שבתקנה 2(8)?
  - הרשות: המפתח הוא דין המדינה וארה"ב לא מכבדת פרטיות
  - Schrems II אולי פתר את הבעיה הזו:
    - צריך לבדוק גם את מידתיות הגישה למידע בידי הרשויות במדינה המקבלת + זכות עמידה
    - בנוסף להתחייבות חוזית של המקבל
  - ויצר אחרת: ההעברה חייבת להיות מלווה בבדיקת הדין במדינה השלישית

AYR

תודה!

אייל שגיא

EyalS@ayr.co.il