GDPR ותקשורת מקצועית: מדוע הרוב מפרים את הכללים מבלי לדעת זאת

כמעט כל משרד, קליניקה או חברת ייעוץ שולחים מסמכי לקוחות באמצעות אפליקציות שהשרת שלהן נמצא מחוץ לאזור הכלכלי האירופי. ללא כוונת זדון, אך במקרים רבים תוך הפרת התקנה, מבלי שאיש הזהיר אותם.

המסמך שנוסע רחוק יותר ממה שאתם חושבים

סיטואציה יומיומית: יועצת מס מקבלת בהודעות מסמך עם נתוני לקוח. איש מכירות מעביר בצ'אט הצעת מחיר לקולגה. רופאה משתפת באותה דרך דוח קליני עם שותף לעבודה. אף אחד לא חושב פעמיים. זה נורמלי. זה נוח. זה מה שנעשה בכל יום בכל משרד בכל עיר באירופה.

אבל המסמך הזה, במקרים רבים, בדיוק נסע לשרת בארצות הברית. הוא אוחסן – ולו זמנית, ולו "מוצפן במנוחה" – בענן שלא איש המקצוע ולא הלקוח שלו שולטים בו. הוא עבר דרך מערכות שיכולות טכנית לאנדקס מטא-נתונים הקשורים לתוכן. ולתקנת הגנת הנתונים הכללית האירופית יש כמה דברים די ברורים לומר על כך.

מה הנורמה דורשת

ה-GDPR – ובעקבותיו הפסיקה של בית הדין לצדק של האיחוד האירופי (במיוחד פסק דין Schrems II, C-311/18, משנת 2020) – קובע כי יש להגן על נתונים אישיים של אזרחים אירופיים באופן הולם. אם נתונים אלו עוזבים את האזור הכלכלי האירופי, על בעל השליטה להבטיח שהמקבל מציע רמת הגנה ש"דומה במהותה" לזו האירופית. בפועל, המשמעות היא ששליחת נתוני לקוחות באמצעות שירותים שהשרתים שלהם נמצאים תחת סמכות השיפוט של ארה"ב, מבלי שבוצעה הערכת השפעה ומבלי שיושמו ערבויות משלימות – סעיפים חוזיים סטנדרטיים, אמצעים טכניים נוספים כמו הצפנה ניתנת לאימות וכד' – עלולה להוות הפרה של התקנה. גם אם עד עכשיו אף אחד לא אמר כלום.

וזה לא רק על תוכן ההודעות. המטא-נתונים – מי שולח מה למי, מתי, באיזו תדירות, מאיפה – הם גם נתונים אישיים לפי התקנות, לפי פרשנות חוזרת של הוועדה האירופית להגנת נתונים (EDPB). שירות האוסף מטא-נתונים מהתקשורת המקצועית של משתמש מעבד נתונים אישיים של לקוחותיו של אותו משתמש, מבלי שהם מודעים לכך או נתנו הסכמה כלשהי לעיבוד כזה.

דפוס החשיבה הנפוץ – "אני משתמש באפליקציה רק לכתיבה; האפליקציה אינה ספק נתונים של הלקוח שלי" – הוא שגוי מבחינה משפטית. אם נתוני הלקוח עוברים דרך תשתית של צד שלישי, אותו צד שלישי מעבד את הנתונים הללו. ואם הוא מעבד אותם, חייב להיות בסיס חוקי, הסכם עיבוד נתונים וערבויות מתאימות.

מי אחראי

השאלה מי נושא באחריות המשפטית אינה אקדמית. ה-GDPR מבחין בין *בעל השליטה* (מי שמחליט אילו נתונים מעובדים ולאיזו מטרה) לבין *המעבד* (מי שעושה זאת באופן מהותי בשמו של בעל השליטה). איש המקצוע ששולח מסמכי לקוחות הוא בעל השליטה. ספק אפליקציית ההודעות הוא במקרים רבים המעבד בפועל. ללא הסכם עיבוד – וללא רוב הסעיפים שהסכם כזה אמור להכיל – בעל השליטה לא מילא את חובתו.

הפרשנות המקלה אומרת: "רוב אנשי המקצוע אינם יודעים זאת". הפרשנות המחמירה אומרת: "אי ידיעת החוק אינה פוטרת מעונש". והפרשנות של כל עורך דין מומחה להגנת נתונים שמתייעצים איתו בנושא היא בדרך כלל המחמירה.

למי זה חשוב באופן קונקרטי

לכל איש מקצוע או חברה הפועלים, אפילו מדי פעם, עם מידע אישי של צדדים שלישיים:

- עורכי דין המקבלים תיעוד לקוחות (חוזים, תביעות, הצהרות, דוחות רכוש).
- רופאים ואנשי מקצוע אחרים בתחום הבריאות המשתפים נתוני בריאות – הנחשבים לפי סעיף 9 ל-GDPR כ-*קטגוריות מיוחדות* עם משטר הגנה מוגבר –.
- יועצי מס ומנהלים אדמיניסטרטיביים הפועלים עם נתוני זיהוי, מס ובנק.
- מחלקות משאבי אנוש המנהלות תיעוד עבודה ואישי של עובדים.
- נציגי מכירות המקבלים פרטי התקשרות ולעיתים קרובות מידע עסקי רגיש מלקוחות פוטנציאליים ולקוחות קיימים.

בכל המקרים, המידע מוגן על ידי ה-GDPR. בכל המקרים, בפרקטיקה המקובלת, מידע זה זורם בערוצים שסמכות השיפוט שלהם אינה מאפשרת להכריז עליהם כ"דומים במהותם" למסגרת האירופית ללא ערבויות נוספות. לא מכוונת זדון. מתוך הרגל. ובגלל תשתית טכנולוגית שבמשך חמש עשרה שנים העמידה את הנוחות לפני הציות.

הטיעון של "כולם עושים את זה"

כדאי לצפות מראש את ההתנגדות הנפוצה ביותר: "אם כולם עושים את זה, זה לא יכול להיות בעיה אמיתית". זהו טיעון מובן לחלוטין ומשפטית אין לו שום תוקף. העובדה שפרקטיקה נפוצה אינה הופכת אותה לתואמת את התקנה. רשויות הגנת הנתונים הטילו בשנים האחרונות סנקציות על מספר חברות בדיוק בגלל דרכי שימוש בהודעות שנראו תמימות עד לרגע הביקורת.

המציאות התפעולית הנוכחית היא שהסיכון מבחינת הסתברות הוא נמוך – נדיר מאוד שביקורת של הרשות תבדוק את כלי ההודעות הספציפיים של משרד בינוני – אך גבוה מבחינת השפעה אם הוא מתממש. זהו סיכון שרובם לוקחים מבלי לדעת שהם לוקחים אותו. כלומר, מבלי שהעריכו האם הכלי שבו הם משתמשים תואם את האחריות המשפטית של בעל השליטה.

עקבות דיגיטליים הם רטרואקטיביים

יש טיעון שני, כמעט סימטרי לקודם, שכדאי לצפות מראש: *"אם זה היה בעיה רצינית, הממשל כבר היה מתחיל לבדוק את זה"*. המציאות הנצפית הנוכחית נותנת לו צדק שטחי. ביקורות על שימוש לא ראוי בהודעות בחברות קטנות ובעיקר אצל עצמאים כמעט אינן קיימות כיום – לא בגלל שההתנהגות מותרת, אלא בגלל שלממשל ברוב מדינות האיחוד האירופי חסרים המשאבים האנושיים הנדרשים לביקורת של מיליוני חייבים.

זה מה שהפרקטיקה הנצפית היום מרמזת. אבל זה לא מה שהעשור הבא מרמז. שני וקטורים מתכנסים כדי לשנות את האיזון בפרקי זמן קצרים יחסית.

ראשית: עקבות דיגיטליים הם רטרואקטיביים. כל הודעה שנשלחת דרך אפליקציה עם שרת מרכזי נשארת רשומה – לפחות במטא-נתונים – בתשתית שנשמרת. מה שנשלח לפני שישה חודשים עדיין ניתן לביקורת טכנית היום. מה שנשלח היום יהיה ניתן לביקורת בעוד חמש שנים. היעדר ביקורת בהווה אינו ערובה להיעדר ביקורת בעתיד. זו דחייה של ההערכה, לא פטור ממנה.

שנית: יכולת הביקורת המנהלית תגדל באופן מואץ. הכנסת כלי בינה מלאכותית לתהליכי הבקרה מבטלת את צוואר הבקבוק האנושי שעד כה הגן – דה-פקטו, לא דה-יורה – על חברות קטנות ועצמאיים. מערכת המסוגלת להצליב כמויות אדירות של מטא-נתונים, הצהרות מס, מרשמי מסחר וחובות דיווח על פרצות אבטחה אינה זקוקה למפקחים: היא זקוקה לגישה. והגישה באמצעות דרישות מספקים עם נוכחות משפטית באיחוד האירופי במסגרת הנורמטיבית הנוכחית היא אפשרית לחלוטין.

לכך מתווסף גורם פחות טכני אך מכריע באותה מידה: מדינות אירופה נמצאות בתהליך של חוב הולך וגדל ועליהן, כמעט ללא יוצא מן הכלל, להרחיב את בסיס המס שלהן. הסנקציה המנהלית הנובעת מאי-ציות ל-GDPR היא במונחים

פיסקאליים טהורים מקור הכנסה גדל ונוח פוליטית. זו אינה השערה: זו מגמה נצפית בדוחות השנתיים של רשויות הגנת הנתונים האירופיות, שבהם היקף הסנקציות הכולל עולה מזה מספר שנות כספים רצופות.

המסקנה התפעולית עבור בעל השליטה אינה אזעקת שווא אלא מפוכחת: **ההחלטה כיצד מנוהלת היום התקשורת עם הלקוחות מוערכת מול יכולת הביקורת של השנה שבה תגיע הביקורת, לא מול הנוכחית.** ויכולת זו תהיה, בטווח זמן סביר, שונה מהותית מזו של היום. מי שמתחיל לעשות דברים נכון היום לא יהיה בסדר רק מהיום: העקבות שנוצרים מרגע זה ואילך יהיו תואמים לנורמה, וזה מגן רטרואקטיבית על התקופה הבאה. מי שימשיך כפי שהיה עד כה יצבור עקבות ניתנים לביקורת שהתאימות שלהם תוערך לפי הסטנדרטים – והמשאבים – של השנים הבאות.

מה משתנה עם ארכיטקטורה אחרת

קיימות חלופות טכניות שבהן הנתונים אינם מאוחסנים בתשתית של צדדים שלישיים, אלא נוסעים ישירות מהמכשיר של השולח למכשיר של המקבל. בארכיטקטורה זו, הציות ל-GDPR בכל הנוגע להעברות בינלאומיות אינו תלוי בסעיפים חוזיים סטנדרטיים, לא ברצון הטוב של הספק ולא בביקורות עתידיות. הוא תלוי בכך ש*אין העברה*. ועל מה שאינו קיים אי אפשר לעבור.

זהו אינו פתרון בלעדי ואינו היחיד האפשרי. אך הוא שונה מבחינה מבנית, והציות הנורמטיבי מפסיק להיות נספח תהליכי והופך לתוצאה ישירה של התכנון. עבור איש מקצוע הלוקח את אחריותו כבעל שליטה ברצינות, ההבדל הזה משמעותי.

הגיליון הבא של Cuadernos ינתח בפירוט את פסק דין Schrems II והשלכותיו המעשיות עבור חברות קטנות ובינוניות התלויות בשירותי ענן מארה"ב, חמש שנים לאחר פרסומו.

מקורות ומסגרת נורמטיבית

- תקנה (EU) 2016/679 (GDPR), במיוחד פרק V בנושא העברות בינלאומיות.
- CJUE C-311/18 ("Schrems II"), 16 ביולי 2020.
- EDPB – המלצות 01/2020 על אמצעים המשלימים את כלי ההעברה.
- רשויות הגנת הנתונים – דוחות שנתיים עם מקרי סנקציות בגין שימוש לא ראוי בהודעות מיידיות בסביבות מקצועיות.

← הקודם החיסיון המקצועי בעידן הדיגיטלי הבא → כשאין אף אחד באמצע

קריאות אחרונות

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

קחו את המאמר הזה אתכם לכל מקום שתצטרכו.

Markdown ↓ · טקסט פשוט ↓ · PDF ↓

הקובץ יורד למכשיר שלכם. משם תוכלו לשמור אותו, לייבא אותו ל-Solo2 או לשתף אותו היכן שתרצו. Cuadernos לא מחליטה על היעד עבורכם.

חותם שעווה · SHA-256 ef6e76587fb3bfc6fda32529a6332232f86f2d87f3fc172218fffd4e8e1e07fd

Cuadernos Lacre · פרסום של Menzuri Gestión S.L. ·
נכתב על ידי R.Eugenio · נערך על ידי צוות Solo2.

אתר זה אינו משתמש בעוגיות (cookies) ואינו טוען משאבים מצד שלישי. הוא משתמש במונה ביקורים אנונימי באירוח עצמי (Umami, בשרת האירופי שלנו) ובמינימום ה-JavaScript הנדרש להעדפת ערכת הנושא הבהירה/כהה שלכם. ללא מעקבים, ללא פרופילינג, ללא שיתוף נתונים. אם תרצו לעקוב אחרינו: RSS.