GDPR och professionell messaging: varför de flesta bryter mot reglerna utan att veta om det

Nästan varje kontor, klinik eller konsultbyrå skickar klientdokument via appar vars server befinner sig utanför Europeiska ekonomiska samarbetsområdet. Utan onda avsikter, men i många fall i strid med förordningen utan att någon varnat dem.

Dokumentet som färdas längre än du tror

En vardagssituation: en skatterådgivare får ett dokument med kunduppgifter via en meddelandetjänst. En säljare skickar en offert vidare till en kollega via chatt. En läkare delar en klinisk rapport med en kollega på samma sätt. Ingen tänker två gånger på det. Det är det normala. Det är det bekväma. Det är vad som görs varje dag på varje kontor i varje stad i Europa.

Men det dokumentet har i många fall just färdats till en server i USA. Det har lagrats – om än tillfälligt, om än "krypterat i vila" – i ett moln som varken yrkesutövaren eller klienten kontrollerar. Det har passerat system som tekniskt kan indexera metadata kopplad till innehållet. Och den europeiska dataskyddsförordningen har en hel del klart att säga om det.

Vad regelverket kräver

GDPR – och i förlängningen rättspraxis från EU-domstolen (särskilt Schrems II-domen, C-311/18, från 2020) – fastslår att personuppgifter för europeiska medborgare måste vara adekvat skyddade. Om dessa uppgifter lämnar Europeiska ekonomiska samarbetsområdet måste den personuppgiftsansvarige garantera att mottagaren erbjuder en skyddsnivå som är "i allt väsentligt likvärdig" med den europeiska. I praktiken innebär det att skicka kunduppgifter via tjänster vars servrar lyder under amerikansk jurisdiktion, utan att ha gjort en konsekvensbedömning och implementerat kompletterande skyddsåtgärder – standardavtalsklausuler, ytterligare tekniska åtgärder som verifierbar kryptering etc. – kan utgöra ett brott mot förordningen. Även om ingen har sagt något än.

Och det handlar inte bara om meddelandenas innehåll. Metadata – vem som skickar vad till vem, när, hur ofta, varifrån – är också personuppgifter enligt regelverket, enligt upprepad tolkning från Europeiska dataskyddsstyrelsen (EDPB). En tjänst som samlar in metadata från en användares yrkesmässiga kommunikation behandlar personuppgifter om den användarens klienter, utan att dessa har kännedom om det eller har gett sitt samtycke till sådan behandling.

Det vanliga tankemönstret – "jag använder bara appen för att skriva; appen är inte en dataleverantör till min klient" – är juridiskt felaktigt. Om klientens uppgifter passerar genom en tredje parts infrastruktur behandlar denna tredje part dessa uppgifter. Och om denne behandlar dem måste det finnas en laglig grund, ett personuppgiftsbiträdesavtal och adekvata garantier.

Vem som är ansvarig

Frågan om vem som bär det juridiska ansvaret är inte akademisk. GDPR skiljer mellan *personuppgiftsansvarig* (den som bestämmer vilka uppgifter som behandlas och varför) och *personuppgiftsbiträde* (den som utför behandlingen rent faktiskt, på uppdrag av den ansvarige). Yrkesutövaren som skickar klientdokument är den ansvarige. Leverantören av meddelandeappen är i många fall i praktiken ett biträde. Utan ett biträdesavtal – och utan de flesta av de klausuler som ett sådant avtal bör innehålla – har den ansvarige inte uppfyllt sin skyldighet.

Den välvilliga tolkningen är: "de flesta yrkesutövare vet inte om detta". Den strikta tolkningen är: "okunnighet om lagen är ingen ursäkt". Och tolkningen hos varje specialiserad dataskyddsjurist som rådfrågas i ärendet är i allmänhet den strikta.

För vem detta är viktigt i praktiken

För varje yrkesutövare eller företag som hanterar, även om det bara sker sporadiskt, personlig information om tredje part:

- Advokater som tar emot dokumentation från klienter (avtal, stämningsansökningar, yttranden, förmögenhetsrapporter).
- Läkare och annan vårdpersonal som delar hälsouppgifter – som betraktas som *särskilda kategorier* enligt art. 9 GDPR, med ett förstärkt skydd –.
- Skatterådgivare och administratörer som hanterar identifikations-, skatte- och bankuppgifter.
- HR-avdelningar som hanterar arbets- och personaldokumentation för anställda.
- Säljare som tar emot kontaktuppgifter och ofta känslig affärsinformation från prospekt och kunder.

I alla fall skyddas informationen av GDPR. I alla fall, i vanlig praxis, passerar denna information genom kanaler vars jurisdiktion inte tillåter att de förklaras "i allt väsentligt likvärdiga" med det europeiska regelverket utan kompletterande skyddsåtgärder. Inte av ondska. Av vana. Och på grund av en teknisk infrastruktur som har prioriterat bekvämlighet framför efterlevnad under femton år.

Argumentet "alla gör det"

Man bör föregripa den vanligaste invändningen: "om alla gör det kan det inte vara ett verkligt problem". Det är ett fullt förståeligt argument och har juridiskt sett ingen kraft. Det faktum att en praxis är utbredd gör den inte förenlig med förordningen. Integritetsskyddsmyndigheten (IMY) har under de senaste åren sanktionerat flera företag just för användning av meddelandetjänster som verkade harmlösa fram till tidpunkten för granskningen.

Den nuvarande operativa verkligheten är att risken är låg i termer av sannolikhet – det är mycket sällsynt att en granskning från IMY auditerar de specifika meddelandeverktygen hos en medelstor byrå – men hög i termer av effekt om den realiseras. Det är en risk som de flesta tar utan att veta att de tar den. Det vill säga utan att ha utvärderat om verktyget som används är i linje med den personuppgiftsansvariges juridiska ansvar.

Det digitala spåret är retroaktivt

Det finns ett andra argument, nästan symmetriskt med det föregående, som bör föregripas: *"om detta vore ett allvarligt problem skulle myndigheterna redan ha börjat granska det"*. Den nuvarande observerade verkligheten ger det rätt på ytan. Granskningar för felaktig användning av meddelandetjänster i små företag och framför allt hos egenföretagare är idag nästan obefintliga – inte för att beteendet är tillåtet, utan för att myndigheterna, i Sverige och i stora delar av EU, saknar de mänskliga resurser som krävs för att granska miljontals ansvariga.

Det är vad dagens observerade praxis antyder. Det är inte vad det kommande decenniet antyder. Två vektorer sammanstrålar för att förändra balansen på relativt kort tid.

För det första: det digitala spåret är retroaktivt. Varje meddelande som skickas via en app med en central server förblir registrerat – åtminstone i metadata – i en infrastruktur som består. Det som skickades för sex

månader sedan är tekniskt sett fortfarande möjligt att granska idag. Det som skickas idag kommer fortfarande att vara möjligt att granska om fem år. Frånvaron av en nuvarande granskning är ingen garanti för frånvaron av en framtida granskning. Det är ett uppskjutande av utvärderingen, inte ett undantag.

För det andra: den administrativa granskningskapaciteten kommer att växa accelererat. Införandet av verktyg för artificiell intelligens i granskningsprocesserna eliminerar den mänskliga flaskhalsen som hittills har skyddat – i praktiken, inte i rätten – små företag och egenföretagare. Ett system som kan samköra massiva metadata, skattedeklarationer, bolagsregister och skyldigheter att anmäla personuppgiftsincidenter kräver inga inspektörer: det kräver åtkomst. Och åtkomst, genom förelägganden till leverantörer med juridisk närvaro i EU, är fullt genomförbar under det nuvarande regelverket.

Till detta tillkommer en mindre teknisk men lika avgörande faktor: de europeiska staterna befinner sig i en process med ständigt växande skuldsättning och behöver, nästan utan undantag, utöka sin skattebas. De administrativa sanktionsavgifter som följer av brott mot GDPR är, i rent fiskala termer, en växande och politiskt bekväm inkomstkälla. Det är ingen gissning: det är en observerbar trend i de europeiska dataskyddsmyndigheternas årsredovisningar, där den totala volymen av sanktioner har ökat under flera på varandra följande räkenskapsår.

Den operativa slutsatsen för den personuppgiftsansvarige är inte alarmistisk, utan nykter: **beslutet om hur kommunikationen med klienter hanteras idag utvärderas mot granskningskapaciteten det år granskningen sker, inte mot den nuvarande.** Och den kapactieten kommer, inom en rimlig tidsram, att vara väsentligt annorlunda än idag. Den som börjar göra saker rätt idag kommer inte bara att ha ryggen fri från och med idag: det spår som genereras från och med nu kommer att vara förenligt med regelverket, och det skyddar retroaktivt den tid som kommer. Den som fortsätter som hittills kommer att ackumulera ett granskningsbart spår vars efterlevnad kommer att bedömas mot standarderna – och resurserna – under de kommande åren.

Vad som ändras med en annan arkitektur

Det finns tekniska alternativ där data inte lagras i tredje parts infrastruktur, utan istället färdas direkt från sändarens enhet till mottagarens. I den arkitekturen beror efterlevnaden av GDPR när det gäller internationella överföringar inte på standardavtalsklausuler, leverantörens goda vilja eller framtida granskningar. Den beror på att det *inte sker någon överföring*. Och det som inte finns kan man inte bryta mot.

Detta är inte en exklusiv lösning eller den enda möjliga. Men den är strukturellt annorlunda, och regelefterlevnaden upphör att vara ett procedurellt tillägg och blir en direkt konsekvens av designen. För en yrkesutövare som tar sitt ansvar som personuppgiftsansvarig på allvar, spelar den skillnaden roll.

Nästa del av Cuadernos kommer att i detalj analysera Schrems II-domen och dess praktiska konsekvenser för små och medelstora företag som är beroende av amerikanska molntjänster, fem år efter dess publicering.

Källor och regelverk

- Förordning (EU) 2016/679 (GDPR), särskilt kapitel V om internationella överföringar.
- EU-domstolens dom i mål C-311/18 ("Schrems II"), den 16 juli 2020.
- EDPB – Rekommendationer 01/2020 om åtgärder som kompletterar överföringsverktygen.
- Integritetsskyddsmyndigheten (IMY) – Årsredovisningar med fallstudier av sanktioner för felaktig användning av snabbmeddelanden i yrkesmiljöer.

← FöregåendeTystnadsplikten i den digitala tidsåldernNästa →När ingen är emellan

Senaste läsning

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ta med dig den här artikeln dit du behöver den.

↓ Markdown ↓ Klartext ↓ PDF

Filen laddas ner till din enhet. Därifrån kan du spara den, importera den till Solo2 eller dela den var du vill. Cuadernos bestämmer inte destinationen åt dig.

Lacksigill · SHA-256 c39a951ffcbdb6837d285857164a00f57ab4ff4f5406a66c36270026f7a4a393

Cuadernos Lacre · En utgåva från Menzuri Gestión S.L. ·
skriven av R.Eugenio · redigerad av teamet bakom Solo2.