Analyse · 16. maj 2026

← Forrige·Næste →

GDPR og professionel messaging: Hvorfor de fleste overtræder reglerne uden at vide det

Næsten ethvert kontor, klinik eller rådgivningsvirksomhed sender klientdokumenter via applikationer, hvis server befinder sig uden for Det Europæiske Økonomiske Samarbejdsområde. Uden onde hensigter, men i mange tilfælde i strid med forordningen, uden at nogen har advaret dem.

Dokumentet, der rejser længere end du tror

En hverdagssituation: En skatterådgiver modtager et dokument med klientdata via messaging. En sælger videresender et tilbud til en kollega via chat. En læge deler en klinisk rapport med en kollega ad samme vej. Ingen tænker to gange over det. Det er normalt. Det er praktisk. Det er det, der gøres hver dag på ethvert kontor i enhver by i Europa.

Men det dokument er i mange tilfælde lige rejst til en server i USA. Det er blevet gemt – selvom det er midlertidigt, selvom det er "krypteret ved hvile" – i en sky, som hverken den professionelle eller klienten kontrollerer. Det har passeret systemer, der teknisk kan indeksere metadata knyttet til indholdet. Og den europæiske databeskyttelsesforordning har noget ret klart at sige om det.

Hvad lovgivningen kræver

GDPR – og i forlængelse heraf retspraksis fra Den Europæiske Unions Domstol (navnlig Schrems II-dommen, C-311/18, fra 2020) – fastslår, at personoplysninger om europæiske borgere skal være passende beskyttet. Hvis disse data forlader Det Europæiske Økonomiske Samarbejdsområde, skal den dataansvarlige garantere, at modtageren tilbyder et beskyttelseniveau, der er "væsentligt svarende" til det europæiske. I praksis betyder det, at afsendelse af klientdata via tjenester, hvis servere er under amerikansk jurisdiktion, uden at have foretaget en konsekvensanalyse og implementeret supplerende sikkerhedsforanstaltninger – standardkontraktbestemmelser, yderligere tekniske foranstaltninger såsom verificerbar kryptering osv. – kan udgøre en overtrædelse af forordningen. Også selvom ingen har sagt noget endnu.

Og det drejer sig ikke kun om indholdet af beskederne. Metadata – hvem der sender hvad til hvem, hvornår, hvor ofte, hvorfra – er også personoplysninger ifølge reglerne, ifølge gentagne fortolkninger fra Det Europæiske Databeskyttelsesråd. En tjeneste, der indsamler metadata fra en brugers professionelle kommunikation, behandler personoplysninger om denne brugers klienter, uden at disse har kendskab til det eller har givet samtykke til en sådan behandling.

Den gængse tankegang – "jeg bruger kun appen til at skrive; appen er ikke en dataleverandør for min klient" – er juridisk forkert. Hvis klientens data passerer gennem en tredjeparts infrastruktur, behandler denne tredjepart disse data. Og hvis vedkommende behandler dem, skal der være et retsgrundlag, en databehandleraftale og passende garantier.

Hvem er ansvarlig

Spørgsmålet om, hvem der bærer det juridiske ansvar, er ikke akademisk. GDPR skelner mellem den *dataansvarlige* (den, der beslutter, hvilke data der skal behandles og til hvad) og *databehandleren* (den, der gør det materielt på vegne af den ansvarlige). Den professionelle, der sender klientdokumenter, er den ansvarlige. Udbyderen af messaging-appen er i mange tilfælde faktuelt databehandler. Uden en databehandleraftale – og uden de fleste af de bestemmelser, som en sådan aftale bør indeholde – har den ansvarlige ikke opfyldt sin forpligtelse.

Den milde fortolkning er: "de fleste professionelle ved ikke dette". Den strenge fortolkning er: "ukendskab fritager ikke for ansvar". Og fortolkningen hos enhver specialiseret advokat i databeskyttelse, der rådføres herom, er generelt den strenge.

For hvem dette konkret er vigtigt

For enhver professionel eller virksomhed, der håndterer, selv lejlighedsvis, personoplysninger om tredjeparter:

- Advokater, der modtager dokumentation fra klienter (kontrakter, sagsanlæg, erklæringer, formuerapporter).
- Læger og andet sundhedspersonale, der deler helbredsoplysninger – der betragtes som *særlige kategorier* ifølge art. 9 GDPR med skærpede regler –.
- Skatterådgivere og administrative konsulenter, der håndterer identifikations-, skatte- og bankdata.
- HR-afdelinger, der administrerer arbejds- og personaledokumentation for medarbejdere.
- Sælgere, der modtager kontaktoplysninger og ofte følsomme forretningsoplysninger fra emner og kunder.

I alle tilfælde er oplysningerne beskyttet af GDPR. I alle tilfælde går disse oplysninger i daglig praksis via kanaler, hvis jurisdiktion ikke tillader, at de erklæres "væsentligt svarende" til den europæiske ramme uden yderligere sikkerhedsforanstaltninger. Ikke af onde hensigter. Af vane. Og på grund af en teknologisk infrastruktur, der har prioriteret bekvemmelighed over overholdelse i femten år.

Argumentet "alle gør det"

Det er klogt at foregribe den hyppigste indvending: "hvis alle gør det, kan det ikke være et reelt problem". Det er et fuldt ud forståeligt argument, og det har juridisk set ingen vægt. Det faktum, at en praksis er udbredt, gør den ikke i overensstemmelse med forordningen. Datatilsynet har i de seneste år sanktioneret flere virksomheder netop for messaging-brug, der virkede harmløs indtil inspektionstidspunktet.

Den nuværende operative virkelighed er, at risikoen i form af sandsynlighed er lav – det er meget sjældent, at et tilsyn auditerer de specifikke messaging-værktøjer i et mellemstort kontor – men høj i form af konsekvens, hvis den materialiserer sig. Det er en risiko, som de fleste påtager sig uden at vide, at de påtager sig den. Det vil sige uden at have vurderet, om det anvendte værktøj er på linje med den dataansvarliges juridiske ansvar.

Det digitale spor er retroaktivt

Der er et andet argument, næsten symmetrisk til det foregående, som vi bør foregribe: *"hvis dette var et alvorligt problem, var myndighederne allerede begyndt at inspicere det"*. Den nuværende observerede virkelighed giver det overfladisk ret. Inspektioner for forkert brug af messaging i små virksomheder og især hos selvstændige er i dag næsten ikke-eksisterende – ikke fordi adfærden er tilladt, men fordi myndighederne i Danmark og i store dele af EU mangler de nødvendige menneskelige ressourcer til at auditere millioner af forpligtede parter.

Det er det, den i dag observerede praksis antyder. Det er ikke det, det næste årti antyder. To faktorer konvergerer for at ændre balancen inden for relativt korte tidsrammer.

For det første: Det digitale spor er retroaktivt. Enhver besked sendt via en applikation med en central server forbliver registreret – i det mindste i metadata – i en infrastruktur, der består. Det, der blev sendt for seks måneder siden, er teknisk set stadig auditerbart i dag. Det, der sendes i dag, vil stadig være auditerbart om fem

år. Fraværet af en nuværende inspektion er ikke en garanti for fraværet af en fremtidig inspektion. Det er en udsættelse af vurderingen, ikke en fritagelse.

For det andet: Den administrative inspektionskapacitet vil vokse accelereret. Introduktionen af værktøjer med kunstig intelligens i inspektionsprocesser eliminerer den menneskelige flaskehals, som indtil nu – reelt, ikke juridisk – har beskyttet små virksomheder og selvstændige. Et system, der er i stand til at krydstjekke massive metadata, skatteopgørelser, erhvervsregistre og meddelelsespligter om brud, kræver ikke inspektører: Det kræver adgang. Og adgangen via anmodninger til udbydere med juridisk tilstedeværelse i EU er fuldt ud gennemførlig under det nuværende lovgrundlag.

Hertil kommer en mindre teknisk, men lige så afgørende faktor: De europæiske stater er i en proces med vedvarende stigende gældsætning og har, næsten uden undtagelse, brug for at udvide deres skattegrundlag. Den administrative sanktion som følge af manglende overholdelse af GDPR er i rent fiskale termer en voksende og politisk bekvem indtægtskilde. Det er ikke gætterier: Det er en observerbar tendens i de europæiske datatilsyns årsrapporter, hvor det samlede volumen af sanktioner har været stigende i flere på hinanden følgende regnskabsår.

Den operative konklusion for den dataansvarlige er ikke alarmistisk, men nøgtern: **Beslutningen om, hvordan kommunikation med klienter håndteres i dag, vurderes i forhold til inspektionskapaciteten i det år, hvor inspektionen finder sted, ikke i forhold til den nuværende.** Og denne kapacitet vil inden for en rimelig tidshorisont være væsentligt anderledes end i dag. Den, der begynder at gøre tingene rigtigt i dag, vil ikke kun være i orden fra i dag: Det spor, der genereres fra dette øjeblik, vil være i overensstemmelse med reglerne, og det beskytter retroaktivt det forløb, der kommer. Den, der fortsætter som hidtil, vil akkumulere et auditerbart spor, hvis overholdelse vil blive vurderet i forhold til standarderne – og ressourcerne – i de kommende år.

Hvad ændrer sig med en anden arkitektur

Der findes tekniske alternativer, hvor data ikke gemmes i tredjeparts infrastruktur, men i stedet rejser direkte fra afsenderens enhed til modtagerens. I den arkitektur afhænger overholdelse af GDPR med hensyn til internationale overførsler ikke af standardkontraktbestemmelser, eller af udbyderens gode vilje eller fremtidige audits. Det afhænger af, at der *ikke er nogen overførsel*. Og det, der ikke eksisterer, kan ikke overtrædes.

Dette er ikke en eksklusiv løsning eller den eneste mulige. Men den er strukturelt anderledes, og overholdelse af reglerne ophører med at være et proceduremæssigt bilag og bliver en direkte konsekvens af designet. For en professionel, der tager sit ansvar som dataansvarlig alvorligt, gør denne forskel en forskel.

Næste udgave af Cuadernos vil i detaljer analysere Schrems II-dommen og dens praktiske konsekvenser for små og mellemstore virksomheder, der er afhængige af amerikanske cloud-tjenester, fem år efter dens offentliggørelse.

Kilder og lovgrundlag

- Forordning (EU) 2016/679 (GDPR), især kapitel V om internationale overførsler.
- EU-Domstolen C-311/18 ("Schrems II"), 16. juli 2020.
- EDPB – Anbefalinger 01/2020 om foranstaltninger, der supplerer overførselsinstrumenterne.
- Datatilsynet – Årsrapporter med eksempler på sanktioner for forkert brug af instant messaging i professionelle miljøer.

← ForrigeTavshedspligten i den digitale tidsalderNæste →Når der ikke er nogen imellem

Seneste læsning

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Tag denne artikel med dig, hvor du har brug for den.

↓ Markdown ↓ Almindelig tekst ↓ PDF

Filen downloades til din enhed. Derfra kan du gemme den, importere den til Solo2 eller dele den, hvor du vil. Cuadernos beslutter ikke destinationen for dig.

Laksegl · SHA-256 5b1db98b223608182baad71fea532b87dce07a894508303922d0cd75c23ffaa3

Cuadernos Lacre · En udgivelse fra Menzuri Gestión S.L. ·
skrevet af R.Eugenio · redigeret af holdet bag Solo2.