Refleksion · 16. maj 2026

← Forrige·Næste →

Tavshedspligten i den digitale tidsalder

Når kommunikationen mellem den professionelle og klienten foregår via en teknisk uegnet kanal, brydes hemmeligheden ikke på dagen for lækagen. Den blev brudt længe før, i det øjeblik værktøjet blev valgt.

Et problem, som næsten ingen ser

En advokat modtager et følsomt dokument fra en klient på sin telefon. En læge drøfter en delikat diagnose med en kollega. En psykolog koordinerer behandlingen af en patient med en psykiater. En skatterådgiver sender data for en erklæring, der afventer revision. Alle gør det via instant messaging. Og næsten ingen stopper op for at tænke over, hvor de beskeder reelt ender.

Svaret er i de fleste tilfælde det samme: på en server, som den professionelle ikke kontrollerer, i et land, hvis lovgivning vedkommende ikke nødvendigvis kender, administreret af en virksomhed, hvis forretningsmodel – i direkte økonomiske termer – er at akkumulere data. Beskeden kan være krypteret i transit. Men når den først når serveren, er det en kopi gemt i en tredjeparts infrastruktur, underlagt denne tredjeparts operative, juridiske og kommercielle beslutninger. Ikke den professionelles.

Hvad lovgivningen siger

Den europæiske databeskyttelsesforordning er entydig i sin artikel 32: Enhver, der behandler personoplysninger, skal gennemføre "passende" tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risikoen. Foranstaltningernes tilstrækkelighed vurderes ikke ud fra, "hvad appen siger, den gør", men ud fra den reelle risiko. Hvis klientdata ender på en server, hvis jurisdiktion ikke garanterer et beskyttelsesniveau svarende til Det Europæiske Økonomiske Samarbejdsområdes, påtager den dataansvarlige – det vil sige den professionelle – sig en risiko, som vedkommende sandsynligvis ikke er helt klar over.

Og det er ikke kun GDPR. Tavshedspligten, der er reguleret specifikt for advokater, læger, psykologer, revisorer, journalister og andre, kræver, at kommunikationen med klienten er fortrolig. Ikke "så fortrolig som muligt". Fortrolig uden forbehold. Hvis den anvendte tekniske kanal ikke kan garantere dette, påtager den professionelle sig en risiko, som vedkommendes fagetik ikke tillader.

Paradokset er, at risikoen er usynlig. Ingen auditerer kontorets messaging. Ingen beder om databehandleraftalen fra chatudbyderen. Risikoen dukker først op, når det er for sent: en lækage, et offentliggjort brud, en retskendelse fuldbyrdet på et andet kontinent uden meddelelse til brugeren.

Hvad en professionel har brug for teknisk

Hvad en person med tavshedspligt har brug for, er faktisk overraskende enkelt set fra et kravsperspektiv:

- En kanal, hvor beskederne går direkte fra afsenderens enhed til modtagerens, uden at passere en mellemliggende server, der gemmer kopier.
- En infrastruktur, hvis jurisdiktion og politikker er på linje med GDPR ved design, ikke ved erklæring.

- En måde at identificere sig over for samtalepartneren uden at skulle udlevere professionelle kontakter (klientnavne, telefonnumre, kontaktbog) til en tredjepart.
- Et verificerbart system – ikke baseret på udbyderens ord – til at bekræfte, at beskeden nåede den rigtige person.

Det er ikke en krævende liste. Det er faktisk det, man tog for givet i præ-digital professionel kommunikation. Et anbefalet brev opfyldte alle disse kriterier. Et telefonopkald fra kontorets omstilling til klientens ligeledes. Det mærkelige er ikke, at disse garantier kræves i dag: Det mærkelige er, at de er gået tabt ved overgangen til den digitale kanal, uden at nogen lagde mærke til det.

Forskellen mellem at kryptere og ikke at gemme

Der er en nyttig metafor. At kryptere en besked og gemme den på en server svarer til at lægge et dokument i en pengeskab og efterlade pengeskabet hjemme hos en fremmed. Pengeskabet er godt. Dokumentet kan i princippet ikke læses. Men dokumentet *er stadig hjemme hos en anden*. Og denne anden kan modtage en retskendelse, blive udsat for et computerangreb, ændre sine servicevilkår, blive købt af en anden virksomhed med en anden etik eller forsvinde i morgen.

Det strukturelle alternativ – ikke proceduremæssigt, ikke baseret på tillid – er, at dokumentet aldrig forlader kontoret. At det rejser direkte fra den professionelles bord til klientens bord uden nogen form for mellemmand. Det er det, punkt-til-punkt kommunikation mellem enheder gør teknisk: Det eliminerer mellemmanden. Ikke at mellemmanden er ond. Det er bare det, at for så vidt angår tavshedspligten, er mellemmanden *unødvendig*. Og det unødvendige skal i ethvert system, der ønsker at være sikkert, elimineres af princip.

Spørgsmålet om ansvar

I sidste ende er spørgsmålet, som enhver professionel med tavshedspligt bør kunne svare på med et rungende ja, følgende:

> Hvis en samtale med en af mine klienter i morgen bliver lækket, og en domstol eller en faggruppe spørger mig, hvordan jeg håndterer fortrolighed, kan jeg så teknisk bevise, at den kanal, jeg brugte, ikke gemmer kopier i tredjeparts infrastruktur? Kan jeg bevise, at dataene aldrig forlod enhederne hos de to personer, der deltog i samtalen? Kan jeg bevise, uden at være afhængig af et firmas ord fra et andet kontinent, at fortroligheden var garanteret af arkitekturen og ikke af et løfte?

Hvis svaret er nej, er problemet ikke værktøjet i sig selv. Problemet er, at man har delegeret et ansvar til et værktøj, som værktøjet ikke var designet til at understøtte. Det svarer til at lægge fortrolige sagsakter i en gennemsigtig konvolut og stole på, at postbuddet ikke kigger.

Det værktøj, en professionel vælger til at kommunikere med sine klienter, siger meget om, hvordan vedkommende værdsætter deres tillid. Der findes værktøjer designet til, at denne tillid ikke afhænger af løfter, men af arkitekturen. Og der findes værktøjer, der ikke gør. At kende forskellen er en del af arbejdet.

Citeret lovgrundlag

- Forordning (EU) 2016/679 (GDPR), især art. 5, 25 (databeskyttelse gennem design) og 32 (behandlingssikkerhed).
- Retsplejeloven § 170 (Vidnefritagelse for personer med tavshedspligt).
- Straffeloven § 152 (Brud på tavshedspligt).
- Sundhedsloven § 40 (Tavshedspligt for sundhedspersoner).

← ForrigeKryptering er ikke det samme som privatliv: Hvad metadata fortæller om digNæste →GDPR og professionel messaging: Hvorfor de fleste overtræder reglerne uden at vide det

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 899528adb87f387ee70b29812bcc9d4c3e042e8b12f1e46ea70e8087fba5f53b

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