Refleksjon · 16. mai 2026

← Forrige·Neste →

Taushetsplikten i den digitale tidsalderen

Når kommunikasjonen mellom den profesjonelle og klienten foregår via en teknisk uegnet kanal, brytes ikke hemmeligheten den dagen lekkasjen skjer. Den ble brutt lenge før, i det øyeblikket verktøyet ble valgt.

Et problem nesten ingen ser

En advokat mottar et sensitivt dokument fra en klient på telefonen sin. En lege diskuterer en delikat diagnose med en kollega. En psykolog koordinerer behandlingen av en pasient med en psykiater. En skatterådgiver sender data for en erklæring som venter på revisjon. Alle gjør det via instant messaging. Og nesten ingen stopper opp for å tenke på hvor disse meldingene egentlig havner.

Svaret er i de fleste tilfeller det samme: på en server som yrkesutøveren ikke kontrollerer, i et land hvis lovgivning vedkommende ikke nødvendigvis kjenner, administrert av et selskap hvis forretningsmodell er – i direkte økonomiske termer – å akkumulere data. Meldingen kan være kryptert under transport. Men når den først når serveren, er det en kopi lagret i en tredjeparts infrastruktur, underlagt denne tredjepartens operative, juridiske og kommersielle beslutninger. Ikke yrkesutøverens.

Hva lovgivningen sier

Den europeiske personvernforordningen er utvetydig i sin artikkel 32: enhver som behandler personopplysninger må gjennomføre "egnede" tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er tilpasset risikoen. Tiltakenes egnethet vurderes ikke ut fra "hva appen sier den gjør", men ut fra den reelle risikoen. Hvis klientdata havner på en server hvis jurisdiktion ikke garanterer et beskyttelsesnivå tilsvarende Det europeiske økonomiske samarbeidsområdes, påtar den behandlingsansvarlige – det vil si yrkesutøveren – seg en risiko vedkommende sannsynligvis ikke er helt klar over.

Og det er ikke bare GDPR. Taushetsplikten, som er spesifikt regulert for advokater, leger, psykologer, revisorer, journalister og andre, krever at kommunikasjonen med klienten er konfidensiell. Ikke "konfidensiell så langt det er mulig". Konfidensiell uten forbehold. Hvis den tekniske kanalen som brukes ikke kan garantere dette, påtar yrkesutøveren seg en risiko som vedkommendes yrkesetikk ikke tillater.

Paradokset er at risikoen er usynlig. Ingen auditerer kontorets messaging. Ingen ber om databehandleravtalen fra chat-leverandøren. Risikoen dukker først opp når det er for sent: en lekkasje, et publisert brudd, en rettskjennelse fullbyrdet på et annet kontinent uten varsel til brukeren.

Hva en yrkesutøver trenger teknisk

Hva en person med taushetsplikt trenger er egentlig overraskende enkelt sett fra et kravsperspektiv:

- En kanal der meldingene går direkte fra senderens enhet til mottakerens, uten å passere en mellomliggende server som lagrer kopier.
- En infrastruktur hvis jurisdiksjon og retningslinjer er på linje med GDPR ved design, ikke ved erklæring.

- En måte å identifisere seg for samtalepartneren uten å måtte utlevere profesjonelle kontakter (klientnavn, telefonnumre, kontaktbok) til en tredjepart.
- Et verifiserbart system – ikke basert på leverandørens ord – for å bekrefte at meldingen nådde riktig person.

Det er ingen krevende liste. Det er faktisk det som ble tatt for gitt i den før-digitale yrkeskommunikasjonen. Et rekommandert brev oppfylte alle disse kriteriene. En telefonsamtale fra kontorets sentralbord til klientens likeså. Det merkelige er ikke at disse garantiene kreves i dag: det merkelige er at de har gått tapt i overgangen til den digitale kanalen, uten at noen merket det.

Forskjellen mellom å kryptere og å ikke lagre

Det finnes en nyttig metafor. Å kryptere en melding og lagre den på en server tilsvarer å legge et dokument i en safe og etterlate safen hjemme hos en fremmed. Safen er god. Dokumentet kan i prinsippet ikke leses. Men dokumentet *er fortsatt hjemme hos en annen*. Og denne andre kan motta en rettskjennelse, bli utsatt for et dataangrep, endre sine tjenestevilkår, bli kjøpt opp av et annet selskap med en annen etikk, eller forsvinne i morgen.

Det strukturelle alternativet – ikke prosedyremessig, ikke basert på tillit – er at dokumentet aldri forlater kontoret. At det reiser direkte fra yrkesutøverens bord til klientens bord, uten noen mellommann. Det er det punkt-til-punkt kommunikasjon mellom enheter gjør teknisk: det eliminerer mellommannen. Ikke at mellommannen er ond. Det er bare det at for taushetspliktens del er mellommannen *unødvendig*. Og det unødvendige må, i ethvert system som ønsker å være sikkert, elimineres av prinsipp.

Spørsmålet om ansvar

Til syvende og sist er spørsmålet som enhver yrkesutøver med taushetsplikt bør kunne svare på med et rungende ja, følgende:

> Hvis en samtale med en av mine klienter i morgen blir lekket, og en domstol eller et yrkesforbund spør meg hvordan jeg håndterer konfidensialitet, kan jeg da teknisk bevise at kanalen jeg brukte ikke lagrer kopier i tredjeparts infrastruktur? Kan jeg bevise at dataene aldri forlot enhetene til de to personene som deltok i samtalen? Kan jeg bevise, uten å stole på et firmas ord fra et annet kontinent, at konfidensialiteten var garantert av arkitekturen og ikke av et løfte?

Hvis svaret er nei, er problemet ikke verktøyet i seg selv. Problemet er at man har delegert et ansvar til et verktøy som verktøyet ikke var designet for å håndtere. Det er som å legge konfidensielle saksmapper i en gjennomsiktig konvolutt og stole på at postbudet ikke ser.

Verktøyet en yrkesutøver velger for å kommunisere med sine klienter sier mye om hvordan vedkommende verdsetter deres tillit. Det finnes verktøy designet for at denne tilliten ikke skal avhenge av løfter, men av arkitekturen. Og det finnes verktøy som ikke er det. Å kjenne forskjellen er en del av jobben.

Sitert regelverk

- Forordning (EU) 2016/679 (GDPR), spesielt art. 5, 25 (innebygd personvern) og 32 (behandlingssikkerhet).
- Norsk lovgivning om taushetsplikt (bl.a. advokatforskriften kapittel 12, helsepersonelloven § 21).
- Straffeloven § 209 (Brudd på taushetsplikt).
- Regler for god advokatskikk om taushetsplikt og profesjonshemmelighet.

← ForrigeKryptering er ikke det samme som personvern: hva metadata forteller om degNeste →GDPR og profesjonell messaging: hvorfor de fleste bryter reglene uten å vite det

Siste lesninger

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ta med deg denne artikkelen dit du trenger den.

↓ Markdown ↓ Klartekst ↓ PDF

Filen lastes ned til enheten din. Derfra kan du lagre den, importere den til Solo2 eller dele den hvor du vil. Cuadernos bestemmer ikke destinasjonen for deg.

Lakksegl · SHA-256 1a62bf4cd1f8c04a1ea1dbc4a3874d53b8fb02bf9edc4db7c86c8e784cf37d8a

Cuadernos Lacre · En utgivelse fra Menzuri Gestión S.L. ·
skrevet av R.Eugenio · redigert av teamet bak Solo2.

Dette nettstedet bruker ikke informasjonskapsler (cookies) og laster ikke inn ressurser fra tredjeparter. Det bruker en selvhostet anonym besøksteller (Umami på vår europeiske server) og det minimum av JavaScript som er nødvendig for ditt valg av lyst/mørkt tema. Ingen trackere, ingen profilering, ingen datadeling. Hvis du vil følge oss: RSS.