Професійна таємниця в цифрову епоху

Коли спілкування між професіоналом та його клієнтом відбувається через технічно невідповідний канал, таємниця не порушується в день витоку. Вона була порушена набагато раніше, в момент вибору інструменту.

Проблема, яку майже ніхто не бачить

Адвокат отримує на свій телефон конфіденційний документ від клієнта. Лікар обговорює з колегою делікатний діагноз. Психолог координує з психіатром лікування пацієнта. Податковий консультант надсилає дані декларації, що очікує на перевірку. Всі роблять це через месенджери. І майже ніхто не зупиняється, щоб подумати, де ці повідомлення насправді опиняються.

Відповідь у більшості випадків однакова: на сервері, який професіонал не контролює, в країні, законодавства якої він не обов'язково знає, під керуванням компанії, бізнес-моделлю якої є — у прямих економічних термінах — накопичення даних. Повідомлення може бути зашифрованим під час передачі. Але як тільки воно потрапляє на сервер, воно стає копією, що зберігається в інфраструктурі третьої сторони, підпадаючи під операційні, юридичні та комерційні рішення цієї третьої сторони. Не професіонала.

Що каже законодавство

Європейський загальний регламент про захист даних однозначний у своїй статті 32: кожен, хто обробляє персональні дані, повинен впровадити «відповідні» технічні та організаційні заходи для забезпечення рівня безпеки, що відповідає ризику. Відповідність заходів оцінюється не за тим, «що додаток каже, що він робить», а за реальним ризиком. Якщо дані клієнта потрапляють на сервер, юрисдикція якого не гарантує рівень захисту, еквівалентний рівню Європейського економічного простору, контролер даних — тобто професіонал — бере на себе ризик, про який він, ймовірно, не зовсім усвідомлює.

І це не лише GDPR. Професійна таємниця, яка регулюється спеціально для адвокатів, лікарів, психологів, аудиторів, журналістів та інших, вимагає, щоб спілкування з клієнтом було конфіденційним. Не «якомога конфіденційнішим». Конфіденційним без застережень. Якщо використовуваний технічний канал не може цього гарантувати, професіонал бере на себе ризик, який деонтологія його професії не дозволяє приймати.

Парадокс у тому, що ризик невидимий. Ніхто не проводить аудит месенджерів в офісі. Ніхто не запитує договір про обробку даних у постачальника чату. Ризик виявляється лише тоді, коли вже занадто пізно: витік, опублікований злам, судовий наказ, виконаний на іншому континенті без повідомлення користувача.

Що технічно потрібно професіоналу

Те, що потрібно особі, зобов'язаній зберігати таємницю, насправді дивовижно просто з точки зору вимог:

- Канал, де повідомлення йдуть безпосередньо з пристрою відправника на пристрій одержувача, без проходження через проміжний сервер, який зберігає копії.
- Інфраструктура, юрисдикція та політики якої узгоджені з GDPR за дизайном, а не за декларацією.
- Спосіб ідентифікації з співрозмовником без необхідності передавати професійні контакти (імена клієнтів, номери телефонів, адресну книгу) третій стороні.
- Система, яку можна перевірити — не на основі слів постачальника — щоб підтвердити, що повідомлення дійшло до потрібної людини.

Це не є вимогливим списком. Це насправді те, що вважалося само собою зрозумілим у професійній комунікації доцифрової епохи. Рекомендований лист відповідав усім цим критеріям. Телефонний дзвінок з комутатора офісу до комутатора клієнта — також. Дивно не те, що ці гарантії вимагаються сьогодні: дивно те, що вони були втрачені при переході до цифрового каналу, без того, щоб хтось це помітив.

Різниця між шифруванням та незбереженням

Є корисна метафора. Шифрувати повідомлення та зберігати його на сервері еквівалентно тому, щоб покласти документ у сейф і залишити сейф у будинку незнайомця. Сейф хороший. Документ в принципі неможливо прочитати. Але документ *все ще знаходиться в чужому будинку*. І той хтось може отримати судовий наказ, зазнати кібератаки, змінити свої умови обслуговування, бути купленим іншою компанією з іншою етикою або може зникнути завтра.

Структурною альтернативою — не процедурною, не на основі довіри — є те, щоб документ ніколи не залишав офіс. Щоб він подорожував безпосередньо з робочого столу професіонала на робочий стіл клієнта без будь-якого посередника. Це те, що технічно робить комунікація «точка-точка» між пристроями: вона усуває посередника. Не те щоб посередник був поганим. Просто у випадку професійної таємниці посередник *непотрібний*. А те, що непотрібне, в будь-якій системі, яка прагне бути безпечною, має бути усунуто за принципом.

Питання відповідальності

Зрештою, питання, на яке кожен професіонал із зобов'язанням зберігати таємницю повинен мати змогу відповісти рішучим «так», наступне:

> Якщо завтра станеться витік розмови з одним із моїх клієнтів, і суд або професійна палата запитають мене, як я керую конфіденційністю, чи зможу я технічно довести, що канал, який я використовував, не зберігає копії в інфраструктурі третіх сторін? Чи можу я довести, що дані ніколи не залишали пристроїв двох осіб, які брали участь у розмові? Чи можу я, не покладаючись на слова компанії з іншого континенту, довести, що конфіденційність була гарантована архітектурою, а не обіцянкою?

Якщо відповідь «ні», проблема не в конкретному інструменті. Проблема в тому, що інструменту було делеговано відповідальність, для підтримки якої інструмент не був спроектований. Це як покласти конфіденційні файли в прозорий конверт і вірити, що листоноша не зазирне всередину.

Інструмент, який професіонал обирає для спілкування зі своїми клієнтами, багато говорить про те, як він цінує їхню довіру. Є інструменти, спроектовані так, щоб ця довіра не залежала від обіцянок, а від архітектури. І є інструменти, які не є такими. Знання різниці — частина роботи.

Цитована нормативна база

- Регламент (ЄС) 2016/679 (GDPR), зокрема ст. 5, 25 (захист даних на етапі проектування) та 32 (безпека обробки).

- Українське законодавство про професійну таємницю (напр., Закон про адвокатуру та адвокатську діяльність ст. 22, Основи законодавства про охорону здоров'я ст. 39-1).
- Кримінальний кодекс України, ст. 145 (Незаконне розголошення лікарської таємниці) та ст. 397.
- Етичні кодекси професійних організацій щодо конфіденційності та професійної таємниці.

← ПопереднійШифрування не означає конфіденційність: що метадані говорять про васНаступний
→GDPR та професійний обмін повідомленнями: чому більшість порушує правила, не знаючи про це

Останні матеріали

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Візьміть цю статтю з собою куди завгодно.

↓ Markdown ↓ Звичайний текст ↓ PDF

Файл буде завантажено на ваш пристрій. Звідти ви можете зберегти його, імпортувати в Solo2 або поділитися ним де завгодно. Cuadernos не вирішує місце призначення за вас.

Сургучна печатка · SHA-256 f971cc54ed2eef80cce1894909d57c3d0b5b215c0688f3c804198dc97fcf2b99

Cuadernos Lacre · Видання Menzuri Gestión S.L. ·
автор R.Eugenio · під редакцією команди Solo2.