Размисъл · 16 май 2026 г.

← Предишна·Следваща →

Професионалната тайна в цифровата ера

Когато комуникацията между професионалиста и неговия клиент се осъществява през технически неподходящ канал, тайната не се нарушава в деня на изтичането. Тя е била нарушена много по-рано, в момента на избора на инструмента.

Проблем, който почти никой не вижда

Адвокат получава на телефона си поверителен документ от клиент. Лекар обсъжда с колега деликатна диагноза. Психолог координира с психиатър лечението на пациент. Данъчен консултант изпраща данните от декларация, чакаща ревизия. Всички го правят чрез незабавни съобщения. И почти никой не се спира да помисли къде всъщност попадат тези съобщения.

Отговорът в повечето случаи е един и същ: на сървър, който професионалистът не контролира, в страна, чието законодателство не е задължително да познава, управляван от компания, чийто бизнес модел е – в преки икономически термини – натрупването на данни. Съобщението може да е криптирано при предаването. Но след като достигне сървъра, то е копие, съхранявано в инфраструктурата на трета страна, подвластно на оперативните, правните и търговските решения на тази трета страна. Не на професионалиста.

Какво казва законодателството

Европейският общ регламент относно защитата на данните е недвусмислен в своя член 32: всеки, който обработва лични данни, трябва да приложи „подходящи“ технически и организационни мерки, за да гарантира ниво на сигурност, съответстващо на риска. Подходящността на мерките не се измерва по това „какво приложението казва, че прави“, а по реалния риск. Ако клиентските данни попаднат на сървър, чиято юрисдикция не гарантира ниво на защита, еквивалентно на това в Европейското икономическо пространство, администраторът – тоест професионалистът – поема риск, за който вероятно не е напълно наясно.

И това не е само GDPR. Професионалната тайна, регулирана специално за адвокати, лекари, психолози, одитори, журналисти и други, изисква комуникацията с клиента да бъде поверителна. Не „възможно най-поверителна“. Поверителна без уговорки. Ако използваният технически канал не може да гарантира това, професионалистът поема риск, който деонтологията на неговата професия не му позволява да поеме.

Парадоксът е, че рискът е невидим. Никой не одитира съобщенията в офиса. Никой не иска договора за обработка на данни от доставчика на чат. Рискът излиза наяве едва когато е прекалено късно: изтичане, публикуван пробив в сигурността, съдебно разпореждане, изпълнено на друг континент без уведомяване на потребителя.

Какво технически е необходимо на професионалиста

Това, от което се нуждае лице, обвързано с професионална тайна, всъщност е изненадващо просто от гледна точка на изискванията:

- Канал, в който съобщенията отиват директно от устройството на изпращача до устройството на получателя, без да минават през междинен сървър, който съхранява копия.
- Инфраструктура, чиято юрисдикция и политики са съобразени с GDPR чрез дизайн, а не чрез декларация.
- Начин за идентифициране със събеседника, без да е необходимо да се предават професионални контакти (имена на клиенти, телефонни номера, адресна книга) на трета страна.
- Проверяема система – не основана на думите на доставчика – за потвърждаване, че съобщението е достигнато до правилния човек.

Това не е взискателен списък. Това всъщност е това, което се приемаше за даденост в предцифровата професионална комуникация. Препоръчаното писмо отговаряше на всички тези критерии. Телефонното обаждане от централата на офиса до тази на клиента – също. Странното не е, че тези гаранции се изискват днес: странното е, че са загубени при прехода към цифровия канал, без никой да забележи.

Разликата между криптиране и несъхраняване

Има полезна метафора. Криптирането на съобщение и съхраняването му на сървър е еквивалентно на поставянето на документ в сейф и оставянето на сейфа в дома на непознат. Сейфът е добър. Документът по принцип не може да бъде прочетен. Но документът *все още се намира в чужд дом*. И този някой може да получи съдебно разпореждане, да претърпи кибератака, да промени условията си за ползване, да бъде купен от друга компания с друга етика или да изчезне утре.

Структурната алтернатива – не процедурна, не основана на доверие – е документът никога да не напуска офиса. Да пътува директно от бюрото на професионалиста до бюрото на клиента без никакъв посредник. Това е, което технически прави комуникацията „точка до точка“ между устройствата: елиминира посредника. Не че посредникът е лош. Просто в случая с професионалната тайна посредникът е *излишен*. А излишното във всяка система, която се стреми да бъде сигурна, трябва да бъде елиминирано по принцип.

Въпросът за отговорността

В крайна сметка въпросът, на който всеки професионалист със задължение за пазене на тайна трябва да може да отговори с категорично „да“, е следният:

> Ако утре изтече разговор с някой от моите клиенти и съд или професионална палата ме попитат как управлявам поверителността, мога ли технически да докажа, че каналът, който използвах, не съхранява копия в инфраструктурата на трети страни? Мога ли да докажа, че данните никога не са напускали устройствата на двамата души, участвали в разговора? Мога ли, без да разчитам на думата на компания от друг континент, да докажа, че поверителността е била гарантирана от архитектурата, а не от обещание?

Ако отговорът е не, проблемът не е в конкретния инструмент. Проблемът е, че на един инструмент е делегирана отговорност, за чиято поддръжка инструментът не е бил проектиран. Това е като да поставите поверителни папки в прозрачен плик и да се надявате, че пощальонът няма да погледне.

Инструментът, който професионалистът избира за комуникация с клиентите си, казва много за това как той цени тяхното доверие. Има инструменти, проектирани така, че това доверие да не зависи от обещания, а от архитектурата. И има инструменти, които не са такива. Познаването на разликата е част от работата.

Цитирана нормативна рамка

- Регламент (ЕС) 2016/679 (GDPR), по-специално чл. 5, 25 (защита на данните на етапа на проектирането) и 32 (сигурност на обработването).
- Българско законодателство относно професионалната тайна (напр. Закон за адвокатурата чл. 33, Закон за здравето чл. 27).
- Наказателен кодекс, чл. 145 (нарушаване на тайна).
- Етични кодекси на професионалните организации относно поверителността и професионалната тайна.

← ПредишнаКриптирането не е поверителност: какво казват метаданните за васСледваща →GDPR и професионалните съобщения: защо повечето хора нарушават правилата, без да го знаят

Скорошни четива

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Вземете тази статия със себе си навсякъде, където ви е необходима.

↓ Markdown ↓ Обикновен текст ↓ PDF

Файлът ще бъде изтеглен на вашето устройство. Оттам можете да го запазите, импортирате в Solo2 или споделите където пожелаете. Cuadernos не решава дестинацията вместо вас.

Восъчен печат · SHA-256 64cd257ed2961000a30387bf7aee7243d2884c354025c046c9a3edefb5d55537

Cuadernos Lacre · Публикация на Menzuri Gestión S.L. ·
написана от R.Eugenio · редактирана от екипа на Solo2.