Размышление · 16 мая 2026 г.

← Предыдущий·Следующий →

Профессиональная тайна в цифровую эпоху

Когда общение между профессионалом и его клиентом происходит через технически неподходящий канал, тайна не нарушается в день утечки. Она была нарушена гораздо раньше, в момент выбора инструмента.

Проблема, которую почти никто не видит

Адвокат получает на свой телефон конфиденциальный документ от клиента. Врач обсуждает с коллегой деликатный диагноз. Психолог координирует с психиатром лечение пациента. Налоговый консультант отправляет данные декларации, ожидающей ревизии. Все делают это через мессенджеры. И почти никто не останавливается, чтобы подумать, где эти сообщения на самом деле оказываются.

Ответ в большинстве случаев одинаков: на сервере, который профессионал не контролирует, в стране, законодательства которой он не обязательно знает, под управлением компании, бизнес-моделью которой является — в прямых экономических терминах — накопление данных. Сообщение может быть зашифрованным во время передачи. Но как только оно попадает на сервер, оно становится копией, хранящейся в инфраструктуре третьей стороны, подпадая под операционные, юридические и коммерческие решения этой третьей стороны. Не профессионала.

Что говорит законодательство

Европейский общий регламент по защите данных однозначен в своей статье 32: каждый, кто обрабатывает персональные данные, должен внедрить «соответствующие» технические и организационные меры для обеспечения уровня безопасности, соответствующего риску. Соответствие мер оценивается не по тому, «что приложение говорит, что оно делает», а по реальному риску. Если данные клиента попадают на сервер, юрисдикция которого не гарантирует уровень защиты, эквивалентный уровню Европейской экономической зоны, контролер данных — то есть профессионал — берет на себе риск, о котором он, вероятно, не совсем осознает.

И это не только GDPR. Профессиональная тайна, которая регулируется специально для адвокатов, врачей, психологов, аудиторов, журналистов и других, требует, чтобы общение с клиентом было конфиденциальным. Не «как можно более конфиденциальным». Конфиденциальным без оговорок. Если используемый технический канал не может этого гарантировать, профессионал берет на себя риск, который деонтология его профессии не позволяет принимать.

Парадокс в том, что риск невидимый. Никто не проводит аудит мессенджеров в офисе. Никто не запрашивает договор об обработке данных у поставщика чата. Риск обнаруживается только тогда, когда уже слишком поздно: утечка, опубликованный взлом, судебный приказ, исполненный на другом континенте без уведомления пользователя.

Что технически нужно профессионалу

То, что нужно лицу, обязанному хранить тайну, на самом деле удивительно просто с точки зрения требований:

- Канал, где сообщения идут напрямую с устройства отправителя на устройство получателя, без прохождения через промежуточный сервер, который хранит копии.
- Инфраструктура, юрисдикция и политики которой согласованы с GDPR по дизайну, а не по декларации.
- Способ идентифицироваться с собеседником без необходимости передавать третьей стороне профессиональные контакты (имена клиентов, номера телефонов, адресную книгу).
- Система, которую можно проверить — не на основе слов поставщика — чтобы подтвердить, что сообщение дошло до нужного человека.

Это не является требовательным списком. Это на самом деле то, что считалось само собой разумеющимся в профессиональной коммуникации доцифровой эпохи. Заказное письмо соответствовало всем этим критериям. Телефонный звонок с коммутатора офиса до коммутатора клиента — также. Странно не то, что эти гарантии требуются сегодня: странно то, что они были потеряны при переходе к цифровому каналу, без того, чтобы кто-то это заметил.

Разница между шифрованием и несохранением

Есть полезная метафора. Шифровать сообщение и хранить его на сервере эквивалентно тому, чтобы положить документ в сейф и оставить сейф в доме незнакомца. Сейф хороший. Документ в принципе невозможно прочитать. Но документ *все еще находится в чужом доме*. И тот кто-то может получить судебный приказ, подвергнуться кибератаке, изменить свои условия обслуживания, быть купленным другой компанией с другой этикой или может исчезнуть завтра.

Структурной альтернативой — не процедурной, не на основе доверия — является то, чтобы документ никогда не покидал офис. Чтобы он путешествовал напрямую с рабочего стола профессионала на рабочий стол клиента без какого-либо посредника. Это то, что технически делает коммуникация «точка-точка» между устройствами: она устраняет посредника. Не то чтобы посредник был плохим. Просто в случае профессиональной тайны посредник *ненужный*. А то, что ненужное, в любой системе, которая стремится быть безопасной, должно быть устранено по принципу.

Вопрос ответственности

В конце концов, вопрос, на который каждый профессионал с обязательством хранить тайну должен иметь возможность ответить решительным «да», следующий:

> Если завтра произойдет утечка разговора с одним из моих клиентов, и суд или профессиональная палата спросят меня, как я управляю конфиденциальностью, смогу ли я технически доказать, что канал, который я использовал, не хранит копии в инфраструктуре третьих сторон? Смогу ли я доказать, что данные никогда не покидали устройств двух лиц, участвовавших в разговоре? Смогу ли я, не полагаясь на слова компании с другого континента, доказать, что конфиденциальность была гарантирована архитектурой, а не обещанием?

Если ответ «нет», проблема не в конкретном инструменте. Проблема в том, что инструменту было делегировано ответственность, для поддержки которой инструмент не был спроектирован. Это как положить конфиденциальные файлы в прозрачный конверт и верить, что почтальон не заглянет внутрь.

Инструмент, который профессионал выбирает для общения со своими клиентами, много говорит о том, как он ценит их доверие. Есть инструменты, спроектированные так, чтобы это доверие не зависело от

обещаний, а от архитектуры. И есть инструменты, которые не являются такими. Знание разницы — часть работы.

Цитируемая нормативная база

- Регламент (ЕС) 2016/679 (GDPR), в частности ст. 5, 25 (защита данных на этапе проектирования) и 32 (безопасность обработки).
- Законодательство РФ о профессиональной тайне (напр., Основы законодательства РФ об охране здоровья граждан, Кодекс профессиональной этики адвоката).
- Уголовный кодекс РФ, ст. 137 (Нарушение неприкосновенности частной жизни) и ст. 138.
- Кодекс профессиональной этики адвоката в отношении конфиденциальности и профессиональной тайны.

← ПредыдущийШифрование не означает конфиденциальность: что метаданные говорят о васСледующий →GDPR и профессиональный обмен сообщениями: почему большинство нарушает правила, не зная об этом

Недавние материалы

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Возьмите эту статью с собой туда, где она вам понадобится.

↓ Markdown ↓ Простой текст ↓ PDF

Файл будет загружен на ваше устройство. Оттуда вы можете сохранить его, импортировать в Solo2 или поделиться им где угодно. Cuadernos не решает место назначения за вас.

Сургучная печать · SHA-256 4117ae4af3a561e6134a3ebf519316010563c29ad23aa7deb6517bfa4473a8e7

Cuadernos Lacre · Издание Menzuri Gestión S.L. ·
текст R.Eugenio · под редакцией команды Solo2.