GDPR и профессиональный обмен сообщениями: почему большинство нарушает правила, не зная об этом

Почти каждый офис, клиника или консалтинговая фирма отправляет клиентские документы через приложения, серверы которых расположены за пределами Европейского экономического пространства. Без злого умысла, но во многих случаях нарушая регламент, не будучи предупрежденными.

Документ, который путешествует дальше, чем вы думаете

Будничная ситуация: налоговый консультант получает через мессенджер документ с данными клиента. Торговый представитель пересылает через чат предложение коллеге. Врач делится тем же путем клиническим отчетом с коллегой. Никто не думает дважды. Это нормально. Это удобно. Это то, что делается каждый день в каждом офисе в каждом европейском городе.

Но этот документ во многих случаях только что совершил путешествие к серверу в Соединенных Штатах. Он был сохранен — пусть временно, пусть «зашифрованным в состоянии покоя» — в облаке, которое не контролируют ни профессионал, ни его клиент. Он прошел сквозь системы, которые могут технически индексировать метаданные, связанные с содержимым. И Европейский общий регламент по защите данных имеет по этому поводу довольно четкое мнение.

Что требует норма

GDPR — и, как следствие, судебная практика Суда Европейского Союза (в частности решение Schrems II, C-311/18, от 2020 г.) — устанавливает, что персональные данные европейских граждан должны быть защищены надлежащим образом. Если эти данные покидают Европейское экономическое пространство, контролер данных должен гарантировать, что получатель предлагает уровень защиты, «по существу эквивалентный» европейскому. На практике это означает, что отправка данных клиентов через сервисы, серверы которых подпадают под юрисдикцию США, без проведения оценки воздействия и без внедрения дополнительных гарантий — стандартных договорных условий, дополнительных технических мер, таких как проверенное шифрование и т. д. — может представлять собой нарушение регламента. Даже если до сих пор никто ничего не сказал.

И дело не только в содержимом сообщений. Метаданные — кто что направляет кому, когда, как часто, откуда — также являются персональными данными согласно правилам, в соответствии с неоднократным толкованием Европейского совета по защите данных. Сервис, который собирает метаданные из профессиональной коммуникации пользователя, обрабатывает персональные данные клиентов этого пользователя, без их ведома или предоставления какого-либо согласия на такую обработку.

Обычная схема мышления — «я использую приложение только для письма; приложение не является поставщиком данных моего клиента» — юридически ошибочна. Если данные клиента проходят сквозь инфраструктуру третьей стороны, эта третья сторона обрабатывает эти данные. И если она их

обрабатывает, должно быть юридическое основание, договор об обработке данных и соответствующие гарантии.

Кто ответственен

Вопрос о том, кто несет юридическую ответственность, не является академическим. GDPR различает *контролера данных* (кто решает, какие данные обрабатываются и с какой целью) и *процессора* (кто делает это материально от имени контролера). Профессионал, который направляет документы клиентов, является контролером. Поставщик мессенджера во многих случаях является фактическим процессором. Без договора об обработке — и без большинства условий, которые такой договор должен содержать — контролер не выполнил свое обязательство.

Снисходительное толкование говорит: «большинство профессионалов этого не знают». Строгое толкование говорит: «незнание закона не освобождает от ответственности». И толкование любого специализированного адвоката по защите данных, с которым консультируются по этому поводу, обычно является строгим.

Для кого это важно конкретно

Для каждого профессионала или компании, которая хотя бы время от времени оперирует персональной информацией третьих лиц:

- Адвокаты, которые получают клиентскую документацию (договоры, иски, декларации, отчеты об имуществе).
- Врачи и другие медицинские работники, которые делятся данными о здоровье — которые считаются согласно ст. 9 GDPR *особыми категориями* с усиленным режимом защиты.
- Налоговые консультанты и административные менеджеры, которые оперируют идентификационными, налоговыми и банковскими данными.
- Отделы кадров, которые управляют трудовой и личной документацией сотрудников.
- Коммерческие представители, которые получают контактные данные и часто чувствительную бизнес-информацию от потенциальных и существующих клиентов.

Во всех случаях информация защищена GDPR. Во всех случаях в обычной практике эта информация течет каналами, юрисдикция которых не позволяет объявить их «по существу эквивалентными» европейской базе без дополнительных гарантий. Не из-за злого умысла. Из-за привычки. И из-за технологической инфраструктуры, которая на протяжении пятнадцати лет ставила удобство выше соответствия.

Аргумент «все так делают»

Стоит предусмотреть самое распространенное возражение: «если все делают так же, это не может быть реальной проблемой». Это аргумент, который вполне понятен по-человечески, но юридически он не имеет никакой силы. Тот факт, что практика распространена, не делает ее соответствующей регламенту. Органы защиты данных в последние годы наложили санкции на несколько компаний именно за способы использования мессенджеров, которые казались безобидными до момента проверки.

Текущая операционная реальность заключается в том, что риск с точки зрения вероятности низкий — очень редко проверка Органа проводит аудит конкретных инструментов обмена сообщениями офиса среднего размера — но высокий с точки зрения воздействия, если он реализуется. Это риск, который большинство берет на себя, не зная, что они его берут. То есть, без оценки того, соответствует ли используемый инструмент юридической ответственности контролера данных.

Цифровые следы имеют обратную силу

Есть второй аргумент, почти симметричный предыдущему, который стоит предусмотреть: *«если бы это была серьезная проблема, администрация уже начала бы это контролировать»*. Текущая наблюдаемая реальность дает ему поверхностную правоту. Проверок из-за ненадлежащего использования мессенджеров в малых компаниях и особенно у самозанятых сегодня почти не существует — не потому, что поведение разрешено, а потому, что администрации в большей части ЕС не хватает человеческих ресурсов, необходимых для аудита миллионов обязанных субъектов.

Это то, что предполагает сегодняшняя наблюдаемая практика. Но это не то, что предполагает следующее десятилетие. Два вектора сходятся, чтобы изменить баланс в относительно короткие сроки.

Во-первых: цифровые следы имеют обратную силу. Каждое сообщение, направленное через приложение с центральным сервером, остается зарегистрированным — по крайней мере в метаданных — в инфраструктуре, которая сохраняется. То, что было направлено шесть месяцев назад, технически все еще подлежит аудиту сегодня. То, что направляется сегодня, будет подлежать аудиту через пять лет. Отсутствие проверки в настоящее время не является гарантией отсутствия проверки в будущем. Это отсрочка оценки, а не освобождение от нее.

Во-вторых: способность административного аудита будет расти ускоренно. Внедрение инструментов искусственного интеллекта в процессы контроля устраняет человеческое узкое место, которое до сих пор защищало (фактически, а не юридически) малые компании и самозанятых. Системе, способной перекрестно проверять массовые массивы метаданных, налоговые декларации, торговые реестры и обязательства по уведомлению о нарушениях безопасности, не нужны инспекторы: ей нужен доступ. А доступ через запросы к поставщикам с юридическим присутствием в ЕС в рамках нынешней нормативной базы является вполне осуществимым.

К этому добавляется менее технический, но не менее определяющий фактор: европейские государства находятся в процессе постоянного роста долга и им нужно, почти без исключения, расширять свою налоговую базу. Административная санкция, вытекающая из несоблюдения GDPR, является в чисто фискальном выражении растущим и политически удобным источником дохода. Это не предположение: это наблюдаемая тенденция в ежегодных отчетах европейских органов защиты данных, где общий объем санкций растет на протяжении нескольких финансовых лет подряд.

Операционный вывод для контролера не является алармистским, а трезвым: **решение о том, как сегодня управляется коммуникация с клиентами, оценивается относительно способности проверки того года, в котором придет проверка, а не относительно текущей.** И эта способность в разумные сроки будет существенно иной, чем сегодня. Тот, кто начнет делать вещи правильно сегодня, будет в порядке не только с сегодняшнего дня: след, генерируемый с этого момента, будет соответствовать норме, и это защищает ретроактивно будущий период. Тот, кто будет продолжать как раньше, будет накапливать след, подлежащий аудиту, соответствие которого будет оцениваться по стандартам — и ресурсам — следующих лет.

Что меняется с иной архитектурой

Существуют технические альтернативы, в которых данные не хранятся в инфраструктуре третьих сторон, а вместо этого путешествуют напрямую с устройства отправителя на устройство получателя. В этой архитектуре соответствие GDPR относительно международных передач не зависит от стандартных договорных условий, ни от доброй воли поставщика или будущих аудитов. Оно зависит от того факта, что *передачи нет*. А то, чего не существует, невозможно нарушить.

Это не единственное решение и не единственное возможное. Но оно структурно иное, и нормативное соответствие перестает быть процедурным дополнением и становится прямым следствием дизайна. Для

профессионала, который серьезно относится к своей ответственности как контролера, эта разница имеет значение.

Следующий выпуск Cuadernos детально проанализирует решение Schrems II и его практические последствия для малых и средних компаний, зависимых от американских облачных сервисов, через пять лет после его опубликования.

Источники и нормативная база

- Регламент (ЕС) 2016/679 (GDPR), в частности Раздел V относительно международных передач данных.
- Суд ЕС C-311/18 («Schrems II»), 16 июля 2020 г.
- EDPB — Рекомендации 01/2020 относительно мер, которые дополняют инструменты передачи данных.
- Органы защиты данных — Ежегодные отчеты с казуистикой санкций за ненадлежащее использование мессенджеров в профессиональной среде.

← ПредыдущийПрофессиональная тайна в цифровую эпохуСледующий →Когда никого нет посередине

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 019ee1543785a30b8bc7d73665c55732efb5240c04dcd6ba3eb382e54644158c

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

Этот веб-сайт не использует куки-файлы и не загружает ресурсы сторонних лиц. Он использует анонимный счетчик посещений с собственным хостингом (Umami, на нашем европейском сервере) и минимальный объем JavaScript, необходимый для вашего предпочтения светлой/темной темы. Никаких трекеров, никакого профилирования, никакого обмена данными. Если вы хотите следить за нами: RSS.