Аналіз · 16 травня 2026 р.

← Попередній·Наступний →

GDPR та професійний обмін повідомленнями: чому більшість порушує правила, не знаючи про це

Майже кожен офіс, клініка чи консалтингова фірма надсилає клієнтські документи через додатки, сервери яких розташовані за межами Європейського економічного простору. Без злого наміру, але в багатьох випадках порушуючи регламент, не будучи попередженими.

Документ, який подорожує далі, ніж ви думаєте

Буденна ситуація: податковий консультант отримує через месенджер документ з даними клієнта. Торговий представник пересилає через чат пропозицію колезі. Лікар ділиться тим самим шляхом клінічним звітом з колегою. Ніхто не думає двічі. Це нормально. Це зручно. Це те, що робиться щодня в кожному офісі в кожному європейському місті.

Але цей документ у багатьох випадках щойно здійснив подорож до сервера в Сполучених Штатах. Він був збережений — нехай тимчасово, нехай «зашифрованим у стані спокою» — у хмарі, яку не контролюють ні професіонал, ні його клієнт. Він пройшов крізь системи, які можуть технічно індексувати метадані, пов'язані з вмістом. І Європейський загальний регламент про захист даних має з цього приводу досить чітку думку.

Що вимагає норма

GDPR — і, як наслідок, судова практика Суду Європейського Союзу (зокрема рішення Schrems II, C-311/18, від 2020 р.) — встановлює, що персональні дані європейських громадян мають бути належним чином захищені. Якщо ці дані залишають Європейський економічний простір, контролер даних повинен гарантувати, що одержувач пропонує рівень захисту, «по суті еквівалентний» європейському. На практиці це означає, що надсилання даних клієнтів через сервіси, сервери яких підпадають під юрисдикцію США, без проведення оцінки впливу та без впровадження додаткових гарантій — стандартних договірних умов, додаткових технічних заходів, таких як перевірене шифрування тощо — може становити порушення регламенту. Навіть якщо досі ніхто нічого не сказав.

І справа не лише у вмісті повідомлень. Метадані — хто що надсилає кому, коли, як часто, звідки — також є персональними даними згідно з правилами, відповідно до неодноразового тлумачення Європейської ради з захисту даних. Сервіс, який збирає метадані з професійної комунікації користувача, обробляє персональні дані клієнтів цього користувача, без їх відома або надання будь-якої згоди на таку обробку.

Звичайна схема мислення — «я використовую додаток лише для письма; додаток не є постачальником даних мого клієнта» — юридично помилкова. Якщо дані клієнта проходять крізь інфраструктуру третьої сторони, ця третя сторона обробляє ці дані. І якщо вона їх обробляє, має бути юридична підстава, договір про обробку даних та відповідні гарантії.

Хто відповідальний

Питання про те, хто несе юридичну відповідальність, не є академічним. GDPR розрізняє *контролера даних* (хто вирішує, які дані обробляються і з якою метою) та *процесора* (хто робить це матеріально від імені контролера). Професіонал, який надсилає документи клієнтів, є контролером. Постачальник месенджера в багатьох випадках є фактичним процесором. Без договору про обробку — і без більшості умов, які такий договір повинен містити — контролер не виконав своє зобов'язання.

Поблажливе тлумачення каже: «більшість професіоналів цього не знають». Суворе тлумачення каже: «незнання закону не звільняє від відповідальності». І тлумачення будь-якого спеціалізованого адвоката з захисту даних, з яким консультуються з цього приводу, зазвичай є суворим.

Для кого це важливо конкретно

Для кожного професіонала або компанії, яка хоча б час від часу оперує персональною інформацією третіх осіб:

- Адвокати, які отримують клієнтську документацію (договори, позови, декларації, звіти про майно).
- Лікарі та інші медичні працівники, які діляться даними про здоров'я — які вважаються згідно зі ст. 9 GDPR *особливими категоріями* з посиленим режимом захисту.
- Податкові консультанти та адміністративні менеджери, які оперують ідентифікаційними, податковими та банківськими даними.
- Відділи кадрів, які керують трудовою та особистою документацією працівників.
- Комерційні представники, які отримують контактні дані та часто чутливу бізнес-інформацію від потенційних та існуючих клієнтів.

У всіх випадках інформація захищена GDPR. У всіх випадках у звичайній практиці ця інформація тече каналами, юрисдикція яких не дозволяє оголосити їх «по суті еквівалентними» європейській базі без додаткових гарантій. Не через злий намір. Через звичку. І через технологічну інфраструктуру, яка протягом п'ятнадцяти років ставила зручність вище відповідності.

Аргумент «всі так роблять»

Варто передбачити найпоширеніше заперечення: «якщо всі роблять так само, це не може бути реальною проблемою». Це аргумент, який цілком зрозумілий по-людськи, але юридично він не має жодної сили. Той факт, що практика є поширеною, не робить її такою, що відповідає регламенту. Органи захисту даних в останні роки наклали санкції на кілька компаній саме за способи використання месенджерів, які здавалися нешкідливими до моменту перевірки.

Поточна операційна реальність полягає в тому, що ризик з точки зору ймовірності низький — дуже рідко перевірка Органу проводить аудит конкретних інструментів обміну повідомленнями офісу середнього розміру — але високий з точки зору впливу, якщо він реалізується. Це ризик, який більшість бере на себе, не знаючи, що вони його беруть. Тобто, без оцінки того, чи відповідає використовуваний інструмент юридичній відповідальності контролера даних.

Цифрові сліди мають зворотну силу

Є другий аргумент, майже симетричний попередньому, який варто передбачити: *«якби це була серйозна проблема, адміністрація вже почала б це контролювати»*. Поточна спостережувана реальність дає йому поверхневу рацію. Перевірок через неналежне використання месенджерів у малих компаніях і особливо у самозайнятих сьогодні майже не існує — не тому, що поведінка дозволена, а тому, що адміністрації в більшій частині ЄС бракує людських ресурсів, необхідних для аудиту мільйонів зобов'язаних суб'єктів.

Це те, що припускає сьогоднішня спостережувана практика. Але це не те, що припускає наступне десятиліття. Два вектори сходяться, щоб змінити баланс у відносно короткі терміни.

По-перше: цифрові сліди мають зворотну силу. Кожне повідомлення, надіслане через додаток з центральним сервером, залишається зареєстрованим — принаймні в метаданих — в інфраструктурі, яка зберігається. Те, що було надіслано шість місяців тому, технічно все ще підлягає аудиту сьогодні. Те, що надсилається сьогодні, буде підлягати аудиту через п'ять років. Відсутність перевірки в даний час не є гарантією відсутності перевірки в майбутньому. Це відстрочка оцінки, а не звільнення від неї.

По-друге: здатність адміністративного аудиту зростатиме прискорено. Впровадження інструментів штучного інтелекту в процеси контролю усуває людське вузьке місце, яке досі захищало (фактично, а не юридично) малі компанії та самозайнятих. Системі, здатній перехресно перевіряти масові масиви метаданих, податкові декларації, торгові реєстри та зобов'язання щодо повідомлення про порушення безпеки, не потрібні інспектори: їй потрібен доступ. А доступ через запити до постачальників з юридичною присутністю в ЄС у межах нинішньої нормативної бази є цілком здійсненним.

До цього додається менш технічний, але не менш визначальний фактор: європейські держави перебувають у процесі постійного зростання боргу і їм потрібно, майже без винятку, розширювати свою податкову базу. Адміністративна санкція, що випливає з недотримання GDPR, є в чисто фіскальному вираженні зростаючим і політично зручним джерелом доходу. Це не припущення: це спостережувана тенденція у щорічних звітах європейських органів захисту даних, де загальний обсяг санкцій зростає протягом кількох фінансових років поспіль.

Операційний висновок для контролера не є алармістським, а тверезим: **рішення про те, як сьогодні керується комунікація з клієнтами, оцінюється відносно спроможності перевірки того року, в якому прийде перевірка, а не відносно поточної.** І ця спроможність у розумні терміни буде суттєво іншою, ніж сьогодні. Той, хто почне робити речі правильно сьогодні, буде в порядку не лише відсьогодні: слід, що генерується з цього моменту, відповідатиме нормі, і це захищає ретроактивно майбутній період. Той, хто продовжуватиме як раніше, накопичуватиме слід, що підлягає аудиту, відповідність якого буде оцінюватися за стандартами — і ресурсами — наступних років.

Що змінюється з іншою архітектурою

Існують технічні альтернативи, в яких дані не зберігаються в інфраструктурі третіх сторін, а натомість подорожують безпосередньо з пристрою відправника на пристрій одержувача. У цій архітектурі відповідність GDPR щодо міжнародних передач не залежить від стандартних договірних умов, ні від доброї волі постачальника чи майбутніх аудитів. Вона залежить від того факту, що *передачі немає*. А те, чого не існує, неможливо порушити.

Це не єдине рішення і не єдине можливе. Але воно структурно інше, і нормативна відповідність перестає бути процедурним додатком і стає прямим наслідком дизайну. Для професіонала, який серйозно ставиться до своєї відповідальності як контролера, ця різниця має значення.

Наступний випуск Cuadernos детально проаналізує рішення Schrems II та його практичні наслідки для малих та середніх компаній, залежних від американських хмарних сервісів, через п'ять років після його опублікування.

Джерела та нормативна база

- Регламент (ЄС) 2016/679 (GDPR), зокрема Розділ V щодо міжнародних передач даних.
- Суд ЄС C-311/18 («Schrems II»), 16 липня 2020 р.
- EDPB — Рекомендації 01/2020 щодо заходів, які доповнюють інструменти передачі даних.

- Органи захисту даних — Щорічні звіти з казуїстикою санкцій за неналежне використання месенджерів у професійному середовищі.

← ПопереднійПрофесійна таємниця в цифрову епохуНаступний →Коли посередині нікого немає

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 128f15f915db70e003e9233a8a9ff96ab6dc2434b5e1d0f98e4a992b43617734

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