Анализ · 16 май 2026 г.

← Предишна·Следваща →

GDPR и професионалните съобщения: защо повечето хора нарушават правилата, без да го знаят

Почти всеки офис, кабинет или консултантска фирма изпраща клиентски документи чрез приложения, чийто сървър се намира извън Европейското икономическо пространство. Без лоша воля, но в много случаи в нарушение на регламента, без никой да ги е предупредил.

Документът, който пътува повече, отколкото си мислите

Ежедневна ситуация: данъчен консултант получава чрез съобщение документ с клиентски данни. Търговски представител препраща чрез чат оферта на колега. Лекар споделя по същия начин клиничен доклад с колега. Никой не се замисля два пъти. Нормално е. Удобно е. Това се прави всеки ден във всеки офис във всеки европейски град.

Но този документ в много случаи току-що е пътувал до сървър в Съединените щати. Той е бил съхранен – макар и временно, макар и „криптиран в покой“ – в облак, който нито професионалистът, нито неговият клиент контролират. Преминал е през системи, които технически могат да индексират метаданни, свързани със съдържанието. А европейският Общ регламент относно защитата на данните има какво да каже по въпроса доста ясно.

Какво изисква нормата

GDPR – и впоследствие практиката на Съда на Европейския съюз (по-специално решението Schrems II, C-311/18, от 2020 г.) – установява, че личните данни на европейските граждани трябва да бъдат подходящо защитени. Ако тези данни напускат Европейското икономическо пространство, администраторът трябва да гарантира, че получателят предлага ниво на защита, което е „по същество равностойно“ на европейското. На практика това означава, че изпращането на клиентски данни чрез услуги, чиито сървъри са под юрисдикцията на САЩ, без да е извършена оценка на въздействието и без да са приложени допълнителни гаранции – стандартни договорни клаузи, допълнителни технически мерки като проверяемо криптиране и др. – може да представлява нарушение на регламента. Дори ако досега никой нищо не е казал.

И не става въпрос само за съдържанието на съобщенията. Метаданните – кой какво изпраща на кого, кога, колко често, откъде – също са лични данни според разпоредбите, според многократните тълкувания на Европейския комитет по защита на данните. Услуга, която събира метаданни от професионалната комуникация на даден потребител, обработва лични данни на клиентите на този потребител, без те да знаят за това или да са дали съгласие за такова обработване.

Обичайната мисловна схема – „използвам приложението само за писане; приложението не е доставчик на данни на моя клиент“ – е правно погрешна. Ако данните на клиента преминават през инфраструктурата

на трета страна, тази трета страна обработва тези данни. И ако ги обработва, трябва да има правно основание, договор за обработка на данни и подходящи гаранции.

Кой е отговорен

Въпросът кой носи правната отговорност не е академичен. GDPR прави разлика между *администратор* (който решава какви данни за каква цел се обработват) и *обработващ лични данни* (който прави това материално от името на администратора). Професионалистът, който изпраща клиентски документи, е администратор. Доставчикът на приложението за съобщения в много случаи е фактически обработващ. Без договор за обработка – и без повечето клаузи, които такъв договор трябва да съдържа – администраторът не е изпълнил задължението си.

Благосклонното тълкуване гласи: „повечето професионалисти не знаят това“. Строгото тълкуване гласи: „непознаването на закона не е извинение“. А тълкуването на всеки специализиран адвокат по защита на данните, консултиран по въпроса, обикновено е строгото.

За кого е важно това конкретно

За всеки професионалист или компания, които макар и от време на време оперират с лична информация на трети страни:

- Адвокати, които получават клиентска документация (договори, искове, декларации, отчети за имущество).
- Лекари и други здравни специалисти, които споделят здравни данни – които се считат за *специални категории* съгласно чл. 9 от GDPR със засилен режим на защита –.
- Данъчни консултанти и административни мениджъри, които оперират с идентификационни, данъчни и банкови данни.
- Отдели „Човешки ресурси“, които управляват трудова и лична документация на служители.
- Търговски представители, които получават данни за контакт и често чувствителна бизнес информация от потенциални и настоящи клиенти.

Във всички случаи информацията е защитена от GDPR. Във всички случаи в обичайната практика тази информация тече през канали, чиято юрисдикция не позволява обявяването им за „по същество равностойни“ на европейската рамка без допълнителни гаранции. Не от лоша воля. От навик. И поради технологична инфраструктура, която в продължение на петнадесет години поставяше удобството пред съответствието.

Аргументът „всички го правят“

Разумно е да се предвиди най-честото възражение: „ако всички го правят, не може да е реален проблем“. Това е напълно разбираем аргумент и правно няма никаква сила. Фактът, че една практика е широко разпространена, не я прави съобразена с регламента. Органи за защита на данните (като КЗЛД в България) санкционираха през последните години няколко компании именно за начини на използване на съобщения, които са изглеждали безобидни до момента на проверката.

Настоящата оперативна реалност е, че рискът по отношение на вероятността е нисък – много рядко се случва проверка на Органа да одитира конкретните инструменти за съобщения на средно голям офис – но висок по отношение на въздействието, ако се материализира. Това е риск, който повечето поемат, без да знаят, че го поемат. Тоест, без да са оценили дали използваният инструмент е в съответствие с правната отговорност на администратора.

Цифровата следа е ретроактивна

Има втори аргумент, почти симетричен на предишния, който си струва да се предвиди: *„ако това беше сериозен проблем, администрацията вече щеше да е започнала да го контролира“*. Настоящата наблюдавана реалност му дава повърхностно право. Контролът за неправилно използване на съобщения в малките фирми и особено при самонаетите лица днес почти липсва – не защото поведението е разрешено, а защото на администрацията в България и в голяма част от ЕС липсват човешки ресурси, необходими за одитиране на милиони задължени субекти.

Това предполага днешната наблюдавана практика. Но това не е това, което предполага следващото десетилетие. Два вектора се сливат, за да променят баланса в относително кратки срокове.

Първо: цифровата следа е ретроактивна. Всяко съобщение, изпратено чрез приложение с централен сървър, остава регистрирано – поне в метаданните – в инфраструктура, която продължава да съществува. Това, което е изпратено преди шест месеца, технически е все още одитируемо днес. Това, което се изпраща днес, ще бъде одитируемо и след пет години. Липсата на настоящ контрол не е гаранция за липса на бъдещ контрол. Това е отлагане на оценката, а не освобождаване от нея.

Второ: капацитетът за административен одит ще расте ускорено. Внедряването на инструменти с изкуствен интелект в процесите на контрол елиминира човешкото тясно място, което досега защитаваше – фактически, а не юридически – малките фирми и самонаетите. Система, способна да засича масови масиви от метаданни, данъчни декларации, търговски регистри и задължения за уведомяване за нарушения на сигурността, няма нужда от инспектори: тя има нужда от достъп. А достъпът чрез изисквания към доставчици с правно присъствие в ЕС в рамките на настоящата нормативна уредба е напълно осъществим.

Към това се добавя по-малко технически, но също толкова решаващ фактор: европейските държави се намират в процес на постоянно растяща задлъжнялост и трябва, почти без изключение, да разширят данъчната си база. Административната санкция, произтичаща от неизпълнение на GDPR, е в чисто фискално изражение нарастващ и политически удобен източник на приходи. Това не е предположение: това е наблюдавана тенденция в годишните доклади на европейските органи за защита на данните, където общият обем на санкциите нараства в продължение на няколко поредни финансови години.

Оперативното заключение за администратора не е алармистко, а трезво: **решението за това как се управлява днес комуникацията с клиентите се оценява спрямо контролния капацитет на годината, в която идва проверката, а не спрямо настоящия.** А този капацитет в разумен срок ще бъде съществено различен от днешния. Който започне да прави нещата правилно днес, няма да бъде изряден само от днес: следата, генерирана от този момент нататък, ще бъде съобразена с нормата и това защитава ретроактивно предстоящия период. Който продължи както досега, ще трупа одитируема следа, чието съответствие ще се оценява спрямо стандартите – и ресурсите – на идните години.

Какво се променя с различна архитектура

Съществуват технически алтернативи, при които данните не се съхраняват в инфраструктурата на трети страни, а вместо това пътуват директно от устройството на изпращача до това на получателя. В тази архитектура спазването на GDPR по отношение на международните трансфери не зависи от стандартни договорни клаузи, нито от добрата воля на доставчика или от бъдещи одити. То зависи от това, че *няма трансфер*. А това, което не съществува, не може да бъде нарушено.

Това не е единственото решение, нито единственото възможно. Но то е структурно различно и нормативното съответствие престава да бъде процедурно допълнение и се превръща в пряко следствие от дизайна. За професионалист, който приема сериозно отговорността си като администратор, тази разлика има значение.

Следващото издание на Cuadernos ще анализира подробно решението Schrems II и неговите практически последици за малките и средните фирми, зависими от облачните услуги на САЩ, пет години след неговото публикуване.

Източници и правна рамка

- Регламент (ЕС) 2016/679 (GDPR), по-специално глава V относно международните трансфери.
- СЕС C-311/18 („Schrems II“), 16 юли 2020 г.
- ЕДПБ – Препоръки 01/2020 относно мерките, които допълват инструментите за трансфер.
- Органи за защита на данните (вкл. КЗЛД) – Годишни доклади с казуистика на санкции за неправилно използване на незабавни съобщения в професионална среда.

← ПредишнаПрофесионалната тайна в цифровата ераСледваща →Когато няма никой по средата

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 f70c9ae1ab087b3d54524cb8d89931ecd494a185570e3e8df5ded4913d0ae0ef

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

Този уебсайт не използва бисквитки и не зарежда ресурси от трети страни. Той използва самохостван анонимен брояч на посещенията (Umami, на нашия европейски сървър) и минималния JavaScript, необходим за предпочитанието ви за светла/тъмна тема. Без тракери, без профилиране, без споделяне на данни. Ако искате да ни последвате: RSS.