Анализ · 25 мая 2026 г.

← Предыдущий·Следующий →

Self-hosting как профессиональная практика

Сервер — это не более чем компьютер. Вопрос не в том, стоит ли его иметь, а в том, где живут данные ваших клиентов, кто их поддерживает и кто несет ответственность, когда что-то идет не так.

Чтобы мы понимали друг друга: Ваши данные всегда живут в чьем-то компьютере: в компьютере гиганта, которому вы все доверяете, в арендованном компьютере, которым управляете вы, или в вашем собственном. Чем больше контроля вы хотите, тем больше ответственности вы на себя берете. Делегирование крупной третьей стороне успокаивает, но не освобождает от ответственности: информация ваша — и ваших клиентов, — и ответственное лицо — вы.

Вопрос между облаком и подвалом

Стоит начать с демистификации слова, которое пугает без причины: сервер. Сервер — это не таинственная машина в охлаждаемой комнате. Это просто компьютер другого человека — или ваш собственный, — который хранит информацию и выдает ее тому, кто ее запрашивает. Десятилетиями мы хранили информацию наших клиентов в папках, в картотеках, на рабочем столе, и никто не терял из-за этого сон. Информация не была пугающей, потому что она была на бумаге; она не должна быть пугающей и потому, что она на диске.

«Облако» тоже не является чем-то эфирным. Это компьютер компании, почти всегда находящийся далеко и почти всегда принадлежащий кому-то другому. Я узнал это невольно в тот день, когда, будучи уверенным, что мои файлы в безопасности в Google Drive, обнаружил, что папка на моем компьютере содержала не мои документы, а ярлыки к документам, которые жили в другом месте. Если бы то другое место решило закрыться, изменить цену или отменить подписку, мое спокойствие исчезло бы вместе с ним. Я не владел своими вещами; у меня было разрешение на доступ к ним.

Отсюда рождается вопрос этого Cuaderno, который проще сформулировать, чем ответить на него: где должны жить данные ваших клиентов? А ваши собственные? Публичное обсуждение ставит его так, будто есть всего два противостоящих ответа — облако крупных платформ или сделать всё самому, — почти как вопрос выбора стороны. Но путей не два: их три, и ни один из них не является актом веры. Если вчитаться в них не спеша, в них больше нюансов, и они требуют большего, чем кажется.

Это касается вас, что бы вы ни продавали

Легко думать, что конфиденциальность — это дело адвокатов, врачей или журналистов, а остальным нечего скрывать. Это ошибка, и дорогая. Почти любой бизнес хранит данные своих клиентов, подпадающие под действие закона, и многие хранят, сами того не зная, информацию гораздо более конфиденциальную, чем кажется.

Магазин диванов записывает имя, адрес и телефон покупателя; если есть рассрочка — то и его финансовые данные. Фирма по ремонту или дизайну интерьеров хранит фотографии внутренних помещений домов своих клиентов и полные планы их жилищ. Клининговая компания работает с планами офисов, которые она убирает, часто размеченными цветами и цифрами, указывающими, какой сотрудник

куда входит, в какое время и с каким ключом. Ничто из этого не кажется чем-то серьёзным, пока не зададишься вопросом, для кого ещё это могло бы иметь ценность: эти планы уборки, если взглянуть на них другими глазами, — идеальная карта для того, кто захочет проникнуть внутрь, чтобы украсть.

То, что бизнес мал или продает диваны вместо защиты интересов в суде, не делает его данные менее ценными и не заставляет закон перестать к нему применяться. Это лишь приводит к тому, что его владелец склонен меньше об этом думать. А меньше думать о том, что является вашей ответственностью, — это как раз то место, где начинаются проблемы.

Где живут ваши данные?

На этот вопрос есть, по сути, три ответа. И стоит помнить, что «данные» — это не только досье клиента или блок счетов и смет: это ещё и ваши разговоры с ним — по WhatsApp, через профессиональный чат-сервис, через Solo2. Три ответа, которые следуют ниже, — это не степени чистоты и не лестница от хороших к плохим: это три способа распределить одно и то же — контроль и ответственность.

Передать всё провайдеру. Это самый распространённый вариант, и для большинства — единственный, который они знают. Помещаю всё в Google Workspace или в Microsoft 365 и целиком доверяю это провайдеру. Плачу свой взнос и перестаю об этом думать. Самая крайняя форма этого — сервисы, где вы даже не получаете доступа к своим данным: некоторые облачные программы для выставления счетов, например, хранят ваши счета и сметы — и работают очень хорошо, — но информация живёт в их системе, а не в вашей. Пока платите — у вас есть доступ; в тот день, когда вы уходите, вы обнаруживаете, что забрать собственную историю трудно или невозможно. Держать ваши данные в полузаложниках для иного провайдера — это как раз то, что мешает вам уйти к конкуренту. В обмен на удобство я отдаю контроль и — не говоря об этом вслух — ощущение, что ответственность больше не моя. Здесь уместен нюанс, который почти никогда не делают: делегировать не значит американское. Я могу так же удобно передать всё европейскому провайдеру — например, Infomaniak — и одним махом снять бóльшую часть сомнений о международных передачах данных, которые мы видели в «Schrems II», ничего не размещая у себя. Это не Соединённые Штаты против всей остальной вселенной: внутри чистого делегирования уже есть решения, которые важны.

Арендовать и управлять собственным сервером. У меня есть то же самое, что дали бы мне Microsoft или Google, но я настраиваю это сам. Я арендую сервер у европейского провайдера — Hetzner, OVH, Scaleway, — устанавливаю свободное ПО (например, Nextcloud для файлов) и сам администрирую результат. Я получаю реальный контроль: я знаю, что запущено, где и почему. Но машина все равно находится в дата-центре третьей стороны и, прежде всего, меняется тот, кто несет последствия. При делегировании, если что-то пойдет не так, вам есть кого винить. При самостоятельном управлении, скорее всего, вина будет вашей.

Хранить на собственном компьютере. Это вариант, о котором почти никто не рассказывает, и это сердце данной тетради. Вам не нужен огромный сервер, работающий круглосуточно внутри макро-дата-центра, чтобы хостить свои данные. Ваш офисный компьютер — это уже сервер: он обслуживает вас. Вы оставляете его включенным в офисе и подключаетесь к нему с ноутбука у клиента или с мобильного телефона, когда вы дома. Мы называем его «офисным компьютером», а не «сервером», но он делает ровно то же самое, что и два предыдущих варианта. Контроль максимален, как и близость: ваши данные находятся там же, где и вы. Обратная сторона, если говорить без прикрас, заключается в том, что ответственность также максимальна. Если пропадет электричество, в Нюрнберге нет дежурного техника: вы сами должны включить рубильник. И для того, чтобы этот компьютер был доступен извне, нужно что-то, что наладит мост между вашим ноутбуком и ним. Это не магия, и об этом стоит знать, прежде чем выбирать этот путь.

И даже не нужно приспосабливать офисный компьютер: существует устройство, придуманное именно для этого, — NAS (его выпускают Synology, QNAP и другие). Как и почти во всём, что мы видели в этих Cuadernos, внутри него нет никакого волшебства: это специализированный компьютер, та же самая

машина, которую вы арендовали бы в центре обработки данных, только рассчитанная на то, чтобы хранить данные и отдавать их по сети, без монитора и клавиатуры. Подключите к нему экран и клавиатуру — и у вас обычный компьютер; установите подходящее программное обеспечение на свой ПК — и у вас NAS. Разница в том, что NAS уже приходит готовым к работе. Вы покупаете его, подключаете дома или в офисе, и он ваш. Вы не платите ежемесячную плату; вы платите один раз, и он принадлежит вам, как любой другой инструмент вашего дела. Вы его включаете, выключаете, при желании увозите в другое место. А поскольку он ваш, ничто не мешает иметь два —один дома, другой в офисе— или три, добавив ещё один в надёжном месте, синхронизированных между собой: ваше собственное резервирование, не завися от того, что его поддерживает кто-то третий. Самостоятельный хостинг, в конечном счёте, — это не одна вещь: это сочетание оборудования, владения, мест размещения и программного обеспечения.

Здесь неизбежно назвать то, что делаем мы, и делаем это без прикрас: в Solo2 этот мост наводит само приложение. Компьютер в вашем офисе остаётся доступным только для ваших доверенных устройств и всегда под шифрованием, а остальные ваши устройства переподключаются к нему сами. Когда клиент общается с вами, именно ваш компьютер — а не чужой — разговаривает с клиентом. Мы не решаем проблему отключения электричества; мы решаем проблему моста. И мы не единственные: почти под каждую потребность сегодня существуют программы — свободные или проприетарные, — которые позволяют именно это: хранить данные на вашем оборудовании и добираться до них извне. Наше — это пример; важна идея, а не марка.

Избыточность — это не суперсила

Здесь возникает немедленное возражение, и оно вполне обоснованно: если у меня все на офисном компьютере, что будет, если он сломается? Вопрос хороший. Ответ заключается в том, что сеть безопасности, которую мы воображаем у крупных провайдеров, более скромная — и более подражаемая, — чем кажется.

Когда я оставляю свои данные в дата-центре транснациональной компании, я верю, что у нее есть копии в нескольких местах. И, вероятно, они есть: во втором месте, может быть, в третьем. Но эта избыточность не бесконечна и, прежде всего, она не моя: это по-прежнему жесткий диск, владельцем которого я не являюсь, управляемый кем-то, кому я доверяю на веру, которую почти никогда не проверяю.

Эту же сеть я могу сплести сам, причем с решающим преимуществом. Мой ежедневный сервис живет на офисном компьютере. Оттуда я храню зашифрованную копию на компьютере дружественной компании — коллеги по профессии, другого доверенного офиса — и еще одну зашифрованную копию, если захочу, у того самого европейского провайдера, о котором мы говорили. Разница во всем: то, что я оставляю снаружи, — это не мой сервис и не мои открытые данные, а зашифрованная копия, которую могу открыть только я. Внешний провайдер хранит закрытый сундук, от которого у него нет ключа. Я не вверяю ему свою информацию: я вверяю ему несколько байтов, которые без меня ничего не значат.

Это было безопасно, пока не перестало быть таковым

Позвольте мне рассказать личную историю, потому что она иллюстрирует это лучше любого аргумента. Более десяти лет я был преданным клиентом CrashPlan — технически выдающегося сервиса резервного копирования. Я делал резервные копии в их облаке для всех своих компьютеров и компьютеров моей семьи — рабочих и домашних, всех без исключения — с версиями, которые я мог восстановить с любой желаемой частотой, возвращаясь во времени к конкретному файлу многомесячной давности. После первой копии сервис передавал только изменения, зашифрованные и сжатые, так что я без особых усилий поддерживал огромный бэкап в актуальном состоянии. Это спасало меня много раз, от пустякового документа до целого диска. Цена росла с годами, и мне было все равно: я платил с удовольствием.

Чего я не знал, так это того, что CrashPlan допустил ошибку в расчетах: по контракту они обещали неограниченное хранилище как в пространстве, так и во времени. А пространство, умноженное на время — многолетняя история, версии каждые несколько минут — растет до тех пор, пока не становится неустойчивым. Однажды они сообщили нам всем, что сервис прекращает работу. Они сделали это элегантно, предоставив щедрый срок почти в один год и дав нам средства для скачивания наших данных. Но куда идти человеку с более чем десятилетней историей версионных копий всех его дисков? Именно тогда обнаруживается, что у вас нет ни способа скачать все сразу, ни места, куда это положить, и что, даже если бы вы могли, новое хранилище стоило бы целое состояние.

Я спас четыре необходимые вещи. Остальное ушло, когда выключили рубильник. Я был спокоен, моя информация была в безопасности... пока не перестала ею быть. И не из-за предательства: CrashPlan повёл себя безупречно — в отличие от Evernote, который годы спустя повёл себя позорно, — просто мой ангел-хранитель в облаке решил, имея на то полное право, перестать им быть. Результат для меня был одинаков: то, что я считал надёжным, исчезло.

То, чему на самом деле учит эта история, больше связано с человеческой природой, чем с технологиями. Когда человек чувствует, что что-то является его ответственностью, он действует превентивно: делает копии, страхуется, проявляет здравое недоверие. Когда он верит — ошибочно — что ответственность несет третья сторона, крупная и платежеспособная, он расслабляется и пускает все на самотек. Это делегированное спокойствие не является осмотрительностью: это, без прикрас, форма безответственности.

Платить — не значит соблюдать правила

Эта тихая безответственность очень похожа на родителей, которые записывают сына в самую дорогую школу, оплачивают ему потом магистратуру и верят, что тем самым они исполнили свой долг. Они не исполнили долг. Быть родителем — значит беспокоиться о том, что он узнал сегодня, о том, чего он не понимает, о его ценностях, о его уверенности в себе. Если в двадцать пять лет этот сын не умеет ни работать, ни вести себя, вина лежит не на школе, которая взяла деньги: она лежит на том, кто делегировал обязанности и заплатил, веря, что этого достаточно. Оплата услуг третьей стороны не освобождает от ответственности. Никогда не освобождала.

С данными происходит то же самое, и недавняя история это подтверждает. Пятьдесят или сто лет назад специалист хранил данные своих клиентов в папках, у себя в кабинете или дома, и чувствовал себя ответственным за них. Редко что-то терялось. Мы перешли в цифровой мир и с поразительной лёгкостью загружаем всё в «облако» — которое есть не что иное, как компьютер транснациональной корпорации, — и перестаём беспокоиться. И часто случаются происшествия, и есть фирмы, которые теряют всё, и тогда говорят: виноват Google, виноват Microsoft. Нет. Информация ваша, или ваших клиентов, но ответственный — вы.

Хостинг собственных данных — это не технический каприз: это возвращение того спокойствия десятилетней давности, знания того, где что находится и почему. Защита данных тем временем испытала резкое колебание маятника — от отсутствия каких-либо норм, когда любой бездумно выставлял данные клиента напоказ, до требования, которое с непропорциональной суровостью ложится на самых маленьких, на самозанятого, который дает телефон клиента курьеру. Я не оспариваю цель; я наблюдаю несоответствие. Но несоответствие не освобождает нас от ответственности: в тот день, когда у администрации появятся средства для масштабного отслеживания и наказания, размер перестанет кого-либо защищать, и разумно не ждать этого дня с неубранным домом. Наличие данных под собственным контролем помогает соблюдать правила и помогает доказать это. И прежде всего, это возвращает вещи на свои места: когда информация принадлежит вам, ответственность полностью лежит на вас — нет третьей стороны, которую можно винить, и нет третьей стороны, чей сбой подставил бы вас под удар.

Ответственность также защищает

Было бы нечестно рисовать это без теней. Занять место посредника означает взять на себя его заботы: поддерживать копии в актуальном состоянии, устанавливать обновления и нести юридическую ответственность — ответственность по RGPD, — которая, на самом деле, никогда не переставала быть полностью вашей (ссылки в сносках детализируют статьи). Есть работа, и есть день, когда что-то ломается не вовремя. Мы этого не скрываем.

Но страх, окружающий это слово, ответственность, откалиброван неверно. Гораздо легче потерять свои файлы в облачном сервисе, который закрывается, или свои фотографии в Google Фото, чем потерять ту папку с важными документами, которая лежит на вашем собственном компьютере: ту, о которой вы знаете, где она, и чьё исчезновение вы бы заметили, как только она пропадёт. То, что вы чувствуете своим, вы бережёте; то, что считаете в сохранности в чужих руках, вы запускаете.

Подумайте о фотоальбомах прежних времён, тех, с проявленными бумажными снимками, хранившихся в ящике. Вы хоть раз слышали, чтобы кто-то сказал, что «потерял» свой семейный альбом? Слышно про дом, который сгорел вместе с альбомом внутри; но просто так потерять — нет. А вот люди, у которых все фотографии были в Google Фото или в Apple Фото и которые остались ни с чем: эта история возвращается каждые несколько месяцев, потому что они верили, что всё в сохранности. Google Фото бережёт ваши фотографии, разумеется; но бережёт их не так, как родители берегут альбом, где запечатлены их дети и внуки. Эту разницу не исправит никакой дата-центр: ответственность, когда она ваша, — не только бремя; это ещё и лучшая гарантия.

Четыре вопроса перед принятием решения

Если вы подумываете о том, чтобы сделать этот шаг в любой из его форм, стоит сначала беспристрастно и честно ответить на четыре вопроса:

1. Какую часть ваших данных вам было бы больно потерять или не иметь возможности забрать? И осторожнее с тем, чтобы списывать со счетов «рутинное»: история счетов кажется самой прозаичной вещью на свете, пока вы не смените программу и не обнаружите, что эти счета принадлежали провайдеру, а не вам — что вы можете, самое большее, распечатать их в PDF, уже не имея возможности искать внутри них. Дело не только в чувствительности: дело в том, кому на самом деле принадлежит то, что вам нужно сохранить.
2. Какой вариант соразмерен вашим реальным техническим возможностям? Собственный, хорошо обслуживаемый компьютер по силам любому; администрировать целый сервер — уже не так. Будьте честны в том, что вы умеете, а что нет. И помните, что между тем, чтобы поднять целый сервер, и тем, чтобы передать всё, есть очень разумная промежуточная территория: программы — свободные или проприетарные, — которые хранят ваши данные на вашем собственном оборудовании и позволяют добираться до них извне. Для многих людей это лучший баланс.
3. Какой у вас план на самый худший день? Взлом, смерть диска, закрытие провайдера, техник на больничном. Если план начинается со слов «этого не должно случиться», это не план.
4. Сумеете ли вы доказать, что соблюдаете правила, если завтра к вам придут с проверкой? Делать хорошо и иметь возможность доказать, что делаешь хорошо, — это не одно и то же. Закон требует второго.

Нет универсального ответа. Есть пропорциональный ответ, принятый с честностью в отношении того, что приобретается и что наследуется. И выше всей техники — одна простая истина: ваши данные живут в чьем-то компьютере. Единственный вопрос, который действительно важен: чей это компьютер, по вашему желанию.

Селф-хостинг не является ни добродетелью, ни пороком: это инструмент с конкретным набором возможностей и обязанностей. Вопрос никогда не заключался в том, стоит ли хостить свои данные, а в том, какие данные, как и с какой сетью поддержки. Возвращение контроля над данными — это не возвращение в подвал и не недоверие ко всему: это возвращение к чувству ответственности за то, что

принадлежит нам, как это было в те времена, когда данные хранились в папке на столе. Эта ответственность, при правильном понимании, и есть настоящая услуга, которую профессионал оказывает своим клиентам.

Источники и дополнительная литература

- Регламент (ЕС) 2016/679 — статья 28 (обработчик), статья 32 (безопасность обработки), статья 33 (уведомление о взломе), статья 37 (назначение ответственного за защиту данных).
- Испанское агентство по защите данных — *Практическое руководство по анализу рисков при обработке персональных данных* (действующая редакция). Рамки для контролеров, принимающих на себя собственные технические функции.
- Европейский совет по защите данных — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Применимо также для проверки пропорциональности в решениях по собственной инфраструктуре.
- Европейская комиссия — публичный справочник поставщиков информационных услуг, созданных в европейской юрисдикции. Административная отправная точка для выявления европейских вариантов управляемого хостинга.
- Nextcloud GmbH (Германия) — *Архитектура Nextcloud Enterprise и документация по соответствию*. Задокументированный случай свободного ПО с вариантами селф-хостинга и управления европейским провайдером; полезно в качестве технического справочника проекта, поддерживаемого в европейской юрисдикции с 2016 года.

← Предыдущий24 слова: что такое криптографическая идентичностьСледующий →Реальная vs мнимая конфиденциальность: вопросы, которые стоит себе задать

Недавние материалы

- Размышление · 29 июня 2026 г. Вы не анонимны
- Размышления · 27 мая 2026 г. То, что подпись не может исправить
- Анализ · 26 мая 2026 г. Реальная vs мнимая конфиденциальность: вопросы, которые стоит себе задать

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 a7fbddb9bff28530629eb23f4e2c47bce15fb43a84ce64292075f50927137e6b

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