



Локализация обработки данных и ограничение свободы трансграничного оборота данных: Глобальные тренды



Алексей Мунтян

Управляющий партнер в компании Privacy Advocates

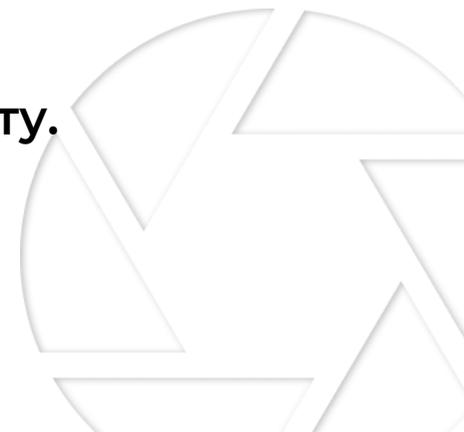
+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru

- 17 лет опыта в защите персональных данных
- Соучредитель «Сообщества профессионалов в области инфоприватности» - RPPA.pro
- Участник центра компетенций Роскомнадзора и научно-технического совета ГРЧЦ
- Сопредседатель Privacy & Legal Innovation кластера РАЭК
- Ex-DPO в Johnson&Johnson, DHL Express, «Альфа-Групп», Sber CIB и Восточно-африканском офисе Управления Верховного комиссара ООН по правам человека



1. В XXI веке требования локализации данных активно эволюционировали в сторону увеличения как диапазона охватываемых данных, так количества стран.
2. Число стран, которые ввели требования локализации данных, почти удвоилось с 35 в 2017 году до 82 в 2025 году.
3. Общее количество действующих требований локализации данных (как формальных, так и фактических) увеличилось более чем втрое с 67 в 2017 году до 214 в 2025 году.
4. На конец 2025 года на планете в стадии рассмотрения находится 58 новых требований локализации данных.
5. Китай (33), Индия (15), Россия (10) и Турция (9) являются мировыми лидерами по количеству требований локализации данных и их охвату.



Аргументация политиков и иных заинтересованных лиц в необходимости локализации данных демонстрирует постоянную эволюцию.

Многие ранее непреднамеренно поддерживали локализацию, поскольку не понимали, как международные компании управляют данными на глобальном уровне, соблюдая при этом местные законы.

Однако все больше политиков открыто поддерживают локализацию как форму протекционизма. Например, во Франции, Индии и Южной Корее творчески подходят к использованию произвольного и непрозрачного лицензирования, сертификации и других нормативных ограничений для создания условий вынужденной локализации данных (и выдавливания из национального рынка иностранных компаний и продуктов).

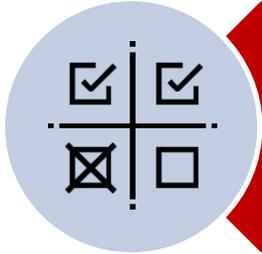


1. Обеспечение конфиденциальности и кибербезопасности (например, Индия).
2. Цифровой протекционизм и суверенитет данных (например, ЕС).
3. Контроль цифрового пространства (например, Китай).
4. Содействие местным правоохранительным и надзорным органам (например, Турция).
5. Геополитические риски и финансовые санкции (например, Россия).

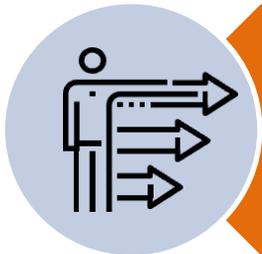




Страны / Категории данных														
Персональные	•	•				•	•	•	•	•	•	•	•	•
Финансовые, налоговые, банковские	•		•		•		•	•		•	•	•		
Платежные	•							•			•	•		•
Геолокационные								•		•	•	•		
Медицинские, генетические					•						•	•		
Государственные	•	•		•		•				•		•	•	
Телекоммуникационные	•		•			•		•			•	•		
Публично-облачные	•						•		•					
Коммерческие, технические											•	•		•



Формальное ограничение передачи определенных типов данных за пределы границ государства



Фактическое ограничение трансграничной передачи путем создания условий, затрудняющих такую передачу – она становится сложной, дорогостоящей и нестабильной



Ограничение оборота данных, определяемых в широких и расплывчатых категориях: «конфиденциальные», «важные», «ключевые» или «относящиеся к национальной безопасности»





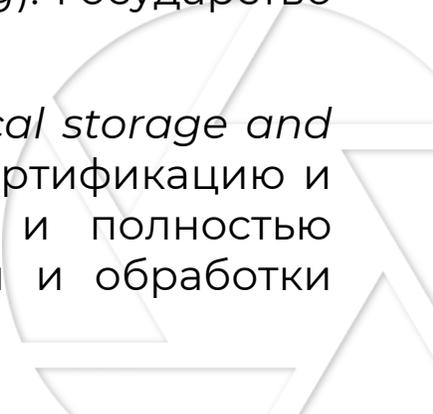
Локальная репликация данных (*Local data mirroring*). Необходимо хранить копию данных локально, но передача данных за пределы страны разрешена. В некоторых случаях требуется соблюдение последовательности обработки данных в виде их локального сбора и/или актуализации.

Локальное хранение данных (*Explicit local data storage*). Данные должны физически находиться в стране их происхождения. В некоторых случаях допускается трансграничный доступ к данным для их обработки, но с условием локализации результатов обработки данных в стране их происхождения.

Вынужденное локальное хранение и обработка данных (*De facto local storage and processing*). Локальное хранение данных является вынужденным из-за строгих требований к трансграничной передаче (например, необходимость получения предварительного одобрения на передачу) и правовой неопределенности в отношении передачи данных, что в сочетании со значительными штрафами и произвольной надзорной практикой создает неприемлемый регуляторный риск.

Локальное хранение и обработка данных (*Explicit local data storage and processing*). Государство явно запрещает трансграничную передачу данных.

Дискриминационное локальное хранение и обработка данных (*Discriminatory local storage and data processing*). Государство применяет дискриминационные лицензирование, сертификацию и другие нормативные ограничения, требующие локального хранения данных и полностью исключющие иностранные организации из процессов локального управления и обработки данных.





Норма о локализации	Содержание нормы
149-ФЗ ст.16 ч.4 п.7	Обладатель информации, оператор информационной системы в случаях, установленных законодательством РФ, обязаны обеспечить на территории РФ баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПД граждан РФ.
152-ФЗ ст.18 ч.5	При сборе ПД, в том числе посредством информационно-телекоммуникационной сети «Интернет», запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПД граждан РФ с использованием баз данных за пределами территории РФ не допускаются.
236-ФЗ ст.10 ч.4, ст.16	В случае неисполнения иностранным лицом, осуществляющим деятельность в сети «Интернет» на территории РФ, предусмотренной законодательством РФ в области ПД обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения ПД граждан РФ с использованием БД, находящихся на территории РФ, в отношении указанного иностранного лица могут применяться меры по запрету на сбор и трансграничную передачу ПД.
126-ФЗ ст.64 ч.1	Операторы связи обязаны хранить на территории РФ текстовые сообщения, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети «Интернет» и пользователей услугами связи – до 6 месяцев, а информацию о фактах приема, передачи, доставки и (или) обработки вышеуказанных данных – до 3 лет.
149-ФЗ ст.10.1 ч.3	Организаторы распространения информации в сети «Интернет» обязаны хранить на территории РФ текстовые сообщения, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети «Интернет» до 6 месяцев, а информацию о фактах приема, передачи, доставки и (или) обработки вышеуказанных данных – до 1 года.
87-ФЗ ст.4 п.6	Экспедитор обязан хранить на территории РФ информацию о заключенных договорах транспортной экспедиции, сторонах этих договоров, лицах, привлекаемых к выполнению этих договоров, свойствах грузов, фактах приема, обработки, погрузки, хранения, разгрузки, передачи, выдачи грузов, маршрутах следования, видах транспорта, осуществляющего их перевозку, иную информацию, размещаемую в информационных системах, используемых при оказании экспедиционных услуг, в течение 3 лет после окончания исполнения договоров.
Закон 4015-1 ст.29.1 п.5	Технические средства страховщика, используемые для хранения баз данных, должны размещаться на территории РФ.
580-ФЗ ст. 14 ч. 3 п. 3	Технические средства службы заказа легкового такси, которые используются для получения, хранения, обработки и передачи заказов легкового такси, базы данных должны размещаться на территории РФ.
381-ФЗ ст. 12¹ п.п. 2-3	Организатор исследований товарных рынков обязан осуществлять запись, систематизацию, накопление, хранение, анализ, извлечение информации, полученной в результате проведенных исследований, с использованием баз данных, находящихся на территории РФ, а также размещать на территории РФ технические средства, используемые для исследований товарных рынков.
ПП РФ №1393 п. 9 пп. «г»	Правообладатель автоматизированной информационной системы оформления воздушных перевозок должен иметь собственную инфраструктуру обеспечения полного жизненного цикла автоматизированной системы, находящуюся на территории РФ и под ее юрисдикцией.
ФСБУ 27/2021 п.25	Экономический субъект должен хранить документы бухгалтерского учета, а также данные, содержащиеся в таких документах, и размещать базы указанных данных на территории РФ. Если в месте ведения деятельности за пределами РФ есть требование хранения документов бухгалтерского учета на территории данной страны, то это хранение должно быть обеспечено.
Приказ ФСТЭК №239 п.31	Входящие в состав значимого объекта 1 и 2 категорий значимости программные и программно-аппаратные средства, осуществляющие хранение и обработку информации, должны размещаться на территории РФ (за исключением случаев, когда размещение указанных средств осуществляется в зарубежных обособленных подразделениях субъекта критической информационной инфраструктуры (филиалах, представительствах), а также случаев, установленных законодательством РФ и (или) международными договорами РФ)



**Privacy
Advocates**

Всегда рады сотрудничеству!

+7 (903) 762-64-15 | corp@privacy-advocates.ru | t.me/prv_adv



Telegram-канал