

Рациональный подход к выполнению требования о локализации баз с персональными данными в РФ

Актуальность материала: **07.01.2026**

Презентация "Рациональный подход к выполнению требования о локализации баз с персональными данными в РФ":

- Мировой опыт: ранжирование типов локализации по степени ограничения свободы оборота данных
- Локализация данных в РФ
- Эволюция требования о локализации баз с данными граждан РФ
- Комментарии к изменениям в требованиях о локализации
- Интерпретация Роскомнадзором уточненных требований о локализации
- Варианты интерпретации уточненных требований о локализации
- Компромиссная интерпретация уточненных требований о локализации
- Общие выводы по уточненным требованиям о локализации
- Ретроспектива правоприменительной практики 2016-2025гг.
- Определение БД с ПД
- Сбор ПД не как действие, а как единый процесс
- Сбор и иные способы получения ПД
- Декомпозиция источников ПД – на примере online-обучения
- Экспресс-схема определения подлежащих локализации БД
- Стратегии реагирования на требование локализации
- Сложности выбора стратегии локализации
- Походы к оценке стоимости стратегий локализации
- Оценка расходов на реализацию стратегий локализации
- Риски и последствия несоблюдения требований о локализации
- Оценка рисков при реализации стратегий локализации
- Формула оценки привлекательности стратегий
- Калькулятор оценки стратегий локализации
- Пример ранжирования стратегий локализации

□ Пример калькулятора расчета привлекательности стратегий локализации

Статья о сути и особенностях рационального подхода к выполнению требования о локализации баз с персональными данными в РФ

Автор: Алексей Витальевич Мунтян, генеральный директор ООО «Лекс Инжиниринг» (Privacy Advocates), соучредитель Общественного учреждения «Сообщество профессионалов в области инфоприватности» (RPPA.pro)

В статье рассмотрена сложившаяся в России регуляторная модель локализации баз персональных данных на фоне роста геополитической напряженности и в рамках стратегии цифрового суверенитета. Проведен анализ действующих нормативных требований к операторам по размещению и хранению персональных данных российских граждан на территории РФ. Выделены исключения для отдельных категорий операторов и ситуации, при которых локализация не требуется. Отдельное внимание уделено авторской методологии по идентификации подлежащих локализации баз данных и выбору оптимальных стратегий выполнения требований на основе риск-ориентированного подхода. Автор подчеркивает относительную гибкость действующих ограничений и отсутствие полного запрета на трансграничную передачу персональных данных после этапа их первоначального сбора. Анализируются позиции государственных органов и ключевые разъяснения профильных регуляторов относительно существа и практики применения требований локализации. Статья может быть полезна юристам, специалистам по информационной безопасности и лицам, ответственным за организацию обработки персональных данных.

Рост мировой геополитической напряженности в первой половине 2014 года между Россией и некоторыми зарубежными странами, взаимные и встречные санкции побудили российские власти выступить с рядом инициатив по обеспечению национальной безопасности. Одной из указанных инициатив стало вступившее в силу с 1 сентября 2015 года требование о так называемой локализации баз с персональными данными (ПД) на территории Российской Федерации.

В настоящем материале автором предпринята попытка описать существо, базовые принципы и особенности юридической обязанности операторов по размещению баз с персональными данными на территории РФ, а также изложить авторскую методологию по определению подлежащих локализации баз данных и рациональной оценке привлекательности возможных стратегий выполнения оператором требований по локализации на основе риск-ориентированного подхода.

1. Мировой опыт ограничения свободы оборота данных

В XXI веке требования локализации данных активно эволюционировали в сторону увеличения как диапазона охватываемых данных, так и количества стран. По оценке автора, число стран, которые ввели требования локализации данных, почти удвоилось с 35 в 2017 году до 82 в 2025 году. 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. Китай (33 требования), Индия (15), Россия (10) и Турция (9) —мировые лидеры по количеству требований локализации данных и их охвату.

Аргументация политиков и иных заинтересованных лиц в необходимости локализации данных постоянно меняется. Многие ранее поддерживали локализацию, глубоко не вникая в то, 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 в сфере обработки данных).

Можно выделить основные мотивы, используемые для обоснования политики локализации данных:

- обеспечение конфиденциальности и кибербезопасности (например, Индия);
- цифровой протекционизм и суверенитет данных (например, ЕС);
- контроль цифрового пространства (например, Китай);
- содействие местным правоохранительным и надзорным органам (например, Турция);
- геополитические риски и финансовые санкции (например, Россия).

Изучение действующих норм в различных странах позволяет сформулировать основные виды ограничений трансграничного оборота данных:

- 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.

Комбинации обозначенных выше видов ограничений трансграничного оборота данных позволяют установить и осуществить ранжирование пяти наиболее часто встречающихся типов локализации по степени ограничения свободы оборота данных (от меньшей к большей степени):

1. 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;
2. 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;
3. 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;
4. локальное хранение и обработка данных (Explicit local data storage and processing). Государство явно запрещает трансграничную передачу данных;
5. 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 исключающие иностранные организации из процессов локального управления и обработки данных.

2. Действующие в РФ требования о локализации данных

По состоянию на 31 июля 2025 года в России действовало порядка десятка норм о локализации данных, баз данных и технических средств, предназначенных для хранения и иной обработки данных (см. таблицу).

По результатам анализа вышеперечисленных требований о локализации данных можно сделать вывод, что регуляторная модель ограничения трансграничного оборота данных в России сочетает черты двух типов локализации данных — «локальная репликация данных» (Local data mirroring) и «локальное хранение данных» (Explicit local data storage), что свидетельствует об относительно мягком подходе российских властей к ограничению трансграничного оборота данных, в том числе персональных, по сравнению с некоторыми другими юрисдикциями.

3. Эволюция требования по размещению баз с персональными данными на территории России в 2014-2025 годах

Первого сентября 2015 года вступил в силу закон¹⁾, которым в ст. 18 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных) была добавлена ч. 5 следующего содержания: «При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона».

Это требование распространяется на всех операторов, за исключением некоторых случаев обработки персональных данных СМИ и органами государственной власти. К исключениям также относится п. 2 ч. 1 ст. 6 Закона о персональных данных в случаях обработки ПД «для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей». Однако, по нашему мнению, такое исключение может применяться только в тех случаях, когда на оператора прямо возлагается обязанность по сбору и дальнейшей обработке персональных данных за рубежом, так как в противном случае операторы получают возможность фактического игнорирования требования о локализации, ссылаясь на необходимость и (или) целесообразность

использования зарубежных баз для сбора ПД в целях надлежащего исполнения операторами собственных юридических обязанностей (например, посредством использования зарубежных сервисов для аутсорсинга ведения кадрового учета, предусмотренного трудовым законодательством РФ). Важная особенность положений ч. 5 ст. 18 Закона о персональных данных — акцент на гражданстве субъектов персональных данных. Ранее законодательство РФ было направлено на защиту прав субъектов персональных данных безотносительно их гражданства.

В случае если оператор поручает другому лицу обработку ПД, включая их сбор, указанное требование распространяется также и на это лицо. При этом оператор обязан обеспечить размещение данных на территории РФ.

Необходимо отметить, что требование распространяется только на обработку ПД при их сборе. Таким образом, последующие действия с персональными данными могут производиться в базах данных на территории иностранных государств. Кроме того, требования о локализации ПД граждан РФ при их сборе не затрагивают трансграничную передачу персональных данных, которая подлежит осуществлению в соответствии с требованиями статьи 12 Закона о персональных данных.

С 1 сентября 2022 года в ч. 3 ст. 6 Закона о персональных данных было уточнено²⁾ требование к договору о поручении обработки ПД, в котором отныне должна быть установлена обязанность лица, обрабатывающего персональные данные по поручению оператора (так называемого обработчика), соблюдать требования, предусмотренные ч. 5 ст. 18 Закона, а, согласно ч. 6 ст. 6 иностранные лица, являющиеся обработчиками для операторов в РФ, несут ответственность перед субъектами ПД в России наравне с отечественными операторами.

Наиболее существенно положения ч. 5 ст. 18 Закона о персональных данных изменились в 2025 году, актуальная редакция которой с 1 июля 2025 года выглядит следующим образом: «При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся за пределами территории Российской Федерации, не допускаются, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона»³⁾.

Представляется нелишним привести ряд наиболее показательных комментариев некоторых федеральных чиновников и политиков к изменениям в требованиях о локализации, которые в определенном смысле раскрывают контекст и мотивацию рассматриваемых изменений.

Вице-премьер Правительства РФ Дмитрий Григоренко: «Требования к обработке персональных данных россиян стали строже: с 1 июля их запрещено накапливать, хранить, обновлять в любых базах за пределами РФ. Поправки уточняют обязанности операторов... осуществлять обработку персональных данных граждан РФ с использованием различных баз данных исключительно на территории РФ. Прежнее регулирование позволяло операторам связи осуществлять хранение и обработку таких данных в том числе за пределами России, что не позволяло обеспечить надежную защиту персональных данных и создавало предпосылки к их утечке»⁴⁾.

Заместитель председателя Совета по развитию цифровой экономики при Совете Федерации РФ, сенатор Артем Шейкин: «Теперь за рубежом не должно быть даже копий баз с персональными данными россиян. Те компании, которые вели запись, систематизацию, накопление, хранение данных в зарубежных базах данных, должны использовать

инфраструктуру, расположенную в РФ»⁵⁾.

Член Комитета Госдумы по инфополитике, ИТ и связи, депутат Антон Немкин: «Это ужесточение законодательства не просто техническая мера, а элемент стратегии цифрового суверенитета. Существует и вероятность того, что какие-то зарубежные сервисы станут менее доступными для жителей РФ, но только в том случае, если они откажутся адаптироваться под требования закона... В этом случае у них есть выбор: либо они локализуют инфраструктуру в России, либо покидают рынок»⁶⁾.

Одним из наибольших опасений российских операторов стали потенциальные ограничения или запреты в отношении возможности осуществлять трансграничную передачу персональных данных, ранее собранных с использованием баз данных, находящихся на территории РФ, в случаях, установленных ч. 1 ст. 6 Закона о персональных данных. Но, по мнению Роскомнадзора⁷⁾, ч. 5 ст. 18 Закона о персональных данных таких ограничений не устанавливается.

Так, положения уточненной реакции ч. 5 ст. 18 Закона о персональных данных можно интерпретировать следующим образом: отныне локализация баз с собранными персональными данными граждан РФ превращается из позитивной обязанности, позволяющей размещать такие базы данных за рубежом после первичной локализации ранее собранных ПД, в императивный запрет размещать базы с персональными данными граждан РФ вне России. В контексте принятой в 2022 году нормы⁸⁾ об экстерриториальности применения российского законодательства в отношении обработки персональных данных иностранными лицами⁹⁾, а также сложившейся в 2022–2025 годах правоприменительной практики можно предположить нацеленность уточненной редакции требования о локализации в первую очередь на иностранные компании и сервисы, осуществляющие сбор ПД на территории РФ с самостоятельными целями или по поручению российских операторов. При этом российские операторы и обработчики с 1 июля 2025 года из-за возросших регуляторных рисков и (временной) правовой неопределенности будут пытаться не размещать собранные на территории РФ персональные данные в зарубежных базах данных, а также формально не признавать использование последних в обработке собранных в России ПД.

4. Интерпретация содержания и основные принципы выполнения юридической обязанности операторов по размещению баз с персональными данными на территории России

В начале августа 2015 года на сайте Минкомсвязи открылся раздел «Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года»¹⁰⁾. В нем есть ответы на вопросы, подготовленные на основании информации, которая получена от представителей бизнеса, научного сообщества и органов государственной власти (Совета Федерации, Минкомсвязи, Роскомнадзора). Роскомнадзор в ноябре 2016 года опубликовал свой комментарий, в том числе касательно ч. 5 ст. 18 Закона о персональных данных¹¹⁾. Следует обратить внимание, что публикуемые в этих источниках разъяснения иногда противоречат друг другу¹²⁾. Также нижеприведенные интерпретации норм не всегда могут считаться официальными разъяснениями, так как не все эти органы, например Роскомнадзор, наделены правомочием давать их.

Мы выделили десять тезисов из интерпретации Роскомнадзором и Минкомсвязью содержания ч. 5 ст. 18 Закона о персональных данных:

- нормы ч. 5 ст. 18 Закона о персональных данных распространяются на всех операторов в РФ;
- сбор персональных данных — это процесс целенаправленного получения данных непосредственно от субъекта или привлеченных для этого третьих лиц. Обязанность по их локализации в базе данных на территории РФ возникает только в период сбора ПД. Если, например, в зарубежной системе на основании собранных и локализованных в РФ данных о работнике определяется его грейд¹³⁾, делается вывод о необходимости направления работника на повышение квалификации или о его продвижении по службе, то такие ПД нельзя рассматривать как получаемые во время сбора, т.е. они не были получены от субъекта или через уполномоченных оператором лиц;
- база персональных данных — это упорядоченный массив ПД, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных);
- формирование и актуализация базы с персональными данными российских граждан в процессе их сбора должны осуществляться на территории РФ. Требования ч. 5 ст. 18 не позволяют осуществлять отдельные процедуры, в том числе хранение ПД, в базах данных на территории иностранного государства в процессе сбора персональных данных российских граждан;
- каждый случай, в котором при сборе ПД будет осуществляться одновременное хранение баз данных на территории РФ и иностранного государства, будет нарушением ч. 5 ст. 18, поскольку оператор при сборе персональных данных допустит их хранение в базах данных за пределами РФ. После сбора ПД, т.е. после формирования базы с персональными данными на территории РФ, недопустимо изменение условий ее хранения путем переноса такой базы данных на территорию иностранного государства;
- в ч. 5 ст. 18 отсутствует запрет на трансграничную передачу персональных данных. Обработка ПД посредством их передачи, в том числе на территорию иностранного государства, является трансграничной передачей. Допускается передача ПД российских граждан, содержащихся в базах данных, находящихся в РФ, в том числе на территорию иностранных государств, в порядке и в соответствии с условиями, определенными законодательством о ПД (см. ст. 12 Закона о персональных данных);
- информационная система персональных данных¹⁴⁾ может обладать географически распределенной структурой. Часть ее элементов может находиться за пределами РФ;
- оператор в РФ по-прежнему обладает правом поручить обработку ПД иностранному лицу и осуществлять их трансграничную передачу. Например, российские дочерние организации могут передавать персональные данные своих работников в зарубежные информационные системы и базы данных (HR-системы, ERP-системы и т.п.), операторами которых являются иностранные материнские компании или иные организации;
- обработка ПД для целей, не предусмотренных международным договором РФ или законом, может быть осуществлена оператором в рамках исполнения требований, предусмотренных ч. 5 ст. 18, путем размещения в центрах обработки данных на территории РФ базы данных, содержащей персональные данные граждан РФ, большего размера или аналогичного объема ПД, передаваемых на территорию иностранного государства;
- операторы должны самостоятельно определять процедуру установления гражданства субъекта персональных данных. Если у оператора возникли трудности или сомнения в правильной идентификации гражданства субъектов ПД, то он может осуществлять хранение персональных данных этих субъектов в базах данных, размещенных на территории РФ.

Таким образом, операторам, обрабатывающим или организующим обработку персональных данных граждан РФ, рекомендуется соблюдать следующие базовые принципы комплаенса для

соблюдения требований ч. 5 ст. 18 Закона о персональных данных:

1. сбор персональных данных, в том числе с территории иностранных государств, ведется только в базах данных на территории РФ;
2. объем и актуальность персональных данных, хранящихся в базах данных на территории РФ, должны быть равны или превосходить соответствующие показатели в отношении персональных данных, хранящихся в зарубежных базах данных;
3. получение новых персональных данных посредством использования (анализа) имеющихся персональных данных, которые были собраны в базах данных на территории РФ и переданы за рубеж, может производиться с помощью зарубежных баз данных и без предварительной локализации в РФ.

При этом соблюдения только этих базовых принципов будет недостаточно для определения подлежащих локализации баз данных и рациональной оценке привлекательности возможных стратегий выполнения оператором требований по локализации на основе риск-ориентированного подхода. Указанные вопросы будут более подробно рассмотрены в следующих разделах статьи.

5. Определение баз данных, подлежащих локализации

При определении понятия «база данных» следует учитывать, что в законодательстве и правоприменительной практике существует несколько вариантов его содержания, например:

- представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ)¹⁵⁾;
- совокупность взаимосвязанных данных, организованных в соответствии со схемой базы данных таким образом, чтобы с ними мог работать пользователь¹⁶⁾
- упорядоченный массив данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных), например таблица в формате Excel, в которой содержатся персональные данные¹⁷⁾.

Согласно п. 10 ст. 3 Закона о персональных данных информационная система персональных данных — это совокупность содержащихся в базе данных ПД и обеспечивающих их обработку информационных технологий и технических средств. Иначе говоря, база данных — неотъемлемый элемент информационной системы ПД. При определении массива данных, содержащего персональные данные, в качестве базы данных дополнительным квалифицирующим признаком является возможность формального определения базы данных в качестве составного элемента информационной системы персональных данных, расположенной на территории РФ.

Не менее важная задача для оператора — определение момента завершения сбора персональных данных и окончания применимости требования ч. 5 ст. 18 Закона о персональных данных. Так, согласно комментарию Роскомнадзора от 9 ноября 2016 года первичное формирование базы данных с собранными персональными данными на бумажных носителях с последующим их внесением в базу данных информационной системы персональных данных, используемую в целях, аналогичных сбору персональных данных на бумажных носителях, следует рассматривать как единый процесс; разделение указанного

единого процесса на отдельные действия законодательством РФ в области персональных данных не предусмотрено, и отдельные виды обработки персональных данных, предусмотренные ч. 5 ст. 18, должны осуществляться как единый процесс в правовом поле законодательной нормы, обязывающей хранить персональные данные на территории РФ.

Иными словами, определение момента завершения сбора персональных данных и окончания применимости требования ч. 5 ст. 18 — не самая тривиальная задача в силу сложности и комплексности некоторых процессов обработки персональных данных. То есть необходимо досконально изучать всю цепочку целенаправленных операций с персональными данными как «единого процесса» обработки ПД и быть готовым аргументированно, с доказательствами обосновать точку завершения их сбора. В качестве такой точки завершения сбора персональных данных представляется целесообразным обозначать расположенную на территории РФ базу данных, формально являющуюся составным элементом информационной системы персональных данных, расположенной на территории РФ. В противном случае оператор рискует столкнуться с негативной для него правоприменительной практикой. Например, в постановлении мирового судьи Таганского района города Москвы от 28 июля 2023 по делу № 5-1176/23 о привлечении компании Ookla LLC к административной ответственности за повторное невыполнение требования о локализации баз с персональными данными указано, что «конкретное нахождение баз данных (в том или ином государстве) доказыванию не подлежит», т.е. именно на операторе лежит бремя доказывания факта нахождения баз с ПД граждан РФ на территории РФ. Иначе говоря, добросовестность оператора судом не презюмируется.

При определении момента окончания сбора персональных данных оператору необходимо иметь четкое представление обо всех возможных способах их получения из различных источников и возможность разделить указанные способы получения на имеющие и не имеющие отношение к сбору ПД.

В качестве получаемых путем сбора можно определить следующие категории ПД:

1. предоставленные данные¹⁸⁾ — это персональные данные, полученные от физических лиц или их представителей, например путем заполнения физическими лицами веб-форм на сайте или представлением своего резюме при отзыве на вакансию;
2. распространенные данные¹⁹⁾ — это персональные данные, взятые из общедоступных или открытых источников, например путем исследования учетных записей пользователей в социальных сетях;
3. наблюдаемые данные²⁰⁾ — это персональные данные, фиксируемые путем отслеживания поведения физических лиц, например посредством онлайн-трекинга поведения пользователей интернет-ресурсов, сбора данных о геолокации, видеонаблюдения.

В качестве получаемых иным образом, отличным от сбора, можно определить следующие категории ПД:

1. принятые данные²¹⁾ — это персональные данные, полученные не от физических лиц или их представителей, а от других лиц, например рекомендация от бывшего или действующего работодателя соискателя;
2. инициированные данные²²⁾ — это персональные данные, образованные путем взаимодействия с физическими лицами (и) или совершения действий в их отношении, например заключение с договора физическим лицом или предъявление ему искового требования;
3. назначенные данные²³⁾ — это персональные данные, временно или постоянно присвоенные физическим лицам, например номер социального страхования,

наименование должности;

4. производные данные²⁴⁾ — это персональные данные, синтезированные после простого анализа других данных, например путем расчета прибыльности клиента по количеству посещений и купленных товаров;
5. предполагаемые данные²⁵⁾ — это персональные данные, спрогнозированные после продвинутого анализа наборов данных, например путем расчета кредитного рейтинга или прогнозирования состояния здоровья.

Далее вниманию читателей предлагается схема экспресс-определения подлежащих локализации баз с ПД (рис. 1), которая позволит оперативно, с минимальными трудозатратами и приемлемой точностью проанализировать большое количество баз данных. Как показывает наш десятилетний опыт применения схемы, она обладает точностью 95%, т.е. только в отношении каждой двадцатой проанализированной базы данных требуется проведение дополнительной оценки в отношении применимости требований о локализации.

Рис. 1. Схема экспресс-определения подлежащих локализации баз с персональными данными

К приведенной схеме необходимо добавить несколько примечаний: — направленность интернет-ресурса или мобильного приложения на территорию РФ ранее определялась в том числе адресом сайта в российской доменной зоне (.ru, .рф, .su, whois-service.ru/domains/?id=russian); русскоязычной версией пользовательского интерфейса; возможностью доставки товара, оказания услуги или пользования цифровым контентом в России. Но решение Второго КСОЮ от 26 декабря 2022 года по делу № 16-9987/2022 о сервисе Speedtest.net поставило под сомнение вышеприведенную практику, если на интернет-ресурсе или мобильном приложении отсутствуют какие-либо ограничения для прохождения процедуры регистрации российских пользователей; — требования о локализации подпадают под исключение в случаях, указанных в п. 2, 3, 4, 8 ч. 1 ст. 6 Закона о персональных данных.

6. Способы (стратегии) выполнения требований по локализации

В связи с противоречивостью и фрагментарностью правоприменительной практики и комментариев уполномоченных органов затруднительно сделать однозначные выводы об оптимальных стратегиях выполнения требований к обработке персональных данных операторами, обладающими базами с ПД российских граждан за пределами территории РФ.

Можно выделить десять возможных стратегий выполнения требований ч. 5 ст. 18 Закона о персональных данных, которые также допустимо комбинировать. Они сфокусированы на вопросах логики распределения информационных потоков с ПД внутри и между базами данных и информационными системами, но также в некоторых случаях затрагивают и вопросы правового характера.

Перечислим возможные стратегии выполнения требований по локализации, а также проиллюстрируем их соответствующими принципиальными схемами (см. рис. 2):

1. перенос зарубежной информационной системы ПД целиком в РФ;
2. отказ от автоматизированной обработки ПД;
3. отделение базы данных от иностранных серверов приложений и перенос базы данных в РФ;
4. создание в РФ промежуточной базы данных для сбора, хранения, актуализации и трансграничной передачи ПД;
5. квалификация системы как не имеющей базы данных для сбора ПД и используемой как сервис коммуникации/передачи ПД;
6. передача статуса оператора ПД иностранному лицу, формально не представленному в РФ;
7. обезличивание или шифрование ПД при сборе в зарубежную базу данных;
8. сбор ПД в зарубежную базу данных с последующей их репликацией в российскую базу данных;
9. одновременный параллельный сбор ПД в российскую и зарубежную базы данных;
10. отказ от модификации системы и связанных с ней потоков ПД в зарубежных базах данных.

Рис. 2. Принципиальные схемы возможных стратегий выполнения требований по локализации

Следует дать дополнительные пояснения к некоторым из стратегий и к схеме в целом:

- стратегия № 4 подразумевает создание на территории РФ промежуточной информационной системы или базы данных с целью хранения, уточнения, удаления собираемых в России ПД и их последующей передачи для обработки другому оператору, в том числе за границу. Процессы в зарубежных системах (например, в глобальных системах международных холдингов и групп компаний), связанные с последующей

обработкой персональных данных, сохраняются неизменными или адаптируются для автоматического использования данных из России;

- стратегия № 6 подразумевает отказ от процесса обработки ПД с помощью организации — российского резидента. Она реализуется путем прямого сбора, систематизации, обновления и хранения персональных данных с помощью организации за пределами России, которая будет квалифицироваться в качестве оператора, осуществляющего обработку ПД от своего имени и под свою ответственность;
- каждая из десяти стратегий, отображенных на схеме, имеет соответствующую цветовую индикацию своего краткого описания, которая коррелирует величине сопутствующих юридических (комплаенс) рисков. Так, стратегия № 1 обозначена ярко-зеленым цветом, что демонстрирует ее безрисковость для оператора. Выбор же стратегии № 10 чреват наибольшим риском среди всех, поэтому ее описание имеет темно-красный цвет.

Перечисленные стратегии формировались исходя из презумпции, что обработка ПД при осуществлении процедур по обеспечению непрерывности информационно-технологической инфраструктуры и восстановления ее после сбоев, при разработке и тестировании программных модулей информационных систем, сервисов, платформ и ресурсов не регулируется напрямую ч. 5 ст. 18 Закона о персональных данных. Это предположение основывается на следующем доводе: в рамках резервной информационно-технологической инфраструктуры сред разработки и тестирования программных модулей систем и сервисов не осуществляется сбор ПД субъектов. Персональные данные передаются в указанную инфраструктуру и среды из иных баз с ними. Для минимизации юридических рисков, связанных с обработкой ПД в указанных случаях оператору рекомендуется рассмотреть возможность применения технологий защищенной обработки данных, в том числе шифрования.

7. Оценки привлекательности стратегий выполнения требований по локализации

Оценка стратегий выполняется в отношении только тех систем, базы данных (включающие ПД) которых полностью или частично располагаются за пределами РФ. Выбор той или иной стратегии выполнения требований по локализации основывается на принципе оценки расходов оператора на ее реализацию и минимизации вероятного ущерба оператору. Учитываются как расходы на реализацию стратегии ([CapEx](#)), так и регулярные (ежегодные) расходы на ее поддержание на весь период жизненного цикла ([OpEx](#)). При этом вероятный ущерб оператору условно подразделяется на материальные потери (административные штрафы, удовлетворенные иски, требования к оператору, договорные санкции в отношении оператора), практический ущерб (например, по причине исполнения предписания о модификации процесса обработки ПД в сжатые сроки) и репутационный вред (утрата лояльности клиентов и партнеров, недоверие потенциальных контрагентов и инвесторов, негативный образ оператора в СМИ).

Для просчета рисков, сопутствующих применению стратегий выполнения требований по локализации, необходимо оценить вероятность выявления правонарушения (обнаружить несоответствие могут Роскомнадзор и органы прокуратуры РФ, субъекты ПД, контрагенты оператора и иные лица) и дальнейшего доказывания этого факта в суде. Для этого требуется оценить степень соответствия стратегии требованиям ч. 5 ст. 18 Закона о персональных данных с точки зрения уполномоченных органов, опирающихся на собственное ведомственное мнение, и судов, руководствующихся юридической трактовкой и внутренним убеждением. При

оценке рисков применяется допущение, что в течение жизненного цикла стратегий проверка со стороны уполномоченных органов будет проведена как минимум один раз.

Отметим, что нет необходимости учитывать возможность нарушения оператором требования об уведомлении Роскомнадзора о месте нахождения баз данных, содержащих ПД граждан РФ, предусмотренного п. 10.1 ч. 3 ст. 22 Закона о персональных данных, и привлечения его к ответственности по ч. 10 ст. 13.11 КоАП РФ или по ст. 19.7 КоАП РФ, поскольку указанная обязанность должна быть исполнена оператором вне зависимости от выбора стратегии.

Привлекательность стратегии определяется по формуле, позволяющей оценить величину расходов на ее реализацию:

$C_i + O_i \times T_{lc} + P_{det,i} \times P_{V,i} \times P_{C,i} \times M \times S_1 + P_{det,i} \times P_{V,i} \times P_{M,i} \times D$, где:

C_i — однократные расходы при реализации стратегии i ([CapEx](#));

O_i — периодические расходы при реализации стратегии i ([OpEx](#));

T_{lc} — ожидаемый период жизненного цикла реализации стратегии;

$P_{det,i}$ — вероятность обнаружения баз данных надзорным органом при реализации стратегии i ;

$P_{V,i}$ — вероятность выявления нарушений в обнаруженной базе данных по результатам проверки при реализации стратегии i ;

$P_{C,i}$ — вероятность подтверждения нарушений в обнаруженной базе данных судом при реализации стратегии i ;

M — мультипликатор влияния на бизнес;

S_1 — расходы на реализацию стратегии 1, включая периодические за период жизненного цикла;

$P_{M,i}$ — вероятность публикации информации о нарушении при реализации стратегии i ;

D — совокупность возможных материальных потерь, практического ущерба и репутационного вреда для оператора.

Влияние на бизнес выражается в виде расходов на реализацию стратегии, умноженных на мультипликатор. Мультипликатор зависит от критичности системы для бизнеса, сложности переноса системы, вовлеченности ее в основные бизнес-процессы и находится в промежутке от 1 до 3 единиц.

Вероятность обнаружения баз данных определяется экспертным способом и зависит в первую очередь от того, был ли уведомлен Роскомнадзор о рассматриваемой базе с персональными данными, а также от вовлеченности такой базы в деятельность оператора, и оценивается по шкале от 0 до 100%. Для основных бизнес-процессов вероятность обнаружения базы данных выше. Вероятность выявления нарушения требований по локализации зависит от реализованной стратегии и компетентности проверяющих. Вероятность публикации информации о нарушении (в том числе на интернет-порталах надзорных органов и в СМИ) зависит от значимости нарушения, степени вовлеченности базы данных в основные процессы оператора, а также от известности самого оператора.

С примерами подготовки калькулятора для автоматизированной оценки стратегий локализации и визуального отображения результатов ранжирования стратегий локализации по степени их привлекательности можно ознакомиться по ссылке ниже.

□ Пример калькулятора расчета привлекательности стратегий локализации

A rational approach to complying with the Russian data localisation law

This article analyses Russia's regulatory framework on the localisation of personal data storage amid rising geopolitical tensions and the country's drive for digital sovereignty. The study systematically reviews the key legislative requirements mandating that operators who process personal data of Russian citizens ensure such data is stored within the Russian Federation. The article elaborates on the risk-based methodology proposed for identifying which databases are subject to localisation and how organisations can rationally evaluate compliance strategies. The author emphasises that the current legal approach is relatively flexible: initial collection and storage must occur locally, but subsequent cross-border data transfers are not entirely prohibited. The analysis includes exceptions for specific types of operators and processing scenarios. The structure of the article covers the legal basis for localisation, categorisation of affected databases and strategic guidance for compliance. The findings are particularly relevant for legal practitioners, IT security experts, and data protection officers. Keywords: personal data localisation, personal data databases, Russian localisation laws, Federal Law No. 152-FZ „On Personal Data“, cross-border data transfer, digital sovereignty, data storage regulation, data storage in Russia, international data localisation experience.

INFORMATION ABOUT THE AUTHOR: Alexey V. Muntyan, Chief Executive Officer of LLC „Lex Engineering“ (Privacy Advocates), co-founder of the Public Institution „Community of Information Privacy Professionals“ (RPPA.pro)

[трансграница, локализация, сайты, системы, надзор, ответственность, приземление](#)

1)

Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».

2)

Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон „О персональных данных“, отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона „О банках и банковской деятельности“». URL: <http://publication.pravo.gov.ru/document/0001202207140080> (дата обращения: 26.08.2025).

3)

Федеральный закон от 28.02.2025 № 23-ФЗ «О внесении изменений в Федеральный закон „О персональных данных“ и отдельные законодательные акты Российской Федерации».

4)

См.: Персональные данные россиян запретили хранить на любых базах за рубежом / ТАСС. 2025. 1 марта. URL: <https://tass.ru/obschestvo/23279147> (дата обращения: 26.08.2025).

5)

См.: Сенатор Шейкин рассказал о запрете хранить данные россиян на зарубежных серверах / ТАСС. 2025. 28 февр. URL: <https://tass.ru/obschestvo/23267235> (дата обращения: 26.08.2025).

6)

См.: Капустина Л. Персональные данные россиян нельзя будет хранить за рубежом. Как это скажется на использовании мессенджеров и соцсетей / РГ. 2025. 29 июня. URL: <https://rg.ru/2025/06/29/deputat-rabotu-servisov-ne-obespechivshih-hranenie-dannyh-v-rf-mogut-ogra>

[nichit.html](#) (дата обращения: 26.08.2025).

7)

См.: письмо Роскомнадзора от 24.03.2025 № 134789 «О рассмотрении обращения».

8)

См.: Федеральный закон от 14.07.2022 № 266-ФЗ.

9)

См.: ч. 1.1 ст. 1 Закона № 152-ФЗ, а также вывод в решении Второго КСОЮ от 26.12.2022 по делу № 16-9987/2022 о привлечении компании Ookla LLC к административной ответственности за нелокализацию баз с персональными данными граждан РФ (ч. 8 ст. 13.11 КоАП РФ) в рамках сервиса Speedtest, который хотя прямо не направлен на российскую аудиторию (отсутствуют русскоязычная версия пользовательского интерфейса, Политика конфиденциальности на русском языке, возможность осуществления расчетов в российской валюте и доставки каких-либо товаров на территории РФ), но на сайте speedtest.net нет каких-либо ограничений для прохождения процедуры регистрации российских пользователей, поэтому суд посчитал применимыми требования о локализации.

10)

В настоящее время сайт <http://minsvyaz.ru/ru/personaldata/> недоступен. Копия Разъяснения размещено на интернет-портале RPPA — Общественного учреждения «Сообщество профессионалов в области приватности». См.: Разъяснения Минкомсвязи России от 25.08.2015 «Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года согласно положениям 242-ФЗ». URL: https://rppa.pro/npa/minkomsvyaz_25.08.2015 (дата обращения: 26.08.2025).

11)

См.: Комментарий Роскомнадзора от 09.11.2016 к Федеральному закону от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». URL: https://pd.rkn.gov.ru/docs/Kommentarij_242-FZ_final.docx (дата обращения: 26.08.2025).

12)

Например, Минкомсвязь указывает, что понятие «база данных» на уровне федерального закона раскрыто в абз. 2 ст. 1260 ГК РФ следующим образом: «Базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины». Тут же ведомство поясняет, что при применении ч. 5 ст. 18 Закона № 152-ФЗ под термином «база данных» будет пониматься указанное выше значение, предполагающее, что с помощью ЭВМ одновременно должны быть обеспечены поиск и любая обработка соответствующей информации, что представляется возможным при условии их наличия в электронной форме. Роскомнадзор придерживается мнения, что следует руководствоваться понятием, которое дано в Модельном законе о персональных данных, принятом в Санкт-Петербурге 16.10.1999 постановлением № 14-19 на 14-м пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ: «База персональных данных — упорядоченный массив персональных данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных)». Такое понимание базы данных позволяет распространить требования законодательства о персональных данных на все материалы, содержащие персональные данные, вне зависимости от того, каким образом они скомпонованы и в каком формате обрабатываются — бумажном или электронном.

13)

Грейд (от англ. grade — «уровень, ступень») — система ранжирования должностей в компании по определенным критериям.

14)

См.: п. 10 ст. 3 Закона о персональных данных.

¹⁵⁾

См.: ст. 1260 ГК РФ.

¹⁶⁾

См.: п. 2.1 ГОСТ 34.321-96 «Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными». В том же ГОСТе даны определения термина «схема базы данных»: «Формальное описание данных в соответствии с конкретной схемой данных» и термина «схема данных»: «Логическое представление организации данных». Персональные данные в сообщениях электронной почты содержатся в теле передаваемых сообщений и прикрепленных к сообщениям документах. Данные в документах и теле сообщений неоднородны, не структурированы, не взаимосвязаны, т.е. не организованы логически — не являются частью схемы данных и схемы базы данных. Следовательно, ПД в теле сообщений и прикрепленных документах не входят в состав базы данных, и потому электронная почта не подпадает под определение информационной системы персональных данных (в части сообщений и прикрепленных документов).

¹⁷⁾

См.: Комментарий Роскомнадзора от 09.11.2016 к Федеральному закону от 21.07.2014 № 242-ФЗ.

¹⁸⁾

Сбор персональных данных означает, что оператор или специально привлеченное оператором для этого третье лицо должны их получать непосредственно у первоисточника, т.е. у субъекта персональных данных или его представителя (см.: Комментарий Роскомнадзора от 09.11.2016 к Федеральному закону от 21.07.2014 № 242-ФЗ).

¹⁹⁾

На сбор ПД из общедоступных источников требования ч. 5 ст. 18 Закона о персональных данных распространяются в полном объеме (см. там же).

²⁰⁾

См.: решение Таганского районного суда от 19.12.2018 по делу № 02-4261/2018 о блокировке сайта «Умное голосование» из-за использования сервисов Google Analytics и «Яндекс.Метрика», а также решение Второго КСОЮ от 26.12.2022 по делу № 16-9987/2022 о сервисе Speedtest.net и отнесении сведений о сетевой активности пользователя, cookies, идентификаторов устройства к персональным данным.

²¹⁾

За исключением случаев, когда оператор получает ПД от третьего лица, специально привлеченного оператором для их сбора (см.: Разъяснения Минкомсвязи России от 25.08.2015 «Обработка и хранение персональных данных в РФ...»).

²²⁾ ²³⁾ ²⁴⁾ ²⁵⁾

Эти виды сведений можно квалифицировать как созданные путем использования имеющихся ПД, так как под «использованием персональных данных» можно понимать действия с персональными данными, не относящиеся к иным формам обработки данных (см.: Разъяснения Минкомсвязи России от 25.08.2015 «Обработка и хранение персональных данных в РФ...»).

From:

<https://wiki.privacy-advocates.ru/> - Privacy Advocates | Альманах

Permanent link:

https://wiki.privacy-advocates.ru/lokalizacija_racio

Last update: **2026/10/01 17:07**

