Comply.Pulse

Под запретом теперь не только лишь все зарубежные ИТ-сервисы

С 1 июля 2025 года вступили в силу очередные изменения Федерального закона «О персональных данных» № 152-ФЗ (далее – 152-ФЗ). В этот раз правили часть 5 статьи 18, известную как требование о локализации. С учетом этих изменений ответим на несколько вопросов по локализации и трансграничной передаче персональных данных (далее – ПД). А в конце лонг-рида традиционно делимся практическими рекомендациями для минимизации рисков.

Как было прежде?

Ранее сбор и последующая обработка ПД граждан РФ должны были осуществляться с использованием баз данных, физически находящихся на территории России.

Из-за тотального ужаса и непонимания, как дальше жить с этим требованием, в августе 2015 года появились разъяснения Минкомсвязи России (ныне Минцифры). Хоть эти разъяснения впоследствии и были отозваны с официального сайта ведомства, в них было прямо предусмотрено, что компании могли создавать промежуточные базы данных в России, а основную обработку допускалось проводить за рубежом.

Фактически требование подразумевало, что база данных в России никогда не должна была уступать зарубежной ни по объему, ни по актуальности. На практике это означало, как минимум, следующее:

- Обеспечение последовательности загрузки данных при сборе: сначала данные загружаются на сервер в России и только затем – на зарубежный. Необходимо иметь возможность подтвердить это логами с отметками о времени сохранения данных в обеих базах данных.
- Аналогичную последовательность требовалось обеспечить при любых изменениях ранее собранных данных. Например, при переводе сотрудника на другую позицию или возврате клиентом товара на маркетплейсе такие обновленные данные требуется «локализовать» сперва в российской базе данных, и только затем передать в зарубежную.
- При уничтожении требовалось соблюдать обратную последовательность. Сперва обеспечить удаление данных из зарубежной базы и только затем из российской. Это было необходимо, чтобы избежать ситуации, когда российская база в какой-то момент содержит меньше данных, что является нарушением.

К слову, не все ПД нужно было таким образом «локализовывать», а только те, что собраны оператором от субъекта в результате целенаправленной деятельности. Более того, существенная часть ПД, получаемая от других юридических лиц, например, в рамках отношений «оператор-оператор» или, в отдельных случаях, по поручению – не подлежат обязательной локализации. Локализация не требуется и для производных данных, сформированных на основе ранее собранной информации. Например, это касается назначения сегмента клиенту по истории его покупок.

Если соблюдались эти правила, то можно было без проблем осуществлять трансграничную передачу ПД и использовать зарубежные сервисы. Проверки Роскомнадзора и суды лишь подтверждали это. Такая логика работала на практике, как минимум, до 1 июля.

При этом спойлер – обратите внимание, что многим так любимые сервисы, например, Google (reCAPTCHA, аналитика, формы) и их аналоги – конечно же, и прежде НЕ соответствовали требованиям о локализации по мнению Роскомнадзора. Иными словами, для них ситуация 1 июля не изменилась.

Требование о локализации распространяется не только на российских операторов, но и на иностранные компании, в т. ч. не имеющие официального присутствия в России, но отвечающие критерию направленности деятельности. Такой критерий был сформулирован в тех же разъяснениях Минкомсвязи. Так, для применения к иностранной компании требования о локализации необходимо наличие базовых и любого дополнительного критерия:

Базовые критерии	Вторичные критерии
• использование российского доменного имени (.ru, .su, .рф) кроме случаев отсутствия последующего фактического использования сайта; • наличие русскоязычного интерфейса исключая автоматический перевод на русский язык.	• возможность осуществления расчетов в российских рублях; • исполнение договора на территории РФ; • наличие рекламы на русском языке и другие аналогичные признаки; • иные обстоятельства, например, наличие на сайте способа обратной связи, связанного с Россией.

Оператор может делегировать локализацию ПД своему обработчику по поручению. В этом случае на такого обработчика также распространяется требование о локализации, что прямо предусмотрено в ч. 3 ст. 6 152-ФЗ. Соответственно, этот обработчик будет нести договорную ответственность перед оператором за нарушение поручения. Более того, если привлекается иностранный обработчик, то он несет ответственность перед субъектами ПД и Роскомнадзором наравне с оператором (ч. 6 ст. 6 152-ФЗ).

Что изменилось по буквам?

Итак, как было, мы вспомнили. А вот наглядное сравнение было-стало с частью 5 статьи 18 152-ФЗ:

*«При сборе ПД, в том числе посредством сети «Интернет», **~~оператор обязан обеспечить~~** запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПД граждан РФ с использованием баз данных, **~~находящихся на~~** **за пределами** территории РФ, **не допускаются**, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона».*

На первый взгляд, изменения носят скорее косметический характер. При сравнении старой и новой редакций кажется, что суть осталась прежней. При сборе ПД граждан РФ ранее оператор был обязан обеспечить их обработку в базах, расположенных на территории России, а теперь – запрещено использовать зарубежные базы данных при сборе ПД. Но ключевое, что, как и раньше, такое ограничение действует только на один этап обработки данных – при сборе.

Выражения «обязан обеспечить» и «не допускается» содержат одинаковое императивное требование осуществлять сбор ПД в России, но новая формулировка звучит, пожалуй, ультимативно.

Но тогда зачем?

Такими нововведениями, возможно, в очередной раз хотели простимулировать бизнес перейти на российские ИТ-системы, обеспечивая цифровой суверенитет России. А возможно, это и не так... А возможно, следующим шагом будет реализация инициативы обязать всех операторов ПД перейти на отечественное ПО, включая системы управления базами данных (СУБД). Таково поручение премьер-министра Минцифре, ФСБ и ФСТЭК. Эта инициатива выглядит как дальнейшее развитие тренда дата-национализации. Если само требование хранить и обрабатывать ПД исключительно в России уже создало юридические барьеры для использования зарубежных баз данных и ИТ-сервисов, то запрет на иностранное ПО окончательно «формирует» контур цифрового суверенитета, делая обработку ПД за пределами российского технологического стека не только нежелательной, но и технически/юридически маловозможной.

И все же считать эти шаги частью одной цепи мешает хаотичное принятие новой поправки к требованию о локализации. Ведь изначально редакция законопроекта не предусматривала никаких изменений в требование о локализации. Правка в часть 5 статьи 18 152-ФЗ была внесена только ко второму чтению. И, как следствие, в пояснительной записке к законопроекту отсутствует какое-либо упоминание о том, как и зачем вносятся эти изменения, что, конечно же, затрудняет оценку и выглядит серьезным недостатком законодательного процесса.

Сложившаяся ранее практика не ставила под сомнение возможность операторов использовать иностранные ИТ-системы при соблюдении формального требования иметь и поддерживать первоначальный «слепок» данных на территории России. На практике компании применяли разные сценарии локализации ПД (разные по степени комплаенса и сложности их внедрения), например:

Сценарий локализации ПД	Комплаенс до 1 июля 2025	Выполнимость
Исключение загрузки ПД в ИТ-систему	●●●	●○○
Перенос БД в РФ	●●●	●○○
Автоматизированный перенос ПД из локальной БД в зарубежную	●●●	●●○
Технический перехват ПД в промежуточную базу в РФ перед отправкой в зарубежную систему (interceptor)	●●○	●●○
Ручная загрузка ПД в дублирующую локальную БД	●●○	●●●
Ручная загрузка данных в excel-файл	●○○	●●●
Параллельная обработка ПД на бумажных носителях (договоры, картотеки)	○○○	●●●

Хотят ли в действительности государственные органы эту наработанную практику изменить? Если они нацелены не только на локализацию баз данных, но и на локализацию процесса их обработки, то нас всех, бесспорно, ждут крайне интересные события!

Ещё до вступления изменений в силу нововведения вызвали обеспокоенность у бизнеса. Представители государственных ведомств поспешили внести ясность. Да еще как, смотрите сами:

Сенатор Артем Шейкин: *«Базы с информацией граждан должны находиться на территории России и не иметь копий за ее пределами».*
Член комитета Госдумы Антон Немкин: *«…либо они локализуют инфраструктуру в России, либо покидают рынок».*
Сенатор Владимир Булавин: *«…персональные данные граждан РФ должны обрабатываться с использованием баз данных, расположенных исключительно на территории России, без возможности их дублирования за рубежом…».*

То были радикальные настроения о запрете всякой зарубежной обработки ПД, но есть и более умеренные позиции.

Так, на мероприятиях Роскомнадзора была озвучена позиция контролирующего органа, что существенных изменений не произошло, а дело лишь в уточнении формулировки (например, встреча в Центре евразийского сотрудничества, а также Научно-практический юридический форум СПбГУ).

Более того, в индивидуальных разъяснениях Роскомнадзора от 24.03.2025 г. № 08–134789 и Минцифры от 12.05.2025 г. № П25-44929 указывалось:

«Ограничения на осуществление трансграничной передачи персональных данных, ранее собранных с использованием баз данных, находящихся на территории Российской Федерации, в случаях, установленных ч. 1 ст. 6 Закона, указанной нормой не устанавливаются».

Таким образом, оба ведомства придерживаются единого мнения: передавать ПД за границу можно при соблюдении установленных правил. Хорошо, что у обоих государственных органов единая позиция на сей счет. Это свидетельствует хоть отчасти о предсказуемости правоприменения, что важно для бизнеса.

И что это все-таки значит?

Опасения бизнеса насчет запрета осуществлять трансграничную передачу ПД идут вразрез с тем же самым положением 152-ФЗ о допустимости трансграничной передачи ПД. Не будем вспоминать и Конвенцию № 108, подписантом которой все еще является Россия, и которая прямо разрешает трансграничную передачу. Более того, в обновленной статье нет запрета на использование полученных при сборе и зафиксированных в российской базе ПД с использованием зарубежных баз после их сбора, а также на их передачу или предоставление. Поэтому передавать данные за рубеж по-прежнему можно. Но что же тогда изменилось, спросите вы.

Изменения могут быть вполне практические, хоть и не столь драматичные, если придерживаться более умеренного взгляда, как это делают Роскомнадзор и Минцифры, без радикальных интерпретаций. Хотя, как уже отмечали выше, есть риск, что нарратив нововведений не столько о локализации баз данных, сколько о процессах их обработки. Разбираемся в «глубине» локализации.

Требование о локализации «опыляет» процесс сбора ПД. То есть нет запрета на обработку ПД в зарубежных базах вне рамок сбора ПД, а при сборе запрещено. Возникает вопрос, что же такое сбор ПД, где он начинается и заканчивается?

В законодательстве нет определения понятия «сбор» ПД. Но к нашему удовольствию ранее опубликованные и прежде доступные разъяснения Минкомсвязи содержали несколько опусов на сей счет, а именно:

«…под сбором можно понимать целенаправленный процесс получения персональных данных оператором непосредственно от субъекта персональных данных, либо через специально привлеченных для этого третьих лиц…».

Очень хорошо, что эта формулировка есть, так как существенно ограничивает периметр сбора. Например, не будет сбором:

- получение ПД от другой компании в рамках взаимодействия по модели «оператор-оператор»;
- перенос ПД из одной ИТ-системы в другую внутри инфраструктуры компании;
- случайное (незапрошенное) попадание ПД к компании, а также…
- генерация производных данных компанией.

Но есть еще и такая формулировка в указанных разъяснениях Минцифры:

«…внесение персональных данных в информационную систему персональных данных, используемую в целях, аналогичных сбору данных на бумажных носителях, следует рассматривать как единый процесс, реализация которого должна осуществляться в строгом соответствии с требованиями части 5 статьи 18 Федерального закона № 152-ФЗ…».

Исходя из этого, и в зависимости от радикальности взглядов интерпретатора, формулировка «при сборе» может распространяться на всю последующую обработку ПД. Это фактически запрещает любую зарубежную обработку лицом, собравшим такие ПД, для тех целей обработки ПД, которые им заявлялись при сборе.

К сожалению, существует и судебная практика, в которой судами принимаются еще более смелые суждения о единстве и неразрывности процесса сбора и последующей обработки ПД. Так, в решении Фрунзенского районного суда города Санкт-Петербурга от 01.03.2022 г. по делу № 12-228/2022 отмечалось:

«*…каждый случай, при котором при сборе персональных данных будет осуществляться одновременное хранение баз данных на территории РФ и иностранного государства, будет являться нарушением Федерального закона № 242, поскольку оператор при сборе персональных данных допустит их хранение в базах данных за пределами РФ, после сбора персональных данных, то есть после формирования на территории РФ недопустимы изменения условий ее хранения путем переноса баз данных на территорию иностранного государства…*».

Но мы, с учетом недавних ответов Минцифры и Роскомнадзора, не придерживаемся таких радикальных взглядов.

Что же делать в такой ситуации?

Пока четкая позиция не сформирована, однозначного вывода из имеющегося контекста сделать не получится. Но, исходя из умеренной интерпретации обновленного требования, разъяснений контролирующего и регулирующего органов и с долей оптимизма полагаем необходимым убедиться в следующих мерах:

1. Отделимость сбора от иных действий с ПД

Чтобы передать данные за рубеж и там же их обрабатывать, это должен быть отдельный процесс обработки ПД. Иными словами, передача ПД иностранным сервисам и компаниям возможна, если процесс передачи им ПД отделен от этапа сбора ПД, а процесс обработки ПД, включающий сбор данных, всегда заканчивается в России.

Пример такого разделения процессов обработки данных: российская компания передает ПД своих работников в зарубежные Workday или SAP HR для обучения и развития. В этом случае сбор данных не происходит, поскольку российская компания собрала ПД работников на этапе трудоустройства для целей их оформления и онбординга, например, в 1С ЗУП, а теперь передает в иностранную ИТ-систему

ранее собранные данные для иной цели. То есть это разные процессы обработки, где первый включает сбор и загрузку данных в 1С, а второй – не включает сбор, но включает передачу данных в Workday или SAP HR (если, конечно, при этом не появляется новый объем данных).

Таким образом, для корректного применения обновленного требования о локализации следует четко разделять процессы обработки ПД, в которых осуществляется сбор ПД и те, в которых сбора ПД нет. По нашему опыту, зачастую такое разделение процессов логически оправдано. Ранее компании, руководствуясь оптимизацией трудозатрат DPO-функции, например, по сбору согласий или уведомлению Роскомнадзора, укрупняли цели обработки ПД. Теперь же следует аккуратно посмотреть на описание процессов обработки ПД в реестрах процессов (RoPA) и дробить описание тех процессов, в которых используются зарубежные базы данных. На практике это может выглядеть следующим образом (на примере описания процесса в RoPA):

Цель обработки	Подцели обработки	Сбор ПД	ТГП	Компоненты ИСПД
Оформление трудоустройства	Составление и заключение трудового договора	Да	~~HQ (Германия)~~ Нет	БОСС-кадровик ~~Workday~~ ~~SAP HR~~ SmartКЭДО
Обучение и развитие персонала	Организация обучения Оценка работников	Нет	HQ (Германия)	Workday
Управление персоналом	Планирование рабочего процесса и ресурсов Обеспечение кадровой отчетности	Нет	HQ (Германия)	SAP HR

Важно, чтобы обоснование отсутствия сбора было убедительным и правдоподобным для Роскомнадзора. Попытки искусственно дробить стандартный процесс на множество мелких этапов могут быть расценены как нарушение.

Кроме того, привлечение обработчика за рубежом с последующей передачей собранных им ПД в Россию будет нарушением требования о локализации. Дело в том, что первичная обработка ПД в этом случае осуществляется не в России, и, очевидно, в интересах оператора.

В этом контексте безопаснее передавать ПД зарубежному оператору, чем обработчику по поручению. Ведь самостоятельный оператор, получивший данные, обрабатывает ПД для собственных целей в рамках отдельного процесса, который не связан непосредственно со сбором ПД. Тогда как доказать «отделимость от сбора» обработки ПД обработчиком – сложнее.

2. Технический сценарий локализации

Существует достаточно распространённый технический сценарий обеспечения локализации ПД, известный как «interceptor» или «перехватчик» – перехватывающая техническая база данных. В рамках этого подхода компания использует зарубежную ИТ-систему, но до того, как данные попадут в зарубежную базу, они перехватываются промежуточной базой, которая развернута на российских серверах. Такая база является «технической», потому что у нее ограниченный бизнес-функционал – только хранение данных для обеспечения локализации и, в лучшем случае, аналог бэкапа.

Ранее Роскомнадзор, в т. ч. при выездных проверках, тщательно изучал такой сценарий и не высказывал претензий, поскольку можно было подтвердить правильную последовательность обработки ПД и их локализацию с помощью логов и технической документации.

Однако теперь, с учётом изменений, применение этого сценария становится более рискованным. Вряд ли получится убедить контролирующий орган, что сбор данных заканчивается именно загрузкой их в «перехватчик». Ведь «перехватчик» представляет собой техническую базу данных, не имеющую самостоятельной бизнес-цели, кроме как обеспечения требований локализации. То есть цель обработки ПД на уровне «перехватчика» не будет достигнута.

Рекомендуется тщательно проверить сценарии локализации для сервисов и процессов, к которым применимо требование о локализации, и, на основании этого, принять решение о дальнейшем использовании или корректировке существующих процессов и ИТ-инфраструктуры.

Кто теперь в зоне риска?

Напомним, что штраф за несоблюдение требования о локализации достигает 6 млн рублей за первое нарушение и 18 млн рублей за повторное.

Любопытно, что в КоАП РФ (ч. 8 и 9 ст. 13.11) сохранилась формулировка старой редакции: обязанность оператора обеспечить обработку на территории России вместо ультимативного запрета, как предусматривает обновленное требование о локализации. Пожалуй, это в очередной раз должно свидетельствовать о сохранении прежних подходов правоприменения в части локализации.

Еще раз, любой иностранный сервис, связанный с обработкой ПД, как прежде, так и сегодня сопряжен с рисками их локализации и трансграничной передачи. В этом смысле с 1 июля не изменилось ровным счетом ничего.

На текущий момент судебная практика в большинстве ситуаций привлекает к ответственности владельцев иностранных ИТ-сервисов за нарушение требований локализации, а не компании, использующие эти сервисы (Zoom, Discord, Ookla LLC, Badoo Trading Limited).

Действует мораторий на плановые проверки Роскомнадзора. Но мораторий на внеплановые проверки прекратился с 1 января. Кроме того, у Роскомнадзора есть широкий арсенал инструментов для выявления нарушений, включая автоматический мониторинг сайтов, направление запросов, жалобы субъектов и прочее. Не так давно Минцифры дополнило перечень индикаторов риска двумя фактами неуведомления Роскомнадзора о трансграничной передаче ПД. Все это несколько повышает риск внеплановой проверки Роскомнадзора.

Наконец, нельзя исключить изменения ритма и фокуса контрольно-надзорной деятельности в части локализации ПД в связи с изменениями этого требования.

В любом случае необходимо быть готовыми к получению запросов от контролирующего органа и иметь возможность оперативно предоставить доказательства соблюдения требований по локализации, как минимум, в отношении публично видимых процессов обработки ПД, например, на сайтах. Это позволит минимизировать риски и обеспечить прозрачность взаимодействия с контролирующими органами.

Подведем итоги

Итак, формулировка требования изменилась. Пока сложно с уверенностью сказать, как ее будут на практике интерпретировать контролирующие органы. Но, исходя из имеющихся разъяснений

Роскомнадзора и Минцифры, все же предлагаем пока не занимать радикальную позицию и не «выключать из розетки» все зарубежные сервисы.

Тем не менее, ожидая с тревогой, куда же качнется маятник правоприменения, следует себя обезопасить и выполнить сегодня, как минимум, следующее:

- **Маппинг процессов.** Провести детальный анализ всех бизнес-процессов, в рамках которых происходит и сбор ПД, и взаимодействие с зарубежными базами данных. Необходимо описать каждый процесс, составив реестр процессов (RoPA), если его вдруг еще нет. Это позволит понять, к каким процессам и системам применимо требование о локализации и зафиксировать «на бумаге» логичное разделение процессов, в которых используются зарубежные базы данных и нет сбора ПД, а в каких есть сбор ПД, но нет зарубежных баз данных.
- **Параметры локализации.** Если по результатам анализа принято решение о необходимости локализации, следующим шагом необходимо определить параметры локализации. Важно понять, какие именно данные используются в процессе, какие из них могут обновляться, выступает ли компания самостоятельным оператором или нет, источник получения этих ПД (субъект или нет) и др. На основе этих параметров принимается решение о том, в отношении какого объема данных внутри ИТ-системы требуется локализация. Это позволит реализовать требования законодательства с наименьшими затратами.
- **Техническая локализация.** Определить наиболее подходящий способ технической локализации для каждого процесса. Ранее использовавшийся метод с применением перехватчика данных (interceptor) теперь будет более рискованным. В связи с этим необходимо провести аудит инфраструктуры и понять, каким образом фактически обеспечивается локализация ПД.
- **Defense-файл.** Внимание следует уделить анализу логов, блок-схем и технической документации, а также убедиться, что есть договоры с хостинг-провайдерами или документы, подтверждающие владение собственными серверами. Именно с этими документами предстоит защищаться в случае претензий Роскомнадзора.
- **Договорные обязательства.** Убедиться, что в договорах с провайдерами (особенно зарубежными) предусмотрены требования о локализации данных, включая описание потоков данных и ИТ-архитектуры, исключающих сбор ПД напрямую в зарубежные базы данных, запрет на одностороннее изменение контрагентом порядка обработки данных, ответственность и компенсацию убытков при нарушении таких требований.

И, конечно, после всесторонней оценки рисков, связанных с обновленным требованием о локализации, необходимо оценить стоимость реализации плана «Б», если маятник всё же качнется в сторону более радикальной позиции – тотальная локализация процессов обработки ПД в России.

Артем Дмитриев
Управляющий партнер

artem.dmitriev@comply.ru
+7 961 806 27 76
t.me/artydmitriev

Подписаться на Comply в Telegram