КРОСС
ТЕХНОЛОДЖИС

Аналитическая справка
IV квартал 2025 г.

Новые требования к обезличиванию персональных данных

Автор: Елизавета Сорокина – младший консультант Департамента аудита, консалтинга и оценки соответствия

Введение

С 1 сентября 2025 года вступили в силу изменения в нормативно-правовых актах Российской Федерации (далее – НПА РФ), касающиеся обработки обезличенных персональных данных (далее – ПДн). Значительным изменениям подвергся Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – 152-ФЗ).

Целью внесения изменений является регулирование обработки обезличенных ПДн при их передаче по требованию государства в определенных случаях (глава 1 данной статьи), а также введение правил обезличивания ПДн для собственных нужд операторов ПДн (глава 2 данной статьи).

В этой справке мы детально рассказываем об изменениях и проводим рекомендации для бизнеса. Постатейная аналитика изменений в 152-ФЗ приведена в Приложении 1.

Содержание

Глава 1. Обезличивание ПДн по требованию государства для ГИС

Значение для компаний

С 1 сентября 2025 года по требованию уполномоченного органа по регулированию в сфере информационных технологий (Минцифры России) операторов ПДн могут обязать предоставлять обезличенные сведения в федеральную государственную информационную систему «Единая информационная платформа национальной системы управления данными» (далее – ФГИС ЕИП НСУД), созданную Правительством РФ. Такое требование должно содержать перечень полученных в результате обезличивания ПДн, а также сроки их предоставления.

Проще говоря, если государству понадобятся большие массивы данных для аналитики или социальных проектов, оно будет запрашивать у обладателей данных обезличенные наборы сведений, а не ПДн в чистом виде. Например, могут затребовать у банков агрегированные транзакции, у операторов связи — статистику по звонкам и тому подобное, но всё в таком виде, чтобы нельзя было определить по таким данным конкретного человека.

Таким образом, изменения, внесённые в 152-ФЗ, расширяют законные возможности для работы с обезличенными персональными данными в рамках государственного сектора.

Также даётся конкретное определение, что такое обезличенные ПДн, — данные, обезличенные по требованиям НПА РФ, которые диктуют определенные методы процесса обезличивания, обязательные для всех, кто работает с ФГИС ЕИП НСУД.

Вводится понятие «состав обезличенных данных» — то есть набор ПДн, сгруппированных по определённым признакам, который обезличен настолько, что дальнейшая обработка не позволит установить, кому конкретно они принадлежат. При этом оговаривается, что формирование составов данных будет осуществляться Минцифры России исключительно в случаях, определенных Постановлением Правительства Российской Федерации от 24.04.2025 № 538 «Об утверждении перечня случаев формирования составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определенному признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных» (далее – 538-ПП).

Также установлено, что:

- формирование наборов данных из специальных категорий ПДн (за исключением ПДн, предусмотренных ч. 2.1 ст. 10 152-ФЗ) и биометрических ПДн не допускается;
- доступ к составам данных предоставляется только пользователям ФГИС ЕИП НСУД;
- обработка составов данных пользователями ФГИС ЕИП НСУД осуществляется только в этой системе – запись, извлечение, передача (распространение, предоставление, доступ) составов данных из системы на допускаются;
- по общему правилу запрещается предоставление результатов обработки составов данных иностранным юридическим лицам, иностранным организациям, не являющимся юрлицами, иностранным гражданам и лицам без гражданства.

Основные положения

- Определены в числе прочего порядок обезличивания ПДн и порядок предоставления доступа к ним; обязанности оператора ПДн; требования, которым должны соответствовать граждане РФ и российские юридические лица – пользователи ФГИС ЕИП НСУД, и правила предоставления обезличенных ПДн для неё.

- Введен запрет обработки составов данных и получения результатов обработки составов данных, если их использование может повлечь причинение вреда жизни, здоровью людей, оскорбление нравственности, нарушение прав и законных интересов граждан и организаций, причинение ущерба окружающей среде, обороне страны и безопасности государства, объектам культурного наследия, иным охраняемым законом ценностям.

Особый порядок и контроль

ФГИС ЕИП НСУД, в которую среди прочих входит «подсистема обработки обезличенных данных» (подробнее см. Постановление Правительства РФ от 14.05.2021 г. № 733 «Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении изменений в некоторые акты Правительства Российской Федерации» (далее – 733-ПП)), создана в целях повышения эффективности обмена и использования государственных данных для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, а также в целях повышения эффективности государственного и муниципального управления.

Законодатель при создании данной системы уделил особое внимание защите прав граждан при обмене обезличенными ПДн: введён механизм уведомления субъектов ПДн о планируемой передаче их сведений даже в обезличенном виде, с правом возражения. Такой подход позволяет сбалансировать интересы государства в анализе больших данных и право человека контролировать информацию о себе. Кроме того, доступ к обезличенным данным, размещенным в ФГИС ЕИП НСУД, получат только доверенные лица и организации: ни иностранные компании (за исключением случаев, определенных международным договором РФ, федеральным законом, решением Президента РФ), ни организации с неопределённым статусом собственности, ни люди с судимостями за киберпреступления допущены не будут. Это сделано для снижения рисков утечек и злоупотреблений при дальнейшем использовании обезличенных данных.

Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности ПДн при их обработке по-прежнему осуществляются Роскомнадзором, ФСБ России и ФСТЭК России в пределах их полномочий.

На какие НПА РФ обратить внимание

- Федеральный закон от 08.08.2024 г. № 233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» (далее – 233-ФЗ);
- Постановление Правительства РФ от 14.05.2021 г. № 733 «Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении изменений в некоторые акты Правительства Российской Федерации»;
- Постановление Правительства РФ от 24.04.2025 г. № 538 «Об утверждении перечня случаев формирования составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определенному признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных»;
- Постановление Правительства РФ от 26.06.2025 г. № 961 «О формировании составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определенному признаку, при условии, что последующая обработка таких

данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных, и предоставлении доступа к составам таких данных» (вместе с «Правилами формирования составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определенному признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных», «Правилами предоставления доступа к составам персональных данных, полученных в результате обезличивания персональных данных, сгруппированным по определенному признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных»);

- Постановление Правительства РФ от 01.08.2025 г. № 1154 «Об утверждении требований к обезличиванию персональных данных, методов обезличивания персональных данных и Правил обезличивания персональных данных» (далее – 1154-ПП).

Глава 2. Обезличивание для собственных нужд операторов ПДн

Основные положения

- Допускается использование методов обезличивания ПДн, за исключением случаев, указанных в пункте 9.1 части 1 статьи 6 152-ФЗ.
- Операторам ПДн предписывается определять заранее, какие данные и чьи данные будут обезличиваться.
- В результате обезличивания ПДн должно быть невозможно определить, какому субъекту принадлежат ПДн (без использования дополнительной информации).
- Необходимо оценить достаточность выбранного метода обезличивания для достижения целей обработки данных, полученных в результате процедуры.
- При использовании программ для обезличивания ПДн должна обеспечиваться безопасность и конфиденциальность как подлежащих обезличиванию ПДн, так и полученных в результате процедуры данных.
- Не допускать третьих лиц к данным о регламентах и методах обезличивания, а также к данным об используемых программах для обезличивания ПДн.
- Необходимо исключить совместное хранение массива ПДн, подлежащих обезличиванию, и полученных в результате процедуры обезличенных данных.
- Необходимо вести учёт всех действий по обезличиванию ПДн, а также операций, которые совершаются с полученными в результате процедуры обезличенными данными. Форма такого учёта определяется оператором ПДн, но она должна позволять подтвердить исполнение процедуры обезличивания.
- Операторам ПДн необходимо разработать и утвердить локальные нормативные акты (далее – ЛНА), которые устанавливают порядок обработки ПДн, подлежащих обезличиванию. Эти документы должны регламентировать порядок обезличивания, применяемые методы, алгоритмы, оценки достаточности и тому подобное. ЛНА должны храниться отдельно от обезличенных ПДн и быть недоступными третьим лицам.

Методы обезличивания

При осуществлении обезличивания ПДн допустимо применять по отдельности или в совокупности следующие методы:

- Метод введения идентификаторов.
- Метод изменения состава или семантики ПДн, а именно:
  - удаление атрибутов ПДн;
  - искажение атрибутов ПДн;
  - изменение атрибутов ПДн.
- Метод перемешивания: реализуется путем перестановки отдельных значений и (или) групп значений атрибутов ПДн между собой.
- Метод декомпозиции: реализуется путем разделения массива ПДн, подлежащих обезличиванию, на заданное оператором ПДн количество частей с последующим раздельным их хранением.

На какие НПА РФ обратить внимание

- Приказ Роскомнадзора от 19.06.2025 г. № 140 «Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных, за исключением случаев, указанных в пункте 9.1 части 1 статьи 6 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных» (далее – Приказ № 140).

Глава 3. Когда необходимо обезличивать ПДн

Обезличивание ПДн в ряде случаев не просто право, а прямая обязанность оператора ПДн, закреплённая законом. Ниже перечислены некоторые случаи, когда данные обязательно должны быть обезличены (или уничтожены) во избежание нарушения закона:

1. По требованию уполномоченного органа. Как упоминалось, с 2025 года вводится обязанность операторов ПДн предоставлять государству обезличенные сведения. То есть, если Минцифры России (или ДИТ Москвы – для столичных структур) направит требование о предоставлении данных в ФГИС ЕИП НСУД, оператор ПДн обязан выполнить обезличивание и предоставить данные именно в обезличенном виде. Предоставить необезличенные ПДн даже госорганам нельзя — закон требует именно предварительной анонимизации перед загрузкой сведений в ФГИС ЕИП НСУД. Невыполнение такого требования приравнивается к нарушению (об ответственности за это - ниже).

В этом случае обезличивание необходимо проводить с учетом требований 1154-ПП.

2. По достижении цели обработки ПДн. Согласно 152-ФЗ, после достижения изначальной цели, ради которой собирались данные, дальнейшее их хранение недопустимо (если иное не предусмотрено НПА РФ). Оператор ПДн обязан либо уничтожить такие данные, либо перевести их в обезличенный формат.

В этом случае обезличивание необходимо проводить с учетом требований Приказа № 140.

3. При передаче данных третьим лицам. Если организация хочет передать данные по взаимодействию с клиентами сторонней компании, например, для аналитики. Передавать полный набор клиентских данных избыточно, но можно передать совокупную обезличенную

статистику. Однако в этом случае до передачи необходимо проверить наличие правового основания этих действий, ведь обезличивание – это вид обработки, а для любой обработки нужна легитимная цель и правовое основание из ст. 6 152-ФЗ.

В этом случае обезличивание необходимо проводить с учетом требований Приказа № 140.

Глава 4. Что делать операторам ПДн в связи с изменениями

Новые правила обезличивания данных требуют от операторов ПДн заблаговременной подготовки. Им уже сейчас рекомендуется начать приводить свои процессы в соответствие с изменениями. Ниже приведены рекомендации, которые помогут подготовиться:

- **Разработать или обновить внутренние политики и инструкции.** Если оператор ПДн планирует осуществлять обезличивание ПДн, но у него ещё нет отдельного локального акта, регламентирующего порядок обезличивания, его необходимо утвердить. В документе следует прописать: какие данные подлежат обезличиванию, в каких случаях; как выбирается метод обезличивания; как оценивается достаточность обезличивания; как хранятся и защищаются обезличенные данные. Также необходимо внести изменения в Политику обработки ПДн, добавив положения об обезличивании.
- **Определить и внедрить подходящие методы обезличивания.** Проанализировать, какие из официально утверждённых методов, лучше подходят под существующие наборы данных.
- **Закрепить методы во внутренних актах.** После выбора конкретных методов закон требует формализовать их. Например, при использовании метода изменения состава/семантики данных утвердить отдельный порядок, описывающий, какие атрибуты удаляются или искажаются и как именно. При использовании метода перемешивания — утвердить алгоритм перестановки записей (на сколько позиций сдвигаются значения и тому подобное). При декомпозиции — определить правила разбиения и места раздельного хранения частей данных. Все эти документы должны быть внутренними, храниться отдельно и быть недоступными для посторонних. Также необходимо назначить ответственных за их ведение и актуализацию.
- **Настроить раздельное хранение данных.** Проверить архитектуру информационных систем: оригинальные ПДн и обезличенные должны храниться раздельно. Возможно, потребуются изменения — например, выделить отдельный сегмент или базу для обезличенных наборов, ограничить к ним доступ. Держать таблицы соответствия идентификаторов и реальных данных в защищённом хранилище с ограниченным кругом доступа. В идеале сразу после обезличивания выгружать данные в отдельное место, а исходные удалять (если они больше не нужны для текущих процессов).
- **Назначить ответственных за работу с ФГИС ЕИП НСУД.** Если организация подпадает под требования (например, является оператором больших массивов клиентских данных), целесообразно определить работника или подразделение, которое будет отвечать за взаимодействие с ФГИС ЕИП НСУД. Этот ответственный должен понимать порядок выполнения требований: как принять запрос Минцифры России, в какие сроки подготовить данные, как их загрузить в систему. Возможно, потребуется настроить техническое подключение к ФГИС ЕИП НСУД через СМЭВ (систему межведомственного электронного взаимодействия) — т.е. необходимо проверить, есть ли в организации такая возможность, либо обратиться за разъяснениями в Минцифры России.
- **Обновить договоры**. Если для анализа данных или обезличивания привлекаются внешние подрядчики, убедиться, что в договоре с ними есть обязательство соблюдать все требования закона (например, не получать доступ к исходным данным без необходимости). В случае

передачи ПДн для обезличивания подрядчику, проверить, не нужно ли получить согласие субъектов ПДн на передачу их данных третьим лицам.

- **Обучить персонал**. Ознакомить работников с новыми локальными актами и провести обучение: объяснить новые правила обезличивания, подчеркнуть запрет на хранение вместе ПДн и анонимизированных данных, а также запрет делиться техникой обезличивания.

Глава 5. Какие санкции предусмотрены за нарушение или неисполнение новых требований

Последствия нарушения правил обезличивания ПДн зависят от конкретного нарушения и включают в себя административные штрафы, которые могут достигать нескольких миллионов рублей для юридических лиц и индивидуальных предпринимателей, а также уголовную ответственность по статье 137 УК РФ, предусматривающую лишение свободы на срок до четырех лет, если действия привели к разглашению тайны частной жизни.

Административная ответственность (КоАП РФ)

За утечку ПДн субъектов или уникальных обозначений сведений о физических лицах предусмотрен штраф для юридических лиц до 15 000 000 рублей согласно ч. 12, 13, 14 ст. 13.11 КоАП РФ. При повторном совершении аналогичных нарушений, предусмотренных указанными частями, санкции ужесточаются: в соответствии с ч. 15 той же статьи, возможен штраф в размере до 3% от выручки юридического лица, но не менее 20 000 000 рублей.

За действия (или бездействие) оператора, повлекшие неправомерную передачу ПДн, отнесённых к специальной категории (например, данные о здоровье, религиозных убеждениях, политических взглядах и пр.) и за утечку биометрических ПДн (например, фотографии, голос, отпечатки пальцев, сетчатка глаза и пр.) для юридических лиц предусмотрен штраф в размере до 20 000 000 рублей, в соответствии с ч. 16, 17 ст. 13.11 КоАП РФ. Если лицо, ранее уже подвергнутое административному наказанию за нарушение требований ч. 12–18 ст. 13.11 КоАП РФ, вновь допускает утечку специальных или биометрических ПДн, то в этом случае устанавливается значительно более строгая санкция: штраф до 3% выручки юридического лица, но не менее 25 000 000 рублей.

В целях минимизации потенциальных рисков и предотвращения финансовых потерь, связанных с утечкой ПДн, компания Кросс технолоджис разработала специализированный калькулятор для расчёта возможных штрафов: https://crosstech.ru/calculation/.

Уголовная ответственность (УК РФ)

Статья 137 УК РФ «Нарушение неприкосновенности частной жизни» предусматривает ответственность, если действия с персональными данными были направлены на разглашение сведений, составляющих тайну частной жизни, в публичном выступлении, произведении или СМИ.

- Нарушение наказывается штрафом в размере до 200 000 рублей или в размере заработной платы осужденного за период до 18 месяцев.
- Также могут быть назначены обязательные работы на срок до 480 часов.
- Возможно лишение права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.
- Максимальное наказание – лишение свободы на срок до двух лет.

Иные последствия

Гражданско-правовая ответственность возникает, если в результате неправомерных действий причинены убытки или моральный вред физическим лицам.

Поможем подготовиться к изменениям

Если вам нужно провести оценку соответствия требованиям регуляторов, подключиться к центру ГосСОПКА, спланировать переход на российские СЗИ, провести пентест или решить любые другие задачи ИБ, напишите нам:

Написать

КРОСС ТЕХНОЛОДЖИС

Приложение 1

Изменения в Федеральном законе от 27.07.2006г. № 152-ФЗ «О персональных данных»

Глава 2. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ	
Статья 6. Условия обработки персональных данных	
БЫЛО	**СТАЛО**
9.1) обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления, ~~а также~~ в иных целях, предусмотренных Федеральным законом от 24 апреля 2020 года № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» и Федеральным законом от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», в порядке и на условиях, которые предусмотрены указанными федеральными законами;	9.1) обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления, в иных целях, предусмотренных Федеральным законом от 24 апреля 2020 года № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве, об особенностях обработки персональных данных при формировании региональных составов данных и предоставления доступа к региональным составам данных и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» и Федеральным законом от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», в порядке и на условиях, которые предусмотрены указанными федеральными законами, а также в целях, предусмотренных федеральными законами, указанными в части 1 статьи 4 настоящего Федерального закона, в порядке и на условиях, которые предусмотрены статьей 13.1 настоящего Федерального закона;
2.1. Обработка персональных данных, касающихся состояния здоровья, полученных в результате обезличивания персональных данных, допускается в целях повышения эффективности государственного или муниципального управления, а также в ~~иных~~ целях, предусмотренных Федеральным законом от 24 апреля 2020 года № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» и	2.1. Обработка персональных данных, касающихся состояния здоровья, полученных в результате обезличивания персональных данных, допускается в целях повышения эффективности государственного или муниципального управления в порядке и на условиях, которые предусмотрены статьей 13.1 настоящего Федерального закона, а также в целях, предусмотренных Федеральным законом от 24 апреля 2020 года № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве, об особенностях обработки персональных данных при формировании региональных составов данных и предоставления доступа к региональным составам данных и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» и Федеральным законом от 31 июля 2020 года № 258-ФЗ

Федеральным законом от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», в порядке и на условиях, которые предусмотрены указанными федеральными законами.	«Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», в порядке и на условиях, которые предусмотрены указанными федеральными законами.
Глава 2 **СТАЛО**	
Статья 13.1. Особенности обработки персональных данных, полученных в результате обезличивания персональных данных, при формировании составов данных и предоставления доступа к ним (введена Федеральным законом от 08.08.2024 3 233-ФЗ) 1. Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий (далее – уполномоченный орган в сфере регулирования информационных технологий), в целях повышения эффективности государственного и муниципального управления, а также в иных целях, предусмотренных федеральными законами, указанными в части 1 статьи 4 настоящего Федерального закона, в случаях, определяемых Правительством Российской Федерации, формирует составы персональных данных, полученных в результате обезличивания персональных данных, сгруппированные по определенному признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных (далее – составы данных). Не допускается формирование составов данных из персональных данных, указанных в статье 10 настоящего Федерального закона, за исключением персональных данных, предусмотренных частью 2.1 статьи 10 настоящего Федерального закона, и из персональных данных, указанных в статье 11 настоящего Федерального закона. 2. Для формирования составов данных уполномоченный орган в сфере регулирования информационных технологий направляет операторам, за исключением случаев, предусмотренных статьей 6.2 Федерального закона от 24 апреля 2020 года № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве, об особенностях обработки персональных данных при формировании региональных составов данных и предоставления доступа к региональным составам данных и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных», требование о предоставлении персональных данных, полученных в результате обезличивания персональных данных, в определяемую Правительством Российской Федерации государственную информационную систему уполномоченного органа в сфере регулирования информационных технологий. Указанное требование должно содержать перечень персональных данных, полученных в результате обезличивания персональных данных, которые предоставляются оператором для формирования составов данных, а также сроки их предоставления. 3. Оператор после получения требования, указанного в части 2 настоящей статьи, обязан обезличить обрабатываемые им персональные данные в соответствии с требованиями к обезличиванию персональных данных, методами обезличивания персональных данных и порядком обезличивания персональных данных, которые устанавливаются Правительством Российской Федерации по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (далее – требования к обезличиванию). Выполнение оператором	

требований к обезличиванию должно исключить наличие в персональных данных, полученных в результате обезличивания, информации, доступ к которой ограничен федеральными законами.

4. Оператор в соответствии с требованием, указанным в части 2 настоящей статьи, обязан предоставить персональные данные, полученные в результате обезличивания персональных данных, в государственную информационную систему уполномоченного органа в сфере регулирования информационных технологий. Порядок взаимодействия уполномоченного органа в сфере регулирования информационных технологий с операторами и порядок взаимодействия государственной информационной системы уполномоченного органа в сфере регулирования информационных технологий и информационных систем операторов устанавливаются Правительством Российской Федерации по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности. Уполномоченный орган в сфере регулирования информационных технологий обязан обеспечивать конфиденциальность поступивших от операторов персональных данных, полученных в результате обезличивания персональных данных.

5. Уполномоченный орган в сфере регулирования информационных технологий после поступления от операторов персональных данных, полученных в результате обезличивания персональных данных, формирует составы данных в государственной информационной системе уполномоченного органа в сфере регулирования информационных технологий в соответствии с порядком формирования составов данных, устанавливаемым Правительством Российской Федерации по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

6. Доступ к составам данных предоставляется пользователям государственной информационной системы уполномоченного органа в сфере регулирования информационных технологий в соответствии с порядком, устанавливаемым Правительством Российской Федерации по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

7. Пользователями государственной информационной системы уполномоченного органа в сфере регулирования информационных технологий являются:

1) государственные органы и подведомственные им организации, муниципальные органы и подведомственные им организации, органы государственных внебюджетных фондов;

2) граждане Российской Федерации и российские юридические лица, которые соответствуют следующим требованиям:

а) сведения о гражданине Российской Федерации или юридическом лице внесены в реестр операторов в соответствии со статьей 22 настоящего Федерального закона;

б) юридическое лицо является российским юридическим лицом, которое, если иное не предусмотрено международным договором Российской Федерации, находится под контролем Российской Федерации, и (или) субъекта Российской Федерации, и (или) муниципального образования, и (или) гражданина Российской Федерации, не имеющего гражданства другого государства, и (или) контролируемых ими совместно или по отдельности лиц. При этом под контролем понимается возможность определять решения, принимаемые юридическим лицом, в силу наличия права прямо или косвенно распоряжаться более чем пятьюдесятью процентами общего количества голосов, приходящихся на голосующие акции (доли), составляющие уставный капитал данного юридического лица;

в) в едином государственном реестре юридических лиц отсутствует запись о недостоверности сведений о юридическом лице;

г) сведения о гражданине Российской Федерации или юридическом лице, его единоличном исполнительном органе, членах коллегиального исполнительного органа не включены в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, или в перечни организаций и физических лиц, связанных с террористическими организациями и террористами или с распространением оружия массового уничтожения, указанные в Федеральном законе от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

д) отсутствие у гражданина Российской Федерации или единоличного исполнительного органа юридического лица гражданства иностранного государства;

е) отсутствие у гражданина Российской Федерации или единоличного исполнительного органа юридического лица неснятой или непогашенной судимости за совершение преступления;

ж) гражданин Российской Федерации или единоличный исполнительный орган юридического лица не привлекался в течение пяти лет, предшествующих дню предоставления доступа к государственной информационной системе уполномоченного органа в сфере регулирования информационных технологий, к уголовной ответственности в соответствии со статьями 183, 272, 273, 274.1, 283 и 283.1 Уголовного кодекса Российской Федерации.

8. Порядок проверки соответствия пользователей государственной информационной системы уполномоченного органа в сфере регулирования информационных технологий требованиям, указанным в части 7 настоящей статьи, устанавливается Правительством Российской Федерации по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

9. Доступ к составам данных, сформированным из персональных данных, полученных в результате обезличивания персональных данных, переданных операторами, не являющимися государственными органами и подведомственными им организациями, муниципальными органами и подведомственными им организациями, органами государственных внебюджетных фондов, в случае, если такие персональные данные собраны, уточнены (обновлены, изменены) указанными операторами в течение трех лет до дня предоставления в государственную информационную систему уполномоченного органа в сфере регулирования информационных технологий, предоставляется только пользователям, указанным в пункте 1 части 7 настоящей статьи. Пользователям, указанным в пункте 2 части 7 настоящей статьи, доступ к таким составам данных предоставляется по истечении одного года со дня предоставления персональных данных, полученных в результате обезличивания персональных данных, из которых они сформированы, в государственную информационную систему уполномоченного органа в сфере регулирования информационных технологий.

10. Обработка составов данных пользователями государственной информационной системы уполномоченного органа в сфере регулирования информационных технологий осуществляется только в указанной информационной системе. Не допускаются запись, извлечение, передача (распространение, предоставление, доступ) составов данных из государственной информационной системы уполномоченного органа в сфере регулирования информационных технологий.

11. Не допускаются обработка составов данных и получение результатов обработки составов данных, если использование таких составов данных и результатов их обработки может повлечь причинение вреда жизни, здоровью людей, оскорбление нравственности, нарушение прав и законных интересов граждан и организаций, причинение вреда (ущерба) окружающей среде, обороне страны и безопасности государства, объектам культурного наследия, иным охраняемым законом ценностям. В случае, если использование результатов обработки составов данных может повлечь причинение

вреда обороне страны и безопасности государства, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, вправе принять решение о запрете предоставлять такие результаты обработки составов данных. 12. Не допускается предоставление результатов обработки составов данных иностранным юридическим лицам, иностранным организациям, не являющимся юридическими лицами, иностранным гражданам и лицам без гражданства, за исключением случаев, определенных международным договором Российской Федерации, федеральным законом, решением Президента Российской Федерации.
Статья 23. Уполномоченный орган по защите прав субъектов персональных данных **СТАЛО**
12. Уполномоченный орган по защите прав субъектов персональных данных устанавливает требования к обезличиванию персональных данных и методы обезличивания персональных данных, за исключением случаев, указанных в пункте 9.1 части 1 статьи 6 настоящего Федерального закона.