

УТВЕРЖДЕНО:

Приказом Генерального директора
№ 3 от «14» апреля 2026г

ПОЛОЖЕНИЕ

**об обработке персональных данных в Автономной некоммерческой организации "Центр
регионального развития, реализации социально значимых проектов и поддержки
общественных инициатив "Территория добра"**

Горно-Алтайск, 2026

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных в Автономной некоммерческой организации "Центр регионального развития, реализации социально значимых проектов и поддержки общественных инициатив "Территория добра" (далее — Положение) разработано с учетом требований Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Закон №152-ФЗ) и принятых в соответствии с ним нормативных правовых актов, а также с учетом положений локальных нормативных актов Организации по вопросам обработки и защиты ПДн и устанавливает общие требования к организации обработки персональных данных (далее – ПДн) в Автономной некоммерческой организации "Центр регионального развития, реализации социально значимых проектов и поддержки общественных инициатив "Территория добра" (далее – Организация), а также определяет порядок и условия обработки ПДн, в т.ч. требования к обработке ПДн.

1.2. Требования, изложенные в Положении, распространяются на автоматизированную и неавтоматизированную обработку ПДн в процессах и информационных системах Организации, и являются обязательными для выполнения всеми работниками и должностными лицами Организации, обрабатывающими ПДн, при этом исполнение должностных обязанностей не должно являться основанием для нарушения пунктов данного Положения и других документов, регламентирующих в Организации вопросы обработки ПДн.

1.3. Ознакомление работников Организации с настоящим Положением, в т.ч. с изменениями настоящего Положения, осуществляется под подпись.

2. Термины и определения

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники

Блокирование ПДн – временное прекращение обработки ПДн (кроме хранения), в т.ч. по требованию Субъекта ПДн или Надзорного органа.

Доступ к ПДн – возможность получения ПДн и их использования.

Извлечение ПДн – действия или процесс извлечения ПДн из источников для последующей обработки.

Изменение ПДн – действия, направленные на модификацию ПДн.

Информационная система ПДн (ИСПДн) – совокупность информационных технологий и технических средств, которые обеспечивают обработку ПДн, а также БД, в которых обрабатываются ПДн.

Использование ПДн – действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения действий, порождающих юридические/иные последствия в отношении Субъекта ПДн или других лиц, либо иным образом затрагивающих права и свободы Субъекта ПДн или других лиц.

Материальный носитель информации – бумажный, машинный (электронный) и прочие материальные носители, используемые для воспроизведения и/или хранения информации, содержащей ПДн, обрабатываемой в автоматизированном виде (с использованием средств вычислительной техники) и не автоматизированном виде (без использования средств вычислительной техники).

Надзорный орган - орган, уполномоченный на осуществление государственного контроля и надзора за соответствием обработки ПДн требованиям законодательства, а также соблюдением прав Субъектов ПДн (Роскомнадзор).

Накопление ПДн – действия, направленные на формирование исходного, несистематизированного массива ПДн.

Неправомерная или случайная передача (предоставление, распространение, доступ) ПДн/Инцидент с ПДн – умышленно или неумышленно совершенное неправомерное действие/бездействие, а также иные события, которые привели к незаконному раскрытию ПДн неопределенному кругу лиц, повлекшее (возможно повлекшее) нарушение прав Субъектов ПДн.

Несоответствие, отклонение - отступления от утвержденных процедур и правил, которые косвенно или напрямую могут оказать негативное воздействие на права Субъекта ПДн и причинить ему вред.

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному Субъекту ПДн

Обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Обработка ПДн без использования средств автоматизации (неавтоматизированная обработка) – обработка ПДн, содержащихся в информационной системе ПДн либо извлеченных из такой системы, если такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из Субъектов ПДн, осуществляются при непосредственном участии человека.

Обработчик - физическое или юридическое лицо, государственное учреждение, организация или любой другой орган, который обрабатывает ПДн по поручению Оператора для достижения целей, определенных Оператором ПДн.

Общедоступные источники ПДн – источники ПДн, созданные в целях информационного обеспечения, в которые ПДн включены с письменного согласия Субъекта ПДн (в т.ч. справочники, адресные книги).

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

Передача ПДн – распространение, предоставление или доступ к ПДн.

Персональные данные (ПДн) - любая информация, прямо или косвенно относящаяся к определенному или определяемому физическому лицу (Субъекту ПДн).

Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Раскрытие ПДн – обеспечение доступа к ПДн определенного лица, определенного круга лиц или неопределенного круга лиц, независимо от цели получения указанных ПДн.

Распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Сбор ПДн – целенаправленные действия по получению ПДн непосредственно от Субъекта ПДн или его Представителя.

Систематизация ПДн – действия, направленные на объединение и расположение ПДн в определенной последовательности

Субъект ПДн - определенное или определяемое физическое лицо.

Трансграничная передача ПДн – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и/или в результате которых уничтожаются материальные носители ПДн.

Уточнение ПДн – действия, направленные на обновление или изменение ПДн.

Хранение ПДн – процесс поддержания исходного состава ПДн в виде, обеспечивающем выдачу ПДн по запросам конечных пользователей в установленные сроки.

3. Лицо, ответственное за организацию обработки ПДн в Организации

3.1. Порядок назначения лица, ответственного за организацию обработки ПДн в Организации¹.

3.1.1. В случае, если на должность лица, ответственного за организацию обработки ПДн назначается лицо, которое на момент приема на должность не работает в Организации, то назначение производится путем:

- подписания с ним трудового договора, который подтверждает факт назначения;
- ознакомления лица, ответственного за организацию обработки до подписания трудового договора под подпись с должностной инструкцией² и локальными нормативными актами Организации, которые связаны с трудовой деятельностью работника, согласно ст. 68 Трудового кодекса Российской Федерации (далее – ТК РФ)

На основании заключенного трудового договора в Организации может быть издан приказ/распоряжение о приеме на работу, который подписывается уполномоченным лицом³ в Организации⁴.

3.1.2. В случае, если на должность лица, ответственного за организацию обработки ПДн в Организации, назначается действующий работник, который выполняет иную трудовую функцию/иные должностные обязанности, то назначение осуществляется посредством подписания дополнительного соглашения к трудовому договору и должностной инструкции⁵.

3.2. Лицо, ответственное за организацию обработки ПДн, получает указания непосредственно от исполнительного органа Организации⁶ и подотчетно ему.

3.3. В функции лица, ответственного за организацию обработки ПДн, входят, в частности:

- управление процессом организации обработки и защиты ПДн в соответствии с требованиями законодательства РФ о ПДн, настоящего Положения, а также локальных нормативных актов по вопросам обработки и защиты ПДн;
- разработка локальных нормативных актов по вопросам обработки и защиты ПДн;
- проведение мониторинга изменений действующего законодательства РФ в области ПДн (далее – Мониторинг) и ведение учета проводимого Мониторинга;
- доведение до сведения работников Организации положений законодательства РФ о ПДн, настоящего Положения, локальных нормативных актов Организации по вопросам обработки, требований к защите ПДн;

¹ В случае, если в качестве лица, ответственного за организацию обработки ПДн, назначено юридическое лицо, то в таком случае в Организации издается приказ о том, что соответствующее юридическое лицо будет выполнять функции лица, ответственного за организацию обработки ПДн в Организации.

² Необязательный, но рекомендуемый к подписанию работником документ, и, если такой документ установлен локальными нормативными актами Организации.

³ Например, руководителем Организации.

⁴ Указанные документы являются необязательными с момента внесения изменений в ТК РФ (ФЗ от 22.11.21 №377-ФЗ), но могут быть изданы в Организации, если локальными нормативными актами Организации они определены в качестве документов, необходимых для оформления и учета принимаемых на работу лиц.

⁵ Если такой документ предусмотрен локальными нормативными актами Организации.

⁶ Например, исполнительным органом в Копании может быть генеральный директор.

- организация и осуществление имплементации требований локальных нормативных актов Организации по вопросам обработки и защиты ПДн в процессы Организации, в рамках которых осуществляется обработка ПДн;
- разработка и организация применения правовых, организационных и технических мер защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также иных неправомерных действий в отношении ПДн;
- организация и осуществление оценки эффективности принимаемых мер по обеспечению безопасности ПДн;
- осуществлять внутренний контроль за соблюдением Организацией и его Работниками требований законодательства РФ о ПДн, настоящего Положения, иных локальных нормативных актов Организации по вопросам обработки и защиты ПДн;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществлять контроль за приемом и обработкой обращений и запросов субъектов ПДн или их представителей, обладающих полномочиями на представление интересов субъектов ПДн, по вопросам обработки ПДн субъектов ПДн;
- взаимодействие с уполномоченными органами по вопросам обработки и защиты ПДн в Организации;
- обеспечение уведомления Надзорного органа об изменении сведений об обработке ПДн, а также о намерении Организации осуществлять трансграничную передачу ПДн в целях обеспечения защиты прав субъектов ПДн;
- участие в расследовании Инцидентов с ПДн;
- организация и/или осуществление уведомления Надзорного органа об указанных в Законе №152-ФЗ обстоятельствах в случае установления Инцидента с ПДн.

3.4. Организация обязана предоставлять лицу, ответственному за организацию обработки ПДн, сведения, указанные в ч. 3 ст. 22 Закона №152-ФЗ.

3.5. Сведения, которые Организация обязана предоставлять лицу, ответственному за организацию обработки ПДн в Организации, согласно ч. 3 ст. 22.1 Закона №152-ФЗ и п. 3.4. настоящего Положения в т.ч. необходима для ведения лицом, ответственным за организацию обработки ПДн Реестра процессов, в которых осуществляется обработка ПДн (далее – Реестр процессов) по форме Приложения №1, который может быть представлен в форме электронного документа, который используется в т.ч. для:

- разработки и/или актуализации **Политики в отношении обработки ПДн** в Организации и других локальных нормативных актов Организации по вопросам обработки ПДн;
- направления Уведомления об изменениях в обработке ПДн в Надзорный орган;
- построения системы обработки ПДн;
- проведения внутреннего контроля процессов, в которых осуществляется обработка ПДн;
- подготовки ответов на запросы субъектов ПДн, их представителей и Надзорного органа.

3.6. Актуализация, дополнение и обновление Реестра процессов может осуществляться владельцами процессов в Организации, но при предварительном согласовании с лицом, ответственным за организацию обработки ПДн.

4. Основные этапы процесса организации обработки ПДн

4.1. Мониторинг законодательства

4.1.1. С целью повышения качества и эффективности организации обработки и защиты ПДн в Организации, направленной на соблюдение прав субъектов ПДн на всех этапах обработки ПДн, лицо, ответственное за организацию обработки ПДн, проводит Мониторинг и ведет учет проводимого Мониторинга в **Журнале учета мероприятий по контролю за изменениями законодательства в области ПДн** по форме Приложения №2 к настоящему Положению;

4.1.2. Лицо, ответственное за организацию обработки ПДн по результатам Мониторинга осуществляет обобщение и подготовку информационно-аналитических материалов с привлечением необходимых профильных подразделений Организации и обеспечивает своевременное доведение до сведения работников информации об изменениях (проектах) правовых норм в отношении вопросов обработки и защиты ПДн.

4.1.3. По результатам Мониторинга лицо, ответственное за организацию обработки ПДн, в т.ч. принимает решение:

- о необходимости внесения изменений в действующие локальные нормативные акты Организации по вопросам обработки ПДн;
- о принятии новых локальных нормативных актов по вопросам обработки ПДн;
- об отмене локальных нормативных актов по вопросам обработки ПДн.

4.2. Взаимодействие с Надзорным органом

4.2.1. В соответствии с Законом №152-ФЗ Организация обязана содействовать Надзорному органу в реализации им своих полномочий по контролю и надзору за обработкой ПДн и соблюдением прав субъектов ПДн, в частности:

- предоставлять информацию, необходимую для выполнения функций Надзорного органа;
- оказывать содействие в проведении расследований в части принимаемых мер по организации обработки и защиты ПДн;
- исполнять предписания Надзорного органа в части устранения выявленных нарушений при обработке ПДн;
- исполнять требования Надзорного органа в части предоставления информации о трансграничной передаче ПДн и уведомления о фактах Инцидентов с ПДн;
- исполнять требования Надзорного органа в части реализации прав субъектов ПДн;
- обеспечивать исполнение требований Надзорного органа третьими лицами, которым Организация поручила обработку ПДн;
- приостанавливать передачу ПДн получателю в случае нарушений, выявленных Надзорным органом.

4.2.2. Уведомление о намерении осуществлять обработку ПДн

4.2.2.1. Организация до начала обработки ПДн направляет уведомление в Надзорный орган о своем намерении осуществлять обработку ПДн в соответствии с ч.1 ст. 22 Закона №152-ФЗ, на основании которого Организация включается в Реестр операторов, осуществляющих обработку ПДн⁷.

4.2.2.2. Уведомление о намерении осуществлять обработку ПДн должно содержать сведения, предусмотренные ч. 3 ст. 22 Закона №152-ФЗ и иные сведения, предусмотренные приказом Роскомнадзора от 28.10.2022 № 180⁸. При предоставлении сведений, предусмотренных ч. 3 ст. 22, Организация для каждой цели обработки ПДн указывает категории ПДн, категории

⁷ Реестр операторов, осуществляющих обработку ПДн: <https://pd.rkn.gov.ru/operators-registry/operators-list/>

⁸ Приказ Роскомнадзора от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»

субъектов, ПДн которых обрабатываются, правовое основание обработки ПДн, перечень действий с ПДн, способы обработки ПДн.

4.2.2.3. Уведомление о намерении осуществлять обработку ПДн направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом в Организации.

4.2.3. Уведомление об изменениях в обработке ПДн

4.2.3.1. Предоставление в Надзорный орган информации об изменении сведений, содержащихся в Уведомлении о намерении осуществлять обработку ПДн осуществляется в соответствии со ст. 22 Закона №152-ФЗ в случае произошедших в процессах Организации изменений по отношению к сведениям, ранее направленным в Надзорный орган, в частности, изменения:

- целей обработки ПДн;
- категорий и/или перечня ПДн;
- категорий субъектов ПДн;
- правовых оснований обработки ПДн (для конкретной цели обработки ПДн);
- сведений о месте нахождения баз ПДн;
- иных сведений с учетом требований, установленных приказом Роскомнадзора от 28.10.2022 №180.

4.2.3.2. Формирование Уведомления об изменениях в обработке ПДн осуществляется лицом, ответственным за организацию обработки ПДн, по установленной приказом Роскомнадзора от 28.10.2022 №180 форме на основании информации об изменениях в процессах, выявленных в рамках осуществления анализа и оценки соответствия процессов (в т.ч. пилотов) требованиям к порядку обработки и защиты ПДн, по отношению к сведениям, ранее направленным в Надзорный орган.

4.2.3.3. Уведомление об изменениях в обработке ПДн направляется в адрес Надзорного органа до 15-го числа месяца, следующего за месяцем, в котором возникли (были установлены) изменения, в виде документа на бумажном носителе или в форме электронного документа за подписью уполномоченного лица в установленном в Организации порядке.

4.2.4. Уведомление о прекращении обработки ПДн

4.2.4.1. В случае прекращения обработки ПДн Организация обязана уведомить об этом Надзорный орган в течении 10 рабочих дней по форме, установленной приказом Роскомнадзора от 28.10.2022 №180.

4.2.4.2. Основаниями для прекращения обработки ПДн являются:

- ликвидация Организации;
- реорганизация Организации;
- прекращение деятельности Организации по обработке ПДн;
- аннулирование лицензии;
- наступление срока или условия прекращения обработки ПДн, указанного в Уведомлении о намерении осуществлять обработку ПДн;

• вступившее в законную силу решение суда;

- иные основания.

4.2.4.3. Уведомление о прекращении обработки ПДн направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом в Организации.

4.2.5. Трансграничная передача ПДн

4.2.5.1. До начала осуществления деятельности по трансграничной передаче ПДн Организация в соответствии со ст. 12 Закона №152-ФЗ направляет в Надзорный орган Уведомление о своем намерении осуществлять трансграничную передачу ПДн (далее – Уведомление о трансграничной передаче ПДн).

4.2.5.2. До подачи Уведомления о трансграничной передаче ПДн Организация обязана:

- получить от иностранного третьего лица, которому планируется трансграничная передача ПДн, сведения, указанные в ч.5 ст.12 Закона №152-ФЗ;
- провести оценку соблюдения третьим лицом, которому планируется трансграничная передача ПДн, конфиденциальности ПДн и обеспечения безопасности ПДн при их обработке.

4.2.5.3. Запрос сведений, указанных в ч. 5 ст.12 Закона №152-ФЗ, в адрес иностранного третьего лица направляется подразделением - инициатором трансграничной передачи ПДн в Организации **по форме Приложения №3 к настоящему Положению**. Полученные от иностранного третьего лица сведения о принимаемых мерах направляются лицу, ответственному за организацию обработки в Организации.

4.2.5.4. Оценка соблюдения иностранным третьим лицом, которому планируется трансграничная передача ПДн, конфиденциальности ПДн и обеспечения безопасности ПДн при их обработке осуществляется лицом, ответственным за организацию обработки ПДн.

4.2.5.5. Формирование Уведомления о трансграничной передаче ПДн осуществляется лицом, ответственным за организацию обработки ПДн, **по форме Приложения № 4 к настоящему Положению** на основании положительного заключения по результатам оценки третьих лиц, которым планируется трансграничная передача ПДн.

4.2.5.6. Уведомление о трансграничной передаче ПДн направляется в адрес Надзорного органа в виде документа на бумажном носителе или в форме электронного документа за подписью уполномоченного лица в установленном в Организации порядке.

4.2.5.7. В случае поступления в Компанию запроса от Надзорного органа в отношении сведений, содержащихся в ранее направленном Уведомлении о трансграничной передаче ПДн, в целях оценки достоверности предоставленных сведений, лицом, ответственным за организацию обработки ПДн, в срок не более 10 (десяти) рабочих дней с даты получения такого запроса, способом, указанным в запросе, предоставляются в Надзорный орган запрашиваемые сведения, предусмотренные в п.п. 1-3 ч.5 ст.12 Закона №152-ФЗ. Указанный срок может быть продлен, но не более, чем на 5 (пять) рабочих дней при направлении в адрес Надзорного органа мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.2.5.8. В случае поступления в Компанию от Надзорного органа решения о запрете или об ограничении трансграничной передачи ПДн, Организация обязана направить иностранному третьему лицу, которому осуществляется трансграничная передача ПДн уведомление о запрете или об ограничении трансграничной передачи ПДн и уничтожении ранее переданных ПДн **по форме Приложения №5 к настоящему Положению**.

4.2.5.9. Уведомление о запрете или об ограничении трансграничной передачи ПДн и уничтожении ранее переданных ПДн в адрес иностранного третьего лица, направляется подразделением - инициатором трансграничной передачи ПДн.

4.2.5.10. Полученные от иностранного третьего лица сведения о прекращении обработки ПДн и уничтожении переданных ПДн направляются лицу, ответственному за организацию обработки ПДн.

4.2.6. Уведомление об Инцидентах с ПДн

4.2.6 Порядок уведомления Надзорного органа об Инциденте с ПДн осуществляется в порядке, предусмотренном **Памяткой по уведомлению об Инциденте с ПДн**.

4.3. Разработка локальных нормативных актов по вопросам обработки ПДн, требований к защите ПДн

4.3.1. В целях соблюдения требований ст. ст. 18.1, 19 Закона №152-ФЗ в Организации осуществляется разработка локальных нормативных актов по вопросам обработки ПДн, требований к защите ПДн, а также устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ о ПДн, устранение последствий таких нарушений.

4.3.2. Разработка необходимых правовых, организационных и технических мер для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн осуществляется лицом, ответственным за организацию обработки ПДн. Разработанные локальные нормативные акты обязательны для исполнения всеми подразделениями Организации, осуществляющими обработку ПДн.

4.3.3. Лицо, ответственное за организацию обработки ПДн, организывает и осуществляет имплементацию требований локальных нормативных актов Организации по вопросам обработки ПДн в процессы Организации, в рамках которых осуществляется обработка ПДн, а также контролируют актуальность локальных нормативных актов по вопросам обработки ПДн.

4.3.4. Разрабатываемые локальные нормативные акты не должны противоречить действующему законодательству РФ о ПДн.

4.3.5. В случае изменений законодательства РФ о ПДн, Положение применяется в части, не противоречащей внесенным изменениям, до внесения изменений в Положение.

4.3.6. Лицо, ответственное за организацию обработки ПДн осуществляет пересмотр локальных нормативных актов по вопросам обработки, требования которых затронуты изменениями правовых норм.

4.4. Доведение до работников требований по обработке и защите ПДн

4.4.1. В соответствии со ст. 18.1, 22.1 Закона №152-ФЗ лицо, ответственное за организацию обработки ПДн осуществляет ознакомление работников Организации под подпись в Листе ознакомления с положениями законодательства о ПДн, локальными нормативными актами Организации по вопросам обработки ПДн, требований к защите ПДн (далее – Лист ознакомления) **по форме Приложения № 6 к настоящему Положению.**

4.4.2. В процессе трудовой деятельности работник ознакомливается с положениями вновь изданных локальных нормативных актов по вопросам обработки ПДн, с требованиями к защите ПДн, а также с изменениями к ним посредством подписания Листа ознакомления **по форме Приложения № 6 к настоящему Положению**, который прикладывается к ранее подписанному Листу ознакомления.

4.4.3. В соответствии со ст. 7 Закона №152-ФЗ при приеме на работу работник подписывает Обязательство о неразглашении конфиденциальной информации **по форме Приложения № 7 к настоящему Положению.**

4.4.4. В соответствии с п. 6 постановления Правительства РФ от 15.09.2008 № 687⁹ необходимо провести информирование работников, осуществляющих обработку ПДн без использования средств автоматизации (в т.ч. работников, осуществляющих такую обработку по поручению оператора ПДн), о факте обработки ими ПДн, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных законодательством о ПДн, а также локальными нормативными актами Организации. Форма документа об информировании

⁹ Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

работников, осуществляющих обработку ПДн без использования средств автоматизации, содержится в **Приложении №8 к настоящему Положению**.

4.4.5. Оформление Листов ознакомления, обязательств, уведомлений работника может осуществляться как на бумажном носителе с собственноручной подписью работника, так и в форме электронного документа, подписанного в порядке, установленном в Организации электронной подписью (далее – ЭП). Хранение листов ознакомления, обязательств, уведомлений работника, оформленных на бумажных носителях, осуществляется в личном деле работника. Хранение листов ознакомления, обязательств, уведомлений работника, оформленных в форме электронного документа, осуществляется в порядке, предусмотренном в Организации.

4.4.6. Принятые на работу работники Организации, осуществляющие обработку ПДн, проходят обязательное обучение по вопросам обработки и защиты ПДн.

4.4.7. Обучение и информирование работников Организации по требованиям действующего законодательства, о порядке и особенностях обработки и защиты ПДн в процессе трудовой деятельности, осуществляется лицом, ответственным за организацию обработки ПДн. Обучение и информирование работников осуществляется:

- планово, согласно Плану, утвержденному в Организации;
- внепланово в случае произошедших изменений в требованиях законодательства о

ПДн и локальных нормативных актов Организации;

- при выявлении отклонений при обработке и защите ПДн в процессах Организации.

4.4.8. Обучение и информирование осуществляется в формате обучающих программ, лекций, семинаров, вебинаров, в т.ч. с привлечением сторонних организаций и внешних консультантов. Информирование также может осуществляться путем направления e-mail-рассылок.

4.5. Внутренний контроль за соответствием обработки ПДн

4.5.1. Лицо, ответственное за организацию обработки ПДн осуществляет внутренний контроль за соответствием обработки ПДн в процессах Организации требованиям законодательства о ПДн, настоящего Положения и других локальных нормативных актов Организации, регламентирующих обработку и защиту ПДн.

4.5.2. Мероприятия внутреннего контроля осуществляются в рамках планового и внепланового контроля соответствия с **Методикой проведения внутреннего контроля в Организации**.

4.6. Контроль за приемом и обработкой обращений Субъектов ПДн

4.6.1. Организация, при обращении либо получении запроса Субъекта ПДн или его представителя в отношении обрабатываемых Организацией ПДн в соответствии со ст.ст. 14, 20, 21 Закона №152-ФЗ, убедившись в его законности, обязана исполнить требование Субъекта ПДн или его представителя и предоставить ему информацию о рассмотрении указанного обращения, или запросе, не позднее 10 (десяти) рабочих дней с даты обращения или получения запроса. Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления Организацией в адрес Субъекта ПДн или его представителя мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Информация по обращению должна быть предоставлена Субъекту ПДн или его представителю в доступной форме и в той форме, в которой направлены соответствующее обращение либо запрос, если иное не указано в обращении или запросе¹⁰, и в ней не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Сведения, содержащиеся в обращении или запросе, должны предоставляться Организацией

¹⁰ Ответ на запрос не может быть предоставлен в устной форме, исходя из требований, предъявляемых к запросу ч.3. ст.14 Закона №152-ФЗ.

исключительно в объеме, допускаемом законодательством РФ о ПДн и исключаяющим риск разглашения ПДн, доступ которых не может быть предоставлен Субъекту ПДн в силу закона.

4.6.2. В случае, если Субъект ПДн обратился с запросом в Компанию в устной форме, то ему должна быть дана рекомендация оформить запрос в соответствии с требованиями, предъявляемыми к нему ч.3 ст.14 Закона №152-ФЗ.

4.6.3. В случае отказа Субъекту ПДн или его представителю в предоставлении информации при обращении или по запросу либо при получении запроса Субъекта ПДн или его представителя Организация обязана дать в письменной форме мотивированный ответ, содержащий ссылку на положения законодательства РФ о ПДн, являющиеся основанием для такого отказа, в срок, не превышающий 10 (десяти) рабочих дней со дня обращения или получения запроса Субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления Организацией в адрес субъекта ПДн или его представителя мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.6.4. Контроль за приемом и обработкой обращений Субъектов ПДн осуществляется в целях соблюдения следующих требований:

- соблюдение прав и законных интересов Субъектов ПДн;
- обеспечение качества и полноты принятия мер по законному требованию Субъекта ПДн и предоставление необходимой информации по его обращению;
- соблюдение сроков обработки обращений, установленных законодательством и предоставления ответов;
- своевременность выявления проблем в процессах обработки ПДн, послуживших причиной обращения Субъекта ПДн и реагирование на них.

4.6.5. Все обращения Субъектов ПДн, поступающие в Компанию, подлежат обязательной регистрации, в соответствии с установленным в Организации порядком для соответствующей категории Субъектов ПДн.

4.6.6. Прием и обработка обращений Субъектов ПДн, направление ответов на обращения, осуществляется в соответствии с **Порядком работы с обращениями и запросами** в Организации.

4.6.7. Контроль за приемом обращений и соблюдением сроков их рассмотрения осуществляется лицом, ответственным за организацию обработки ПДн. Результаты контроля могут оформляться в форме отчета, акта или служебной записки. В случае выявления несоответствий в соблюдении сроков обработки обращений или несоответствий в процессах, в которых осуществляется обработка ПДн, лицом, ответственным за организацию обработки ПДн формируются и доводятся до структурных подразделений Организации, которыми допущены несоответствия в обработке ПДн, выявленные несоответствия, с перечнем мер по их устранению, а также осуществляется контроль за их устранением.

4.7. **Контроль за обработкой запросов Надзорного органа**

4.7.1. Все поступающие в Компанию запросы Надзорного органа, по обращениям Субъектов ПДн в отношении обработки их ПДн, подлежат обязательной регистрации в порядке, установленном в Организации и рассмотрению, с последующим формированием и направлением ответа на запрос. При обработке запроса Надзорного органа следует руководствоваться **Порядком работы с обращениями и запросами** в Организации.

4.7.2. Организация обязана сообщить в Надзорный орган по его запросу необходимую информацию в течение 10 (десяти) рабочих дней с даты получения такого запроса, если иной срок не предусмотрен запросом Надзорного органа, либо федеральным законом или иным нормативным правовым актом. Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в

случае направления Организацией в адрес Надзорного органа мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.7.3. Лицом, ответственным за организацию обработки ПДн осуществляется регулярный контроль за соблюдением сроков рассмотрения запросов Надзорного органа, выявление и оценка причин несоответствий обработки ПДн в процессах Организации, в отношении которых поступил запрос.

4.7.4. Результаты контроля лицом, ответственным за организацию обработки ПДн оформляются документально. В материалах по результатам контроля отражаются сведения о проверенных вопросах и выявленных несоответствиях (при их наличии). В случае выявления несоответствий в соблюдении сроков обработки запросов или несоответствий в процессах, в которых осуществляется обработка ПДн, лицом, ответственным за организацию обработки ПДн формируются и доводятся до структурных подразделений Организации, которыми допущены несоответствия в обработке ПДн, выявленные несоответствия, с перечнем мер по их устранению, а также осуществляется контроль за их устранением.

4.8. Сопровождение проверок Надзорного органа по вопросам обработки ПДн

4.8.1. Сопровождение проверок Надзорных органов по вопросам обработки ПДн (далее – Проверки) осуществляется лицом, ответственным за организацию обработки ПДн.

4.8.2. В целях заблаговременной подготовки к проведению Проверок лицо, ответственное за организацию обработки ПДн осуществляет мониторинг ежегодных планов деятельности Надзорного органа (далее – Планы проверок), размещаемых на официальном сайте Надзорного органа на наличие в них запланированных проверок в отношении Организации.

4.8.3. В случае включения Организации в Планы проверок или получения уведомления о внеплановой проверке, лицо, ответственное за организацию обработки ПДн определяет перечень подготовительных мер к проведению Проверки, перечень передаваемых документов, подтверждающих выполнение Организацией обязанностей, установленных применимым законодательством РФ о ПДн, осуществляет сбор и подготовку документов для передачи Надзорному органу.

4.8.4. При сопровождении Проверки, лицо, ответственное за организацию обработки:

- осуществляет сбор и предоставление запрашиваемой Надзорным органом информации, документов и материалов, необходимых для реализации Надзорным органом своих полномочий;
- организует доступ должностных лиц Надзорного органа в помещения, в которых осуществляется обработка ПДн и к ПДн, обрабатываемым в информационных системах¹¹.

4.8.5. По результатам проведения Проверки лицо, ответственное за организацию обработки ПДн, получает результаты Проверки в порядке, установленном Надзорным органом.

5. Требования к обработке ПДн

5.1. Этапы обработки ПДн могут состоять из следующих действий (операций), совершаемых с ПДн¹²:

- Этап 1 – сбор (получение), запись ПДн;
- Этап 2 – систематизация, накопление, хранение ПДн;
- Этап 3 – уточнение (обновление, изменение) ПДн;
- Этап 4 – извлечение, использование ПДн;
- Этап 5 – передача (предоставление, распространение, доступ) ПДн;

¹¹ Самостоятельный доступ к информационным системам и информационным ресурсам, запрещен.

¹² Количество этапов и их последовательность могут не совпадать с указанным перечнем.

- Этап 5 – блокирование, удаление, уничтожение ПДн.

5.2. Этап 1. Сбор (получение), запись ПДн

5.2.1. При **сборе ПДн** должны учитываться законные права субъектов ПДн, цели обработки ПДн и перечень ПДн, необходимый для достижения заявленных целей обработки ПДн, а также требования по обеспечению безопасности ПДн.

5.2.2. Сбор и дальнейшая обработка ПДн должны быть связаны с соответствующими процессами и/или осуществляться с учетом локальных нормативных актов Организации, а также в случаях, установленных действующим законодательством (в т.ч. в рамках взаимодействия с государственными органами и учреждениями, включая контрольные (надзорные) органы, в пределах их полномочий, Банком России, государственными внебюджетными фондами, муниципальными органами и учреждениями).

5.2.3. В Организации для каждого конкретного процесса, в которых осуществляется обработка ПДн, должны быть установлены цели обработки ПДн и для каждой цели – правовые основания обработки ПДн, категории и перечень обрабатываемых в рамках процесса ПДн, категории субъектов ПДн, способы и сроки обработки, в т.ч. хранения, ПДн, порядок их уничтожения с учетом требований применимого законодательства и локальных нормативных актов Организации по вопросам обработки и/или защиты ПДн, а также должен осуществляться контроль за соблюдением целей и сроков обработки ПДн и не должна быть допущена обработка избыточного состава обрабатываемых ПДн по отношению к целям их обработки.

5.2.4. При осуществлении неавтоматизированной обработки ПДн типовые формы документов должны разрабатываться с учетом требований постановления Правительства РФ от 15.09.2008 № 687¹³.

5.2.5. На каждой странице сайта Организации в футере веб-сайта или в мобильном приложении¹⁴, посредством которых осуществляется сбор ПДн, необходимо опубликовать **Политику в отношении обработки ПДн** в Организации.

5.2.6. Источники сбора (получения) ПДн

Организация при наличии соответствующих правовых оснований обработки ПДн может получать (в т.ч. с целью дальнейшей обработки) ПДн из следующих источников:

- **от субъекта ПДн или представителя субъекта ПДн;**
- **от иного лица, а именно:**
 - ☐ от государственного органа или учреждения, Банка России, государственного внебюджетного фонда, муниципального органа или учреждения, иных уполномоченных лиц (если применимо);
 - ☐ от третьего лица по договору, предусматривающему обработку ПДн, в т.ч. передачу;
 - ☐ от иного лица¹⁵.
- **из иных источников, а именно:**
 - ☐ из публичных источников, в которых ПДн подлежат опубликованию или обязательному раскрытию в соответствии с требованиями законодательства;
 - ☐ из СМИ, сайтов в информационно-коммуникационной сети «Интернет» и т.п.;
 - ☐ из общедоступных источников;
 - ☐ из иных источников.

5.2.7. Правовые основания сбора (получения) ПДн

Организация вправе собирать/получать (в т.ч. для дальнейшей обработки) ПДн при наличии

¹³ Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

¹⁴ Указывается только в том случае, если Организация использует мобильное приложение.

¹⁵ Например, в случае, если субъект ПДн является (или будет являться) выгодоприобретателем или поручителем по заключенному (или заключаемому, в т.ч. в рамках закупочной деятельности) договору между Организацией и иным лицом.

любого из следующих условий:

- если субъект ПДн предоставил согласие на обработку ПДн¹⁶ в конкретных, заранее определенных и законных целях с учетом требований, предусмотренных законодательством РФ для соответствующей категории ПДн и вида ПДн с учетом способа раскрытия¹⁷;
- если согласие на обработку ПДн предоставил представитель субъекта ПДн в конкретных заранее определенных целях с учетом требований, предусмотренных законодательством РФ для соответствующей категории ПДн (при этом Организация обязана проверить полномочия представителя);
- если обработка ПДн необходима для заключения или исполнения договора, стороной, выгодоприобретателем или поручителем по которому является субъект ПДн (договор при этом не может содержать следующие положения:
 - ☐ ограничивающие права и свободы субъекта ПДн;
 - ☐ устанавливающие случаи обработки ПДн несовершеннолетних, если иное не предусмотрено законодательством РФ;
 - ☐ допускающие в качестве условия заключения договора бездействие субъекта ПДн).
- если обработка ПДн необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на Компанию функций, полномочий и обязанностей;
- если обработка ПДн необходима для исполнения судебных актов, актов другого органа или должностного лица в соответствии с положениями законодательства об исполнительном производстве;
- если обработка ПДн необходима для осуществления прав и законных интересов Организации или третьих лиц¹⁸ либо для достижения общественно-значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- если осуществляется обработка ПДн, которые должны быть опубликованы или раскрыты в соответствии с федеральными законами РФ;
- если ПДн получены от лица, не являющегося субъектом ПДн, при условии, что Организации предоставлены подтверждения наличия оснований для обработки, в т.ч. передачи ПДн;
- если обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта ПДн, если получение согласия Субъекта ПДн невозможно;
- если обработка ПДн необходима для осуществления научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы Субъекта ПДн;
- если обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн;
- если обработка ПДн, полученных в результате обезличивания ПДн, осуществляется в целях, на условиях и в порядке, предусмотренных федеральными законами, указанными в п. 9.1. ст. 6 Закона №152-ФЗ, при условии участия Организации в соответствующих экспериментальных режимах.

¹⁶ В случае смерти субъекта ПДн согласие на обработку его ПДн могут дать наследники субъекта ПДн (при условии, что согласие на обработку ПДн не было предоставлено субъектом ПДн при жизни).

¹⁷ Под категориями ПДн подразумеваются: биометрические ПДн, специальные категории ПДн, иные ПДн, не являющиеся биометрическими и специальными (выделяются в зависимости от перечня ПДн и характеристик). Под видами ПДн с учетом способа раскрытия подразумеваются: ПДн, разрешенные субъектом ПДн для распространения, а также ПДн, включенные в общедоступные источники ПДн.

¹⁸ Включая государственные органы, государственные учреждения, Банк России, государственные внебюджетные фонды, муниципальные органы и учреждения.

В случае, если в соответствии с законодательством РФ, предоставление ПДн и/или согласия на их обработку является обязательным¹⁹, Организация обязана по запросу субъекта ПДн или в случае его отказа от предоставления ПДн и/или согласия на их обработку разъяснить субъекту ПДн юридические последствия непредставления соответствующих ПДн и/или согласия на их обработку²⁰.

В случае, если предоставление ПДн и/или согласия на их обработку не является обязательным в соответствии с законодательством РФ и непосредственно не связано с исполнением обязательств по заключенному договору, у субъекта ПДн должна быть возможность получить обслуживание без предоставления соответствующих ПДн и/или согласия на их обработку²¹.

5.2.8. Особенности обработки ПДн

5.2.8.1. Обработка Cookies

Перед началом обработки Cookies Организация обязана получить соответствующее согласие субъекта.

Согласие на обработку Cookies должно быть конкретным, предметным, информированным, сознательным и однозначным²². Ссылка на согласие размещается в окне-уведомлении на обработку Cookies и подтверждается посредством явного действия субъекта ПДн (нажатия соответствующей «кнопки» – «Ассерт/Принять»)²³. Молчание или бездействие субъекта ПДн ни при каких обстоятельствах не может считаться согласием на обработку Cookies. Реализация согласий на обработку Cookies с предпроставленной галочкой в чек-боксе не допускается и не считается предоставлением согласия.

Окно-уведомление об обработке Cookies со ссылкой на **Политику использования Cookies** размещается таким образом, чтобы оно было отчетливо видно на экране и легко доступно для субъекта ПДн. До нажатия Субъектом ПДн соответствующей «кнопки» – «Ассерт/Принять» окно-уведомление не должно пропадать со страницы, просматриваемой субъектом ПДн (в том числе не должно быть возможности закрыть уведомление). Окно-уведомление об обработке Cookies не должно существенным образом мешать субъекту ПДн осуществлять доступ к информации на соответствующем ресурсе, а также не должно косвенным образом принуждать субъекта ПДн к предоставлению согласия на обработку Cookies.

5.2.9. Информация, которая должна предоставляться Субъекту ПДн при сборе ПДн и при получении запросов/обращений

5.2.9.1. В соответствии с Законом №152-ФЗ Организация при обращении/получении запроса²⁴ субъекта ПДн (в том числе повторного) или его Представителя и при условии идентификации и/или аутентификации субъекта ПДн и/или идентификации или аутентификации и подтверждении полномочий Представителя Субъекта ПДн, обязан безвозмездно предоставить

¹⁹ Имеются в виду случаи, когда обработка ПДн допускается только при условии получения согласия на обработку ПДн и иные основания обработки не применимы. При этом Организация не вправе ссылаться на установленную федеральным законом обязанность получения соответствующих ПДн и/или согласия на обработку ПДн в качестве основания для получения от Субъекта ПДн дополнительных ПДн, получение которых не является обязательным.

²⁰ Предоставляемые Субъекту ПДн разъяснения должны позволять обеспечить ознакомление Субъекта ПДн с соответствующими юридическими последствиями, а также зафиксировать факт предоставления Субъекту ПДн указанных разъяснений. Разъяснения должны быть предоставлены в установленные законом сроки по тому же каналу, по которому поступил запрос Субъекта ПДн, а в случае устного запроса Субъекта ПДн – незамедлительно.

²¹ Указанный случай определен, в частности, положениями ч. 4 ст. 16 Закона РФ от 07.02.1992 №2300-1 «О защите прав потребителей».

²² Требования к указанным характеристикам указаны в п. 6.1.1. Положения.

²³ С логированием данного действия.

²⁴ Запрос субъекта ПДн должен содержать номер основного документа, удостоверяющего личность Субъекта ПДн или его Представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие Субъекта ПДн в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и/или иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Оператором, подпись Субъекта ПДн или его Представителя.

Субъекту ПДн информацию, указанную в Приложении №9 к настоящему Положению, за исключением случаев ограничения права Субъекта ПДн на доступ к его ПДн, указанных в ч. 8 ст. 14 Закона №152-ФЗ. Контроль за приемом и обработкой обращений осуществляется в соответствии с разделом 4.6. настоящего Положения.

5.2.9.2. Информация должна быть предоставлена в доступной форме и не может содержать ПДн других субъектов ПДн, за исключением случаев, когда имеются законные основания для раскрытия таких ПДн. При предоставлении информации в рамках ответа на обращение/запрос необходимо учесть:

- ответ предоставляется в той форме, в которой направлены соответствующие обращения либо запрос, если иное не указано в обращении/запросе;
- в зависимости от специфики (особенностей) обращения/запроса могут быть приняты иные (дополнительные) меры по реагированию на поступившее обращение/запрос, в т.ч. в случае применимости оснований, указанных в ч. 8 ст. 14 Закона №152-ФЗ, субъект ПДн может быть ограничен в праве на доступ к ПДн.

5.2.9.3. Согласно Закону №152-ФЗ Организация обязана предоставить субъекту ПДн информацию, указанную в Приложении №9 к настоящему Положению (с учетом объема запрашиваемой в рамках обращения/запроса информации), в течение 10 (десяти) рабочих дней с момента обращения/запроса субъекта ПДн или его Представителя либо с момента получения такого обращения/запроса Организацией. Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней, при условии направления Организацией мотивированного уведомления в адрес субъекта ПДн с указанием причин продления срока предоставления запрашиваемой информации.

5.2.9.4. Удовлетворение повторного запроса/обращения Субъекта ПДн и/или его Представителя на получение информации, указанной **Приложении №9 к настоящему Положению** (с учетом запрашиваемых субъектов ПДн и/или его Представителем сведений), осуществляется в следующих случаях:

- соответствующие запрос/обращение направлены не ранее, чем через 30 (тридцать) дней с момента направления субъектом ПДн и/или его Представителем первоначального запроса/обращения, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- сведения и/или обрабатываемые ПДн, на ознакомление с которыми субъект ПДн имеет право, не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения, при этом повторный запрос/обращение, наряду со сведениями, указанными в ч. 3 ст. 14 Закона №152-ФЗ, содержит обоснование направления повторного запроса.

5.2.9.5. При отсутствии какого-либо из обозначенных случаев Организация вправе отказать субъекту ПДн и/или его Представителю в предоставлении запрашиваемой повторно информации с направлением мотивированного обоснования отказа²⁵.

5.2.9.6. В случае отказа в предоставлении запрашиваемой субъектом ПДн или его Представителем информации Организация обязана предоставить в письменной форме мотивированный ответ, содержащий ссылку на положения ч. 8 ст. 14 Закона №152-ФЗ, иного федерального закона или иного не противоречащего применимому законодательству обоснования,

²⁵ При формировании мотивированного обоснования необходимо учитывать, что обязанность по предоставлению доказательств обоснованности отказа в удовлетворении (выполнении) запроса/обращения лежит на Операторе в соответствии со ст. 14 Закона №152-ФЗ.

являющегося основанием для такого отказа²⁶. Субъект ПДн должен быть уведомлен о таком решении и его причинах в сроки, определенные настоящим Положением для реагирования на обращения Субъектов ПДн.

5.2.10. Информация, предоставляемая работникам

5.2.10.1. В соответствии с ТК РФ в случае, когда Организация осуществляет сбор (получает) ПДн работника Организации не от работника Организации, а от иного лица, такой работник должен быть уведомлен об этом заранее и от него должно быть получено согласие в письменной форме. Работник должен получить информацию о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа работника предоставить согласие в письменной форме на их получение.

5.2.11. Информация, предоставляемая Субъектам ПДн при сборе ПДн в рамках процессов, предусматривающих принятие решения на основании исключительно автоматизированной обработки ПДн

5.2.11.1. При сборе ПДн в рамках процессов, предусматривающих принятие решения на основании исключительно автоматизированной обработки ПДн, порождающего юридические последствия в отношении Субъекта ПДн или иным образом затрагивающего его права и законные интересы, необходимо:

- Разъяснить Субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты Субъектом ПДн своих прав и законных интересов.

В качестве способа разъяснения соответствующая информация может, в частности, включаться в письменную форму согласия Субъекта ПДн на обработку его ПДн, направляться посредством уведомлений или доводиться до сведения Субъекта ПДн иным установленными локальными нормативными актами Организации способами. Такое разъяснение Субъекту ПДн проводится до момента подписания им согласия на обработку ПДн, предусматривающего принятие решений, порождающих юридические последствия в отношении Субъекта ПДн, на основании исключительно автоматизированной обработки ПДн.

Текст разъяснений должен содержать:

- ☐ порядок принятия решения на основании исключительно автоматизированной обработки его ПДн;
- ☐ указание на возможные юридические последствия такого решения;
- ☐ указание на возможность заявить возражение против такого решения;
- ☐ порядок защиты Субъектом ПДн своих прав и законных интересов.

Субъект ПДн вправе заявить возражение против принятия решения на основании исключительно автоматизированной обработки ПДн в любой форме, позволяющей установить факт такого возражения от соответствующего Субъекта ПДн и факт получения возражений Организацией.

- Рассмотреть возражение Субъекта ПДн²⁷ не позднее, чем в течение 30 (тридцати) календарных дней со дня его получения, и уведомить Субъекта ПДн о результатах рассмотрения возражения.

²⁶ Например, Организация имеет право отказать в предоставлении информации об обрабатываемых ПДн в случае, если установить личность Субъекта ПДн невозможно, или в случае, предусмотренных Законом №152-ФЗ для отказа в удовлетворении повторного запроса.

²⁷ В рамках рассмотрения возражения, в частности, проводится проверка правильности принятого на основании исключительно автоматизированной обработки ПДн решения, а также иные мероприятия, позволяющие установить наличие или отсутствие нарушения прав и законных интересов Субъекта ПДн.

В случае признания Организацией обоснованности возражения Субъекта ПДн против принятия решения на основании исключительно автоматизированной обработки его ПДн, Организации необходимо исключить принятие решения на основании исключительно автоматизированной обработки ПДн.

В соответствии с ТК РФ в случае, когда осуществляется принятие решений, затрагивающих интересы работников Организации, такие решения не должны приниматься только на основании ПДн работников, полученных исключительно в результате их автоматизированной обработки.

5.2.12. **Запись ПДн** заключается в фиксировании ПДн в ИСПДн, на СВТ и/или на материальном носителе информации (далее –МНИ) в установленных форматах.

Форматы записи определяются типами полей ввода информации в ИС, и формами МНИ.

5.2.12.1. При осуществлении записи ПДн должно выполняться условие о запрете объединения БД, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой. В том числе при фиксации ПДн на МНИ, обработка которых осуществляется в целях несовместимых между собой, необходимо обеспечить разделение выгружаемых наборов данных на любом уровне (логическом, физическом).

5.2.12.2. При сборе ПДн, в т.ч. посредством информационно-телекоммуникационной сети «Интернет», Организацией должна быть обеспечена запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан РФ с использованием баз данных, находящихся на территории РФ.

5.2.12.3. Должен обеспечиваться учет машинных (электронных) МНИ. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных (электронных) МНИ, присвоенные производителями этих МНИ, инвентарные номера технических средств, имеющих встроенные машинных (электронных) МНИ, и иные номера регистрационного учета.

Машинные (электронные) МНИ, встроенные в стационарные технические средства, учитываются в составе таких стационарных технических средств. Учет осуществляется структурными подразделениями, на которые возложены функции осуществления бухгалтерского (финансового) учета материально-технических средств в соответствии с формами учетной документации в установленном в Организации порядке.

При использовании ресурсов стороннего поставщика²⁸ обязанность по учету машинных (электронных) МНИ возлагается на поставщика.

5.2.12.4. Использование для записи ПДн внешних машинных (электронных) МНИ должно быть минимизировано и допустимо только в технологически обоснованных случаях, когда без данных устройств невозможно организовать работу, в т.ч., хранение, передачу ПДн.

Внешние машинные (электронные) МНИ подлежат раздельному от встроенных в портативные или стационарные технические средства учету в журналах учета машинных (электронных) МНИ. Учет машинных (электронных) МНИ осуществляется ответственным уполномоченным работником, назначенным в установленном в Организации порядке.

5.3. **Этап 2. Систематизация, накопление, хранение ПДн**

5.3.1. **Систематизация** - процедура объединения однородных данных по общим признакам и критериям к определенному иерархизированному единству с установлением связей между данными в целях повышения эффективности их обработки и повышения информационной значимости.

²⁸ Здесь и далее под сторонним поставщиком понимается любое стороннее лицо, предоставляющее соответствующие ресурсы.

Систематизация ПДн в ИСПДн осуществляется в целях упорядочивания ПДн по заданным критериям, с учетом особенностей структуры ИСПДн и способствует возможности оперативного обращения к любому нужному составу данных. В зависимости от типа ИСПДн систематизация может проводиться непосредственно действиями пользователя (в «ручном» режиме) или исключительно с помощью автоматизированной обработки.

Систематизация ПДн без использования средств автоматизации осуществляется работниками Организации с помощью физического упорядочивания материальных носителей информации (далее – МНИ) для дальнейшей работы с ними.

5.3.2. Накопление - процесс увеличения исходного массива ПДн, необходимого для выполнения функциональных задач процессов Организации и поддержания ПДн в актуальном состоянии.

Формирование массива ПДн основывается на принципах необходимого содержания, объема и отсутствия избыточности ПДн по отношению к заявленным целям их обработки. Не допускается объединение массивов ПДн, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

Документы на бумажных носителях, содержащие ПДн субъектов ПДн, образуемые в результате деятельности Организации, накапливаются в помещениях Организации в специально выделяемых местах хранения, обеспечивающих сохранность документов и исключающих несанкционированный доступ к ним.

Накопление ПДн осуществляется в электронном виде и на бумажных и электронных носителях в структурных подразделениях Организации.

5.3.3. Хранение²⁹

5.3.3.1. Обработка ПДн должна осуществляться таким образом, чтобы в отношении каждого Субъекта ПДн можно было определить места хранения его ПДн в ИСПДн, СВТ и/или на соответствующих МНИ и установить перечень лиц, осуществляющих обработку ПДн.

5.3.3.2. Форму (электронный или бумажный вид) и сроки хранения документов – носителей ПДн определяет структурное подразделение, в рамках которого образованы документы с учетом требований, установленных федеральным законодательством и локальными нормативными актами Организации.

5.3.3.3. Хранение ПДн может осуществляться следующими способами:

- в электронном виде:
 - ☐ в ИСПДн Организации;
 - ☐ на СВТ;
 - ☐ на внешних машинных (электронных) МНИ.
- на бумажном носителе:
 - ☐ в помещениях структурных подразделений, осуществляющих хранение МНИ, содержащих ПДн, в специально установленных для этого местах;
 - ☐ в архиве³⁰ Организации в соответствии с законодательством РФ об архивном деле³¹.

5.3.3.4. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, но не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен

²⁹ Данный раздел является типовым и Организации необходимо при утверждении Положения определить, что соответствует ее деятельности, и в случае необходимости, внести изменения в данный раздел.

³⁰ В случае, если привлекается третье лицо для оказания услуг по архивному хранению, то необходимо это указать.

³¹ Действие Закона № 152-ФЗ не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих ПДн документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации.

федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

5.3.3.5. Хранение ПДн в электронном виде должно осуществляться с соблюдением применимых требований законодательства к обеспечению безопасности ПДн и принятием мер, исключающих несанкционированный доступ к ПДн, их неправомерное изменение, блокирование, передачу (предоставление, доступ, распространение), а также иные неправомерные действия в отношении ПДн.

5.3.3.6. На бумажных и внешних машинных (электронных) МНИ необходимо обеспечивать раздельное хранение ПДн, обработка которых осуществляется в различных целях. Хранение бумажных и внешних машинных (электронных) МНИ в структурных подразделениях Организации осуществляется при условии разграничения доступа к ним.

5.3.3.7. В структурных подразделениях, в которых осуществляется хранение МНИ, содержащих ПДн, локальными нормативными актами Организации должны быть установлены:

- перечень мер, обеспечивающих сохранность ПДн и исключающих несанкционированный доступ к ПДн, их неправомерное изменение, блокирование, передачу (предоставление, доступ, распространение), иные неправомерные действия в отношении ПДн, а также порядок принятия таких мер;

- перечень лиц, ответственных за реализацию мер, обеспечивающих сохранность ПДн и исключающих несанкционированный доступ к ПДн.

5.3.3.8. Размещение, охрана и организация режима доступа в помещения, в которых осуществляется хранение МНИ, содержащих ПДн, должны обеспечивать сохранность МНИ и конфиденциальность ПДн, в частности:

- размещение помещений и их охрана должны исключать возможность неконтролируемого проникновения в них посторонних лиц, а также предусматривать периодический контроль за состоянием технических средств охраны;

- помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время;

- окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения;

- организация режима доступа в помещения работников, обслуживающего персонала, посетителей в рабочее и нерабочее время должен исключать возможность неконтролируемого пребывания в них посторонних лиц;

- при необходимости помещения оборудуются хранилищами (сейфами), снабженными замками;

- при утере ключа от хранилища или от входной двери в помещение необходимо произвести замену замков.

5.3.3.9. Для временного хранения МНИ, содержащих ПДн, работникам Организации необходимо иметь достаточное число запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных надежными замками. Ключи от этих хранилищ должны находиться у соответствующих работников.

5.3.3.10. До работников должны быть доведены правила обеспечения сохранности МНИ, содержащих ПДн, а также допуска в помещения работников и посетителей в рабочее и нерабочее время.

5.4. Этап 3. Уточнение (обновление, изменение) ПДн

5.4.1. Общая информация

5.4.1.1. Уточнение (обновление, изменение) ПДн осуществляется, в частности, в следующих случаях:

- обращение в Компанию Субъекта ПДн или его Представителя с предоставлением документов, подтверждающих изменение ПДн (если применимо);
- подтверждение факта неточности ПДн Организацией при установлении Организацией расхождений между ранее полученными ПДн и ПДн, предоставляемыми Субъектом ПДн/его Представителем при обращении в Компанию, а также при получении ПДн от третьих лиц;
- подтверждение факта неточности ПДн на основании сведений, предоставленных Надзорным органом.

5.4.1.2. В случае выявления неточных ПДн при обращении Субъекта ПДн или его Представителя либо по их запросу или по запросу Надзорного органа, следует осуществить блокирование ПДн, относящихся к Субъекту ПДн, или обеспечить их блокирование, если обработка ПДн осуществляется другим лицом, действующим по поручению Организации с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы Субъекта ПДн или третьих лиц (включая государственные органы, Банк России, государственные учреждения, государственные внебюджетные фонды, муниципальные органы).

5.4.1.3. В случае подтверждения факта неточности ПДн Организация на основании актуальных сведений, представленных Субъектом ПДн, его Представителем, Надзорным органом, или иных необходимых документов, обязана уточнить ПДн либо обеспечить их уточнение, если обработка ПДн осуществляется другим лицом, действующим по поручению Организации, в течение 7 (семи) рабочих дней со дня предоставления таких сведений и снять блокирование соответствующих ПДн. В случае, если ПДн, в отношении которых произошло уточнение, были переданы третьим лицам, необходимо принять разумные меры для уведомления указанных лиц об уточнении ПДн соответствующего Субъекта ПДн.

5.4.2. Уточнение ПДн в электронном виде

5.4.2.1. Уточнение ПДн, содержащихся в ИСПДн, на внешних машинных (электронных) МНИ производится путем изменения устаревших (не соответствующих действительности) атрибутов ПДн. В ИСПДн должна быть реализована функция уточнения ПДн.

5.4.3. Уточнение ПДн на бумажных МНИ

5.4.3.1. Уточнение ПДн на бумажном носителе производится в том числе путем:

- фиксации на том же бумажном носителе актуального состава данных;
- изготовления нового бумажного носителя с уточненными ПДн;
- замены на бумажный носитель, предоставленный Субъектом ПДн;
- прикладывания сведений об изменении ПДн совместно с первоначальным документом.

5.4.3.2. В случае уточнения ПДн по заявлению Субъекта ПДн или его Представителя или по запросу Надзорного органа Организация обязана уведомить их о произведенных изменениях ПДн.

5.5. Этап 4. Извлечение, использование ПДн

5.5.1. Извлечение ПДн

5.5.1.1. ПДн извлекаются из ИСПДн путем создания выгрузок для дальнейшей обработки в процессах Организации, а также для переноса в другие ИСПДн, СВТ Организации, а также фиксации на бумажных или машинных (электронных) МНИ и для передачи ПДн третьим лицам.

5.5.1.2. Выгрузка ПДн и электронных документов, содержащих ПДн, из ИСПДн осуществляется работниками Организации в рамках процессов Организации, а также в случаях производственной необходимости в соответствии с предоставленными правами доступа.

5.5.1.3. Работником Организации, осуществившим выгрузку ПДн, должен быть обеспечен соответствующий порядок хранения МНИ, на которые была осуществлена запись выгруженных ПДн, в соответствии с требованиями настоящего Положения.

5.5.1.4. По достижении цели, в рамках которой осуществлялось извлечение ПДн, должно быть обеспечено своевременное уничтожение ПДн, размещенных в ИСПДн, или уничтожение МНИ, содержащих ПДн, с учетом соответствующих требований настоящего Положения.

5.5.1.5. Извлечение ПДн из ИСПДн для передачи третьему лицу может осуществляться только при наличии оснований на такую передачу, указанным в этапе «Передача (предоставление) ПДн» настоящего Положения.

5.5.2. Использование ПДн

5.5.2.1. Общая информация

Использование Организацией ПДн осуществляется путем осуществления действий с ПДн с помощью средств вычислительной техники (автоматизированная обработка ПДн, в том числе в информационно-телекоммуникационных сетях) и без использования таких средств (неавтоматизированная обработка ПДн)³².

Использование ПДн осуществляется для достижения конкретных, заранее определенных Организацией целей, установленных с учетом Политики в отношении обработки ПДн в Компани. На основании определенных целей обработки ПДн и образующихся в процессе такой обработки различных видов документов, устанавливаются сроки обработки ПДн.

5.5.2.2. Использование ПДн, полученных из открытых и общедоступных источников, а также включенных в собственные общедоступные информационные источники

Использование Организацией ПДн, полученных из открытых источников или общедоступных источников, а также совершение любых других действий по обработке указанных ПДн, допускается при условии соответствия цели размещения ПДн в открытом источнике или общедоступной источнике цели планируемой обработки ПДн в Организации и при наличии у Организации правового основания (правовых оснований) на обработку ПДн.

Под **открытыми источниками** при этом понимаются:

- публичные источники, в которых ПДн подлежат опубликованию или обязательному раскрытию в соответствии с требованиями законодательства (например, ЕГРЮЛ, ЕГРИП, ЕВР, ФССП России, официальные сайты судов, картотеки судебных дел, официальные сайты и иные ресурсы, содержащие сведения об аффилированных лицах и иную информацию, подлежащую опубликованию);
- средства массовой информации;
- ресурсы информационно-телекоммуникационной сети «Интернет» (например, сайты, каналы в социальных сетях и мессенджерах и т.п., доступ к которым не ограничен);
- иные информационные ресурсы, доступ к которым не ограничен.

Под **общедоступными источниками ПДн** понимаются справочники, адресные книги и иные источники, созданные в целях информационного обеспечения)³³.

Использование Организацией ПДн, полученных из открытых источников, а также совершение любых других действий по обработке указанных ПДн, допускается исключительно при

³² Возможна также смешанная обработка ПДн (сочетающая автоматизированную и неавтоматизированную обработку).

³³ Создание общедоступного источника в форме справочника, адресных книг может быть реализовано исключительно в целях информационного обеспечения, формирование такого источника осуществляется на основании ПДн, сообщаемых Субъектом ПДн.

наличии законных (правовых) оснований на ее осуществление. Наличие ПДн в открытых источниках само по себе не является основанием, позволяющим Организации осуществлять их обработку ПДн, размещенных в открытых источниках. До начала обработки ПДн из открытых источников Организация должна заранее определить конкретные и законные цели их обработки, и обеспечить подтверждение наличия правовых оснований на обработку в указанных целях. В случае, когда основанием размещения ПДн в открытом источнике является согласие Субъекта ПДн на распространение его ПДн³⁴, использование Организацией ПДн, полученных из таких открытых источников, а также совершение любых других действий с указанными ПДн, возможно при условии соблюдения требований п. 5.6.3. настоящего Положения.

Использование Организацией ПДн, включенных в собственные информационные источники³⁵, а также совершение любых других действий с такими ПДн, допускается при соблюдении следующих требований:

- наличие письменного согласия Субъекта ПДн (в случае передачи ПДн работников третьим лицам для включения таких ПДн в их информационные источники должно быть согласие работника на передачу);
- целью должно быть: информационное обеспечение/взаимодействие;
- сведения о Субъекте ПДн должны быть в любое время исключены из собственных информационных источников ПДн по требованию Субъекта ПДн (в т.ч. при отзыве Субъектом ПДн согласия на обработку ПДн, поступлении требования о прекращении обработки ПДн³⁶) либо по решению суда или Надзорного органа, иных уполномоченных органов. Если Организацией были переданы ПДн третьему лицу, за исключением Надзорного органа и иных уполномоченных органов, для включения ПДн в информационные источники указанных лиц Организация обязана принять меры по исключению ПДн из информационного источника ПДн указанными лицами.

5.6. Этап 5. Передача (предоставление, доступ, распространение) ПДн

5.6.1. Передача (предоставление) ПДн

5.6.1.1. Организация вправе осуществлять передачу ПДн³⁷ третьим лицам (в т.ч. иностранным) в следующих случаях:

- передача ПДн осуществляется с согласия Субъекта ПДн на передачу его ПДн (в письменной или любой форме, в зависимости от статуса Субъекта ПДн, категории передаваемых ПДн и действий по их обработке);
- передача ПДн необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на Компанию функций, полномочий и обязанностей, кроме случаев, требующих наличие согласия Субъекта ПДн;
- передача ПДн осуществляется в рамках исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект ПДн, кроме случаев, требующих наличие согласия Субъекта ПДн;
- осуществляется передача ПДн, разрешенных Субъектом ПДн для распространения, с учетом установленных Субъектом ПДн запретов и условий на такую передачу;
- в иных случаях, предусмотренных Законом №152-ФЗ, иными применимыми нормативными правовыми актами.

³⁴ Могут быть иные правовые основания, кроме согласия на распространения.

³⁵ Имеются в виду информационные источники по смыслу ст. 8 Закона №152-ФЗ. Например, справочники, адресные книги.

³⁶ При этом необходимо учитывать требования п.5.2. настоящего Положения в части удовлетворений запросов, обращений Субъекта ПДн или его Представителя.

³⁷ Передача ПДн работников Организации допускается исключительно в соответствии с требованиями ТК РФ.

5.6.1.2. Получение Организацией ПДн от третьего лица и/или передача (предоставление, доступ) ПДн третьим лицам (если применимо), а также поручение обработки ПДн третьему лицу (если применимо) осуществляется с учетом требований настоящего Положения, а также в рамках процессов Организации, в которых, в частности, определяются условия и порядок передачи ПДн на основании договора с третьим лицом (если применимо), предусматривающим такую передачу. В договор должны быть включены цели обработки ПДн, атрибутный состав передаваемых ПДн, условия по передаче и защите ПДн и способ (канал) передачи ПДн.

5.6.1.3. Перед осуществлением передачи ПДн третьим лицам подразделением-инициатором должна быть проведена проверка наличия правовых оснований на такую передачу по каждому Субъекту ПДн.

5.6.1.4. Типовая форма раздела в договор с третьим лицом условиями которого предусмотрена обработка ПДн приведена в **Приложении №10 к настоящему Положению**³⁸.

5.6.1.5. Передача ПДн третьим лицам может осуществляться в следующем виде:

- в электронном виде посредством информационно-телекоммуникационной сети «Интернет» или иных каналов связи с использованием СКЗИ, сертифицированных ФСБ России³⁹;
- на внешних машинных (электронных) МНИ с сопроводительным письмом или по акту приема-передачи по форме **Приложения №11 к настоящему Положению**. Отправленные МНИ списываются с учета в журнале учета МНИ с указанием реквизитов и даты документа, по которому производилась передача МНИ;
- на бумажных носителях, подписанных уполномоченным Представителем передающей Стороны и заверенные печатью (при наличии).

При необходимости придания юридической силы документам, согласовываемым сторонами посредством электронного документооборота, а также подтверждения авторства в отношении передаваемой информации и целостности ПДн, передаваемых в электронном виде, используются программные средства, обеспечивающие проверку электронной подписи (далее – ЭП).

5.6.1.6. Передача ПДн государственным органам и учреждениям, Банку России, муниципальным органам и учреждениям, государственным внебюджетным фондам, иным уполномоченным органам, а также получение ПДн от указанных лиц допускается в отсутствие согласия Субъекта ПДн на обработку его ПДн в порядке и в случаях, предусмотренных законодательством РФ.

5.6.1.7. В процессах Организации запрещается использование мессенджеров⁴⁰, принадлежащих иностранным лицам для передачи платежных документов и/или предоставления информации, содержащей ПДн граждан РФ, данные о переводах денежных средств в рамках применяемых форм безналичных расчетов, сведения, необходимые для осуществления платежей и/или сведения о счетах (вкладах) граждан РФ.

5.6.1.8. Организация, являясь Оператором, вправе поручить⁴¹ обработку ПДн другому лицу с согласия Субъекта ПДн, на основании заключаемого с этим лицом договора (далее – Поручение).

³⁸ Данная форма используется при обработке ПДн при модели отношений «Оператор - Оператор»

³⁹ Указывается только в том случае, если такие есть.

⁴⁰ В соответствии с Законом №149-ФЗ имеются в виду принадлежащие иностранным юридическим лицам и/или иностранным гражданам информационные системы и (или) программы для электронных вычислительных машин, которые предназначены и (или) используются для обмена электронными сообщениями исключительно между пользователями этих информационных систем и/или программ для электронных вычислительных машин, при котором отправитель электронного сообщения определяет получателя или получателей электронного сообщения и не предусматривается размещение пользователями сети «Интернет» общедоступной информации в сети «Интернет». Перечень размещен на сайте Роскомнадзора <https://rkn.gov.ru/news/rsoc/news74710.htm>.

⁴¹ При поручении обработки ПДн необходимо учесть:

Поручение должно соответствовать требованиям ч. 3 ст. 6 Закона №152-ФЗ, учитывать положения ч. 4 ст. 6 Закона №152-ФЗ. В Поручении должны быть указаны:

- цели обработки ПДн;
- состав (перечень) передаваемых ПДн;
- перечень действий (операций) с ПДн, которые будут совершаться этим лицом;
- обязанность этого лица соблюдать конфиденциальность ПДн обеспечивать безопасность ПДн при их обработке, соблюдать требования ч. 5 ст. 18 и ст. 18.1. Закона №152-ФЗ, а также ответственность за несоблюдение данной обязанности;
- требования к защите обрабатываемых ПДн в соответствии со ст. 19 Закона №152-ФЗ;
- порядок информирования передающей стороны о фактах неправомерной или случайной передачи ПДн с учетом ч. 3.1. ст. 21 Закона №152-ФЗ;
- обязанность по запросу Организации в течение срока действия поручения Организации, в т.ч. до начала обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Организации требований, установленных в соответствии с ч. 3 ст. 6 Закона №152-ФЗ.
- обязанность этого лица по уничтожению ПДн или обеспечению их уничтожения.

Типовая форма Поручения приведена в Приложении №12 к настоящему Положению⁴². Для проведения оценки соблюдения третьим лицом, осуществляющим обработку ПДн по поручению Организации, требований по обеспечению конфиденциальности и безопасности обрабатываемых ПДн может быть использована форма Анкеты, приведенная в Приложении №13 к настоящему Положению.

5.6.1.9. Трансграничная передача ПДн и получение ПДн из иностранных государств

Трансграничная передача ПДн осуществляется в соответствии с Законом №152-ФЗ, постановлением Правительства РФ от 16.01.2023 №24⁴³, приказом Роскомнадзора от 05.08.2022 №128⁴⁴ в порядке, предусмотренном п. 4.2.5. настоящего Положения.

До начала осуществления деятельности по Трансграничной передаче ПДн Организация в соответствии со ст. 12 Законом №152-ФЗ направляет в Надзорный орган уведомление о намерении осуществлять Трансграничную передачу ПДн⁴⁵ по форме Приложения №4 к настоящему Положению, а также осуществляет иные действия, предусмотренные Законом №152-ФЗ, в порядке, предусмотренном в п.4.2.5. настоящего Положения.

В случае, если Организация передает ПДн на территорию иностранных государств, порядок трансграничной передачи ПДн определяется в соответствии с п.4.2.5. настоящего Положения. Принятие решение о допустимости трансграничной передачи ПДн осуществляется с учетом статуса

1. лицо, осуществляющее обработку ПДн по поручению Оператора, не обязано получать согласие Субъекта ПДн на обработку его ПДн;

2. ответственность перед Субъектом ПДн в случае, если Организация, являясь Оператором ПДн, поручает обработку таких ПДн другому лицу (резиденту РФ), несет Организация. Если Организация поручает обработку ПДн иностранному физическому лицу или иностранному юридическому лицу, ответственность перед Субъектом ПДн за действия указанных лиц несет Организация и лицо, осуществляющее обработку ПДн по поручению Оператора.

⁴² Данная форма используется при модели отношений «Оператор – Лицо, осуществляющее обработку ПДн по поручению Оператора».

⁴³ Постановление Правительства РФ от 16.01.2023 № 24 «Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан».

⁴⁴ Приказ Роскомнадзора от 05.08.2022 № 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных».

⁴⁵ Направляется отдельно от уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку ПДн. В уведомлении об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку ПДн, указывается только факт осуществления или неосуществления трансграничной передачи ПДн.

иностранного государства, на территорию которого планируется трансграничная передача ПДн:

- иностранное государство обеспечивающее адекватную защиту⁴⁶;
- иностранное государство, не обеспечивающее адекватную защиту.

Перечень иностранных государств, обеспечивающих адекватную защиту прав Субъектов ПДн, утвержден приказом Роскомнадзора от 05.08.2022 №128.

5.6.2. Доступ к ПДн

5.6.2.1. Доступ к обрабатываемым Организацией ПДн предоставляется только тем работникам Организации, которым он необходим для выполнения ими конкретных функций в рамках исполнения должностных обязанностей.

5.6.2.2. При осуществлении доступа работника к ИСПДн ему должен быть предоставлен минимальный набор необходимых прав доступа в рамках закрепленной за пользователем роли.

5.6.2.3. Работники Организации, осуществляющие обработку ПДн с использованием средств автоматизации и без использования таких средств, несут ответственность за несоблюдение требований к обработке и защите ПДн, в том числе за необеспечение конфиденциальности обрабатываемых ПДн и сохранности бумажных и внешних машинных (электронных) МНИ, образующихся в процессе обработки ПДн, разглашение или незаконное использование ПДн, в соответствии с ТК РФ, а также могут быть привлечены к гражданско-правовой, административной и уголовной ответственности в порядке, предусмотренном применимыми нормативными правовыми актами РФ.

Уполномоченным лицом⁴⁷ в Организации утверждаются должностные инструкции для работников, в которых определяются обязанности работников в части соблюдения требований к обработке и защите ПДн, в частности, требования к обеспечению конфиденциальности ПДн, и ответственность за нарушение требований.

5.6.2.4. Учет лиц, допущенных к обработке ПДн, производится средствами АС, посредством которых осуществляется оформление заявок на доступ, либо ИСПДн, в которых осуществляется обработка ПДн. В ИСПДн должна быть реализована возможность выгрузки списков лиц, имеющих доступ к обработке ПДн.

5.6.2.5. Доступ работников к обрабатываемым ПДн должен быть прекращен, в частности, в следующих случаях: отсутствие (прекращение) производственной необходимости, изменение должностных обязанностей, увольнение работника (вне зависимости от оснований увольнения).

5.6.2.6. Прекращение доступа работников или третьих лиц, которым при наличии на то правовых оснований ранее был предоставлен доступ, к обрабатываемым ПДн осуществляется по окончании срока полномочий работника или третьего лица по использованию информационного ресурса, в случае утраты необходимости в предоставлении доступа указанному работнику или третьему лицу к информационному ресурсу.

5.6.2.7. Предоставление доступа к ПДн третьим лицам осуществляется в порядке, предусмотренном п. 5.6.1. настоящего Положения.

5.6.3. Распространение ПДн

⁴⁶ К таким государствам относятся: 1) иностранные государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных; 2) иностранные государства, не являющиеся сторонами указанной Конвенции, но принимающие меры по обеспечению конфиденциальности и безопасности ПДн при обработке, которые соответствуют положениям Конвенции.

⁴⁷ Например, это может быть руководитель Организации.

5.6.3.1. Распространение ПДн осуществляется с согласия Субъекта ПДн на обработку ПДн, разрешенных им для распространения (далее – Согласие на распространение ПДн)⁴⁸, за исключением случаев, когда применимо иное основание распространения ПДн⁴⁹.

Типовая форма Согласия на распространение ПДн приведена в Приложении №14 к настоящему Положению.

5.6.3.2. Согласие на распространение ПДн предоставляется Субъектом ПДн или его Представителем и должно учитывать требования, определенные Законом №152-ФЗ, приказом Роскомнадзора от 24.02.2021 №18⁵⁰, п. 6.1.5. настоящего Положения.

5.6.3.3. Особенности обработки ПДн, разрешенных Субъектом ПДн для распространения:

- не позднее 3 (трех) рабочих дней с момента получения Согласия на распространение ПДн Организация обязана опубликовать на информационном ресурсе, посредством которого осуществляется распространение ПДн, информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц⁵¹;

- действие Согласия на распространение ПДн прекращается с момента:

- ☐ поступления соответствующего требования Субъекта ПДн (например, отзыва Согласия на распространение ПДн; требования о прекращении передачи (распространения, предоставления, доступа) ПДн⁵²;

- ☐ окончания срока, установленного для обработки ПДн, разрешенных Субъектом ПДн для распространения ПДн⁵³.

5.7. Этап 6. Блокирование, удаление, уничтожение ПДн

5.7.1. Блокирование ПДн

5.7.1.1. Блокирование ПДн заключается во временном прекращении обработки ПДн (за исключением случаев, когда обработка необходима для уточнения ПДн).

5.7.1.2. Блокирование осуществляется по факту выявления неточных ПДн или неправомерной обработки ПДн, на основании обращений/запросов Субъектов ПДн, их Представителей или на основании сведений, предоставленных Надзорным органом. Блокирование осуществляется с момента получения обращения/запроса или сведений о неточности ПДн или их неправомерной обработке на период проверки и только в том случае, если блокирование ПДн не нарушает права и законные интересы Субъекта ПДн или Третьих лиц/Партнеров/иных лиц.

5.7.1.3. О результатах проверки по фактам, указанным в обращении или запросе, а также о предпринятых мерах Организация обязана уведомить Субъекта ПДн и/или, когда применимо, Надзорный орган.

5.7.2. Удаление, уничтожение ПДн

5.7.2.1. Уничтожением ПДн является осуществление действий, в результате которых которых становится невозможным восстановить содержание ПДн в ИСПДн, на СБТ, на МНИ, и/или

⁴⁸ Применимо, если отсутствует иное основание обработки (например, сведения подлежат обязательному опубликованию в соответствии с законодательством и др.).

⁴⁹ Например, таким основанием может быть осуществление обработки ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с применимым законодательством; осуществление и выполнение законодательством РФ возложенных на Компанию функций, полномочий, обязанностей.

⁵⁰ Приказ Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения».

⁵¹ В ином случае Организация не вправе распространять ПДн.

⁵² Передача (распространение, предоставление, доступ) ПДн должна быть прекращена в любое время по требованию Субъекта ПДн о прекращении передачи ПДн (распространения, предоставления, доступа). Требование Субъекта ПДн должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) Субъекта ПДн, а также перечень ПДн, обработка которых подлежит прекращению. Указанные в данном требовании ПДн могут обрабатываться только Оператором, которому оно направлено.

⁵³ При наступлении данного события распространение ПДн должно быть прекращено.

в результате которых уничтожаются МНИ, содержащие ПДн, с учетом требований Закона №152-ФЗ, приказа Роскомнадзора от 28.10.2022 №179⁵⁴, применимых локальных нормативных актов Организации⁵⁵.

5.7.2.2. Организация обязана прекратить обработку ПДн субъекта ПДн и произвести уничтожение ПДн, в следующих случаях:

- цели обработки ПДн достигнуты;
- ПДн больше не требуются для достижения целей, для которых они были получены⁵⁶;
- истекли сроки обработки, в т.ч. хранения (включая архивное хранение в ИСПДн в течение срока, установленного в Организации);
- истек срок, в течение которого действует согласие на обработку ПДн;
- окончен срок действия/прекращено действие договора или расторгнут договор, стороной которого или выгодоприобретателем, поручителем по которому являлся Субъект ПДн;
- Организацией выявлены случаи неправомерной обработки ПДн, в т. ч. по обращению Субъекта ПДн или запросу Надзорного органа, когда обеспечить правомерность обработки ПДн невозможно;
- Организацией установлена избыточность состава ПДн по отношению к заявленным целям обработки, когда обеспечить правомерность обработки ПДн невозможно;
- прекратило действовать поручение обработки ПДн, на основании которого Организация обрабатывала ПДн;
- Субъект ПДн отозвал свое согласие на обработку⁵⁷;
- Субъект ПДн направил требование о прекращении обработки ПДн

5.7.2.3. При уничтожении ПДн следует руководствоваться положениями **Памятки по уничтожению ПДн**.

5.7.2.4. При уничтожении ПДн на поступившего требования/обращения (об отзыве согласия на обработку ПДн, о прекращении обработки ПДн, об уничтожении ПДн, о неправомерной обработке ПДн) от Субъекта ПДн или Надзорного органа:

- необходимо установить, есть ли необходимость в продолжении обработки указанных в требовании/обращении ПДн и наличие законных (правовых) оснований на продолжение такой обработки;
- если необходимость в обработке указанных ПДн и/или основания для их обработки отсутствуют, то происходит уничтожение ПДн, в установленном в Организации порядке;
- если в процесс обработки ПДн вовлечены лица, осуществляющие обработку ПДн по поручению Оператора, то в их адрес направляется требование об уничтожении соответствующих ПДн с кратким описанием причины направления запроса (требование Субъекта ПДн или Надзорного органа), а также формой и порядком предоставления подтверждающих документов об уничтожении ПДн;
- в адрес Субъекта ПДн или Надзорного органа, в сроки, установленные законодательством, направляется уведомление о рассмотрении поступившего требования и о

⁵⁴ Приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении требований к подтверждению уничтожения персональных данных».

⁵⁵ При условии отсутствия иных законных оснований для продолжения обработки ПДн (требования законодательства, которыми для Организации установлены полномочия, функции, обязанности, законный интерес и другие, установленные ст. 6 Закона №152-ФЗ).

⁵⁶ Реорганизация и ликвидация юридического лица, а также прекращение деятельности индивидуального предпринимателя может подпадать под случаи уничтожения ПДн, например, при достижении целей обработки ПДн или при утрате необходимости в достижении целей обработки ПДн.

⁵⁷ Данное условие применимо только к тому составу ПДн и целям обработки ПДн, которые соответствуют действующему правовому основанию.

предпринятых мерах по уничтожению ПДн или обоснование о продолжении обработки ПДн, содержащее в частности, основание на обработку ПДн, цели обработки и срок обработки ПДн.

5.7.2.5. Требования к срокам уничтожения ПДн:

- в случае достижения цели обработки ПДн и отсутствия иных оснований на их обработку Организация, в соответствии с Законом №152-ФЗ, обязана прекратить обработку либо обеспечить ее прекращение лицом, осуществляющим обработку по поручению Оператора и уничтожить ПДн или обеспечить их уничтожение в срок, не превышающий 30 (тридцати) календарных дней с даты достижения цели обработки ПДн;

- в случае выявления неправомерной обработки ПДн Организация в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязана прекратить неправомерную обработку ПДн либо обеспечить ее прекращение лицом, осуществляющим обработку по поручению Оператора. В случае если обеспечить правомерность обработки ПДн невозможно, Организация в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки ПДн, обязана уничтожить такие ПДн или обеспечить их уничтожение лицом, осуществляющим обработку по поручению Оператора;

- в случае отзыва Субъектом ПДн согласия на обработку ПДн, при условии, что продолжение обработки ПДн не требуется для достижения целей обработки ПДн, отсутствуют иные основания обработки ПДн, Организация обязана прекратить обработку ПДн либо обеспечить ее прекращение лицом, осуществляющим обработку по поручению Оператора и уничтожить ПДн или обеспечить их уничтожение лицом, осуществляющим обработку по поручению Оператора в срок, не превышающий 30 (тридцати) календарных дней с даты поступления отзыва;

- в случае поступления требования о прекращении обработки ПДн, при условии, что продолжение обработки ПДн не требуется для достижения целей обработки ПДн, отсутствуют иные основания обработки ПДн, Организация обязана прекратить обработку ПДн либо обеспечить ее прекращение лицом, осуществляющим обработку по поручению Оператора в срок, не превышающий 10 (десяти) дней (срок может быть продлен, но не более чем на 5 (пять) рабочих дней). Срок уничтожения ПДн в таком случае определяется в порядке, предусмотренном для случаев, когда достигнута цель обработки ПДн или выявлена неправомерная обработка ПДн;

- в случае предоставления Субъектом ПДн сведений, подтверждающих, что ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Организация обязана в течение 3 (трех) дней произвести блокирование ПДн для проведения проверки предоставленных сведений (блокирование осуществляется на период проверки) и, в случае подтверждения факта незаконного получения ПДн или избыточности ПДн для заявленной цели обработки уничтожить ПДн в течение 7 (семи) рабочих дней с даты получения подтверждающих указанные факты сведений.

В случае отсутствия возможности уничтожения ПДн в течение вышеуказанных сроков Организация осуществляет блокирование таких ПДн и уничтожает ПДн в срок не более, чем 6 (шесть) месяцев, или обеспечивает их уничтожение лицом, осуществляющим обработку по поручению Организации при условии, что иные сроки не установлены применимым законодательством. При этом необходимо определить порядок блокирования ПДн и документирования информации, которая подтверждает (обосновывает) невозможность уничтожения ПДн.

Контроль за соблюдением сроков обработки ПДн в рамках конкретного процесса осуществляется владельцами процессов в Организации.

5.7.2.6. Способы уничтожения ПДн зависят от объекта уничтожения ПДн⁵⁸:

Уничтожение МНИ, содержащих ПДн, осуществляется посредством их физического уничтожения с составлением Акта об уничтожении ПДн **по форме Приложения №15 к настоящему Положению** следующими способами:

- ПДн на бумажных носителях могут уничтожаться путем разрезания носителя (шредером соответствующего класса защиты), сжигания, промышленной переработки);
- ПДн на машинных носителях могут уничтожаться путем механического разрезания, размагничивания, химического травления в агрессивных средах, переплавки.

Уничтожение ПДн, содержащихся в ИСПДн, на СВТ и на машинных (электронных) МНИ, осуществляется путем удаления записей ПДн или удаления файлов программными или аппаратными средствами, исключающими восстановление уничтоженных данных, в том числе остаточной информации с составлением Акта об уничтожении ПДн **по форме Приложения №15 к настоящему Положению**, и регистрацией события в журнале регистрации событий.

Уничтожение при этом производится, например, посредством:

- функционала операционной системы/ПО;
- средств администрирования ПО;
- перезаписи уничтожаемых файлов, случайно сгенерированными символами;
- очистки физического пространства МНИ, включая элементы памяти, специализированным ПО, прошедшим процедуру оценки соответствия;
- методов выборочного уничтожения ПДн (например, записи конкретного атрибута ПДн или конкретного Субъекта ПДн);
- средств защиты информации, которые имеют функционал уничтожения информации.

5.7.2.7. Требования к технологии удаления ПДн:

- уничтожение ПДн должно осуществляться путем гарантированного удаления без возможности восстановления записей в ИСПДн и на бумажных/машинных МНИ;
- методы уничтожения ПДн не должны допускать возникновения после проведения процедуры удаления остаточной информации на МНИ, на страницах ИСПДн и в файловой системе;
- заполнение таблиц данных в ИСПДн должно осуществляться сгенерированными уникальными (случайными) цифровыми, буквенными и символьными значениями, их смешанными значениями, без возможности обратного преобразования;
- алгоритмы формирования уникальных значений для заполнения таблиц данных ИСПДн не должны сохраняться;
- уничтожение ПДн необходимо осуществлять с учетом соблюдения сроков архивного хранения документации;
- уничтожение ПДн на МНИ должно осуществляться совместно с уничтожением ПДн во всех ИСПДн, включая резервные копии и архивные ИСПДн, если осуществлялась запись в электронном виде и наоборот;
- при уничтожении ПДн в ИСПДн и на бумажном/машинном МНИ должен быть обеспечен контроль качества уничтожения ПДн;
- при уничтожении ПДн как в электронном виде, так и на МНИ должна быть обеспечена конфиденциальность уничтожаемых ПДн с учетом настоящего Положения.

5.7.2.8. Конкретные ПДн в записях ИСПДн могут быть временно (на период проверки) заблокированы от несанкционированного использования путем их маркировки для последующего уничтожения в установленные законодательством сроки.

⁵⁸ Данный раздел является типовым и Организации необходимо при утверждении Положения определить, что соответствует ее деятельности, и в случае необходимости, внести изменения в данный раздел.

5.7.2.9. В случаях, когда необходимо обеспечить ссылочную целостность и связанность данных, уничтожение может осуществляться путем заполнения таблиц данных ИСПДн уникальными, случайно сгенерированными цифровыми, буквенными и символьными значениями, при этом алгоритмы формирования уникальных значений для заполнения таблиц данных ИСПДн не должны сохраняться.

5.7.2.10. Уничтожение ПДн осуществляется непосредственно работником (ами) Организации, уполномоченным (ыми) в порядке, установленном локальными нормативными актами Организации, на осуществление уничтожения ПДн;

5.7.2.11. Подтверждение уничтожения ПДн:

- подтверждением уничтожения ПДн в случае уничтожения МНИ, является Акт об уничтожении ПДн, составленный **по форме Приложения №15 к настоящему Положению**;
- подтверждением уничтожения ПДн в ИСПДн являются одновременно Акт об уничтожении ПДн, составленный **по форме Приложения №15 к настоящему Положению**, и выгрузка из журнала регистрации событий).

5.7.2.12. Хранение Актов об уничтожении ПДн и выгрузок из журнала регистрации событий должно осуществляться не менее 3 лет.

5.7.2.13. При уничтожении бумажных МНИ, содержащих ПДн, должно осуществляться уничтожение таких ПДн в соответствующих ИСПДн, включая резервные копии и архивные базы данных, если они ранее не были уничтожены.

5.7.2.14. В случае, если обработка ПДн осуществляется лицом, осуществляющим обработку по поручению Оператора, Организация обязана принять необходимые меры к прекращению обработки ПДн или их блокированию лицом, осуществляющим обработку по поручению Оператора и последующему уничтожению ПДн в установленные Законом №152-ФЗ сроки. В этих целях в договоре с поручением обработки ПДн указываются условия и обязанности Обработчика по прекращению обработки и уничтожению ПДн, а также по предоставлению подтверждающих документов об уничтожении ПДн.

6. Управление согласиями на обработку ПДн

6.1. Требования к согласиям на обработку ПДн

6.1.1. Общие требования к согласиям на обработку ПДн

6.1.1.1. Согласие на обработку ПДн предоставляется посредством совершения активных действий, позволяющих достоверно определить выражение Субъектом ПДн согласия на обработку его ПДн. Для этого согласие должно отвечать следующим требованиям:

- должно быть:
 - ☐ дано свободно, своей волей и в своем интересе;
 - ☐ конкретным, предметным, информированным, сознательным, однозначным.
- может быть дано Субъектом ПДн или его Представителем в любой позволяющей подтвердить факт его получения форме, если законодательством РФ не установлена обязанность получать согласие в письменной форме.

6.1.1.2. Обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем прямых контактов с Субъектом ПДн с помощью средств связи (далее – прямой маркетинг) должна осуществляться только при условии предварительного согласия Субъекта ПДн на обработку ПДн. При этом согласие на обработку ПДн в целях прямого маркетинга является отдельным от согласия на получение рекламы по смыслу законодательства РФ о рекламе.

6.1.2. Согласие Субъекта ПДн в письменной форме

6.1.2.1. Организация, являясь Оператором ПДн, обязана получать согласие Субъекта ПДн в письменной форме в следующих случаях:

- включение ПДн в общедоступные источники ПДн;

- обработка биометрических ПДн;
- обработка специальных категорий ПДн;
- принятие решения на основании исключительно автоматизированной обработки ПДн,

порождающего юридические последствия в отношении Субъекта ПДн или иным образом затрагивающего его права и законные интересы;

- передача ПДн работника Организации третьему лицу, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных ТК РФ или иными федеральными законами.

6.1.2.2. Согласие Субъекта ПДн в письменной форме в соответствии с требованиями ч. 4 ст. 9 Закона №152-ФЗ должно включать в себя, в частности:

- фамилию, имя, отчество (при наличии), адрес (места регистрации или места жительства) субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- фамилию, имя, отчество (при наличии), адрес (места регистрации или места жительства) Представителя Субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого Представителя (при получении согласия от Представителя Субъекта ПДн);

- наименование и юридический адрес Организации;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие;
- наименование или фамилию, имя, отчество (при наличии) и адрес лица, осуществляющего обработку ПДн по поручению Организации, если обработка будет поручена такому лицу;

- общее описание используемых Организацией способов обработки ПДн (автоматизированная и/или неавтоматизированная);

- перечень действий с ПДн, на совершение которых дается согласие;
- срок, в течение которого действует согласие Субъекта ПДн;
- способ отзыва Согласия Субъектом ПДн;
- подпись Субъекта ПДн и дату подписи.

6.1.2.3. Согласие Субъекта ПДн в письменной форме оформляется на бумажном носителе с собственноручной подписью Субъекта ПДн или его Представителя. Содержание согласия должно соответствовать требованиям ч. 4 ст. 9 Закона №152-ФЗ. Равнозначным содержащему собственноручную подпись Субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Законом №63-ФЗ электронной подписью (далее – ЭП). Подписание Субъектами ПДн согласий в письменной форме на бумажном носителе осуществляется в присутствии уполномоченного Организацией лица.

6.1.3. Согласие Субъекта ПДн в форме электронного документа

6.1.3.1. Техническая реализация процесса, в рамках которого осуществляется сбор согласий в электронной форме, должна предусматривать формирование электронного экземпляра документа.

6.1.3.2. Для подписания согласий в форме электронного документа ЭП могут использоваться следующие ЭП:

- ПЭП – Субъектами ПДн, заключившими с Организацией Соглашение об использовании ЭП. ПЭП формируется в порядке, определенном Соглашением об использовании ЭП. При использовании ПЭП должны обеспечиваться:

- проверка и подтверждение осуществления подписи согласия определенным

Субъектом ПДн;

- ② формирование результата ЭП;
- ② неизменность текста согласия при хранении в АС Организации (подтверждение целостности и подлинности электронного документа);
- ② ЭП должна обеспечивать связь с подписанным электронным документом.

• УНЭП – Субъектами ПДн, заключившими с Организацией Соглашение об использовании ЭП. Ключ и сертификат УНЭП изготавливаются УЦ в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

• УКЭП – при условии соответствия требованиям Закона №63-ФЗ. УКЭП должна быть получена в аккредитованном УЦ.

6.1.3.3. Использование ПЭП и УНЭП Субъектов ПДн, обеспечивающее равную юридическую силу согласий в электронной форме и на бумажных носителях, может быть основано только на ранее заключенном между Организацией и Субъектом ПДн соглашении (рамочном договоре), которое допускает такой порядок подписи. Соглашение (рамочный договор) должно устанавливать условия об одинаковой юридической силе документов, подписанных ПЭП и УНЭП, и документов на бумажных носителях. До подписания согласия в письменной форме УНЭП Организация обязана провести идентификацию и аутентификацию Субъекта ПДн, в порядке, предусмотренном в соглашении (рамочном договоре).

6.1.3.4. В случае использования для подписи согласия УКЭП предварительное заключение соглашения (рамочного договора), которое допускает такой порядок подписи, а также идентификация и аутентификация Субъекта ПДн не требуется.

6.1.4. Согласие Субъекта ПДн в любой форме

6.1.4.1. В случаях, не требующих, в соответствии с законодательством, оформления согласия в письменной форме, Организацией может быть получено согласие в любой форме, позволяющей подтвердить факт его получения. Для получения согласия в форме электронного документа у Субъекта ПДн должна быть возможность совершить явное действие, подтверждающее факт предоставления Субъектом согласия на обработку ПДн (если согласие является правовым основанием обработки).

6.1.4.2. Среди допустимых действий:

- ввод ПИН-кода;
- отправка в Компанию ответного SMS-сообщения с Кодом подтверждения;
- нажатие Субъектом ПДн кнопки в графическом интерфейсе (например, «Подтверждаю», «Согласен», «Принимаю» и т.п., что явно свидетельствует об ознакомлении Субъекта с согласием или иными условиями обработки ПДн);
- заполнение Чек-бокса в графическом интерфейсе.

До момента совершения указанных действий Субъекту ПДн должна быть недоступна возможность направления ПДн Организации.

6.1.5. Согласие Субъекта на распространение ПДн

6.1.5.1. Согласие Субъекта на распространение ПДн предоставляется в случае, когда Организации необходимо осуществить распространение ПДн соответствующего Субъекта ПДн и основанием распространения ПДн является согласие. Согласие на распространение ПДн при этом оформляется отдельно от иных согласий Субъекта ПДн.

6.1.5.2. Требования к содержанию Согласия на распространение ПДн приведены в приказе Роскомнадзора от 24.02.2021 № 18⁵⁹. В частности, среди таких требований:

⁵⁹ Приказе Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»

- Согласие на распространение ПДн оформляется отдельно от иных согласий Субъекта ПДн;

- Согласие на распространение ПДн предоставляется способами, определенными Законом №152-ФЗ;

- из Согласия на распространение ПДн должно явно следовать, что Субъект ПДн согласился с распространением ПДн, указанных в Согласии, на условиях, определенных в Согласии на распространение ПДн. Для этого в Согласии на распространение ПДн должно быть прямо указано, что Субъект ПДн согласился с распространением его ПДн (например, в перечне действий, совершаемых с ПДн, должно быть указано «распространение»);

- в Согласии на распространение ПДн Субъекту ПДн должна быть предоставлена возможность установить запреты на передачу (кроме предоставления доступа) ПДн Организацией неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) ПДн неограниченным кругом лиц. Для этого в Согласии на распространение ПДн должна быть реализована (например, в виде отдельных полей) возможность определить перечень ПДн по каждой категории ПДн, для обработки которых Субъект ПДн установил условия и запреты, а также перечень установленных условий и запретов (например, запрет на публикацию ПДн на других ресурсах, запрет на использование ПДн в целях, отличных от целей их распространения, и т.п.);

- в случае, если Субъект ПДн в Согласии на распространение ПДн не установил запретов или условий обработки ПДн, данный факт должен очевидно следовать из содержания Согласия на распространение ПДн.

Согласие на распространение ПДн должно содержать следующую информацию:

- фамилию, имя, отчество (при наличии) Субъекта ПДн;
- контактную информацию (номер телефона, адрес электронной почты или почтовый адрес Субъекта ПДн);

- сведения о Организации, являющемся Оператором ПДн, – наименование, адрес, указанный в Едином государственном реестре юридических лиц, идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен Субъекту ПДн);

- сведения об информационных ресурсах Организации (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с ПДн;

- цель (цели) обработки ПДн;
- категории и перечень ПДн, на обработку которых дается согласие Субъекта ПДн:
 - ☐ ПДн, не относящиеся к специальным категориям ПДн или биометрическим ПДн (например, фамилия, имя, отчество (при наличии), год, месяц, дата рождения, место рождения, адрес, семейное положение, образование, профессия, социальное положение, доходы, другая информация, относящаяся к Субъекту ПДн);
 - ☐ специальные категории ПДн (перечень ПДн указывается, если планируется обработка специальных категорий ПДн);
 - ☐ биометрические ПДн (перечень ПДн указывается, если планируется обработка биометрических ПДн);
- категории и перечень ПДн, для обработки которых Субъект ПДн устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов;

- условия, при которых полученные ПДн могут передаваться Организацией только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных работников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных ПДн (заполняется по желанию Субъекта ПДн);

- срок действия согласия.

Форма Согласия на распространение ПДн с учетом вышеуказанных требований приведена в **Приложении №14 к настоящему Положению.**

6.1.5.3. Если из предоставленного Субъектом ПДн Согласия на распространение ПДн не следует, что Субъект ПДн не установил запреты и условия на обработку ПДн или если в предоставленном Субъектом ПДн Согласии на распространение ПДн не указаны категории и перечень ПДн, для обработки которых Субъект ПДн устанавливает условия и запреты, то Организация не вправе осуществлять распространение ПДн.

6.1.5.4. В случае, если из предоставленного Субъектом ПДн Согласия на распространение ПДн не следует, что Субъект ПДн согласился с распространением ПДн, распространение ПДн не допускается.

6.1.5.5. В случае, если из предоставленного Субъектом ПДн Согласия на распространение не следует, что Субъект ПДн установил запреты и условия на обработку ПДн, указанные в настоящем Положении и Законе №152-ФЗ, или если в предоставленном Субъектом ПДн Согласии на распространение ПДн не указаны категории и перечень ПДн, для обработки которых Субъект ПДн устанавливает условия и запреты, передача (предоставление, доступ, распространение) ПДн не допускается.

6.2. Управление согласиями на обработку ПДн

6.2.1. Обеспечение доказательств наличия согласий на обработку ПДн

6.2.1.1. Организация осуществляет учет и хранение согласий в течение всего срока обработки ПДн, указанного в согласии, а также в течение сроков, установленных законодательством РФ об архивном деле.

6.2.1.2. Локальные нормативные акты, регламентирующие процессы (в т.ч. проектируемые), в которых осуществляется обработка ПДн, предусматривающая получение согласия Субъекта ПДн, должны также содержать положения о том, как и в какие сроки осуществляются получение, учет, хранение и уничтожение указанных согласий, полученных на бумажном носителе, в форме электронного документа или в иной форме. Соответствующими локальными нормативными актами также определяется место хранения согласий в письменной форме на бумажных носителях, а также перечень мер, необходимых для соблюдения условий, обеспечивающих сохранность ПДн, содержащихся в таких согласиях и исключающих несанкционированный к ним доступ, и перечень лиц, ответственных за реализацию указанных мер⁶⁰.

6.2.1.3. Подтверждением факта получения согласия на бумажном носителе является бланк согласия с собственноручной подписью Субъекта ПДн или его Представителя и указанием даты его подписи. Хранение согласий, оформленных на бумажном носителе, в зависимости от вида осуществляется в следующих подразделениях:

- согласие работника в соответствующем подразделении HR в личном деле работника или в структурном подразделении, в интересах деятельности которого осуществляется сбор согласия;

⁶⁰ Данный пункт является типовым и Организации необходимо при утверждении Положения определить имеются ли соответствующие локальные нормативные акты, в ином случае определить, как данное требование может быть реализовано в Организации.

- согласие Субъекта ПДн, не являющегося работником Организации в целях обеспечения доступа на территорию Организации, для которой предусмотрен контроль доступа, в соответствующем структурном подразделении, в функции которого входит обеспечение пропуска на территорию Организации;

6.2.1.4. При получении согласия от Представителя Субъекта ПДн необходимо осуществлять хранение документов, подтверждающих полномочия Представителя, в течение срока, установленного для хранения согласий. Хранение документов, подтверждающих полномочия Представителя осуществляется совместно с согласиями.

6.2.1.5. Уничтожение согласия Субъекта ПДн на обработку его ПДн должно обеспечиваться по истечении установленного в соответствии с требованиями настоящего Положения срока хранения согласия, и в порядке, предусмотренном настоящим Положением и/или иными применимыми локальными нормативными актами Организации.

6.2.1.6. В случае, если согласие Субъекта ПДн на обработку его ПДн, полученное в письменной форме, получается и/или хранится совместно с иными материальными носителями информации (далее –МНИ), содержащими ПДн такого Субъекта ПДн, учет и уничтожение такого согласия осуществляется совместно с иными МНИ, содержащими ПДн, в порядке и в сроки, установленные для таких МНИ.

6.2.1.7. В целях обеспечения подтверждения Организацией получения согласий в электронном виде, в АС Организации должны быть реализованы функции учета полученных согласий и хранения подтверждений (с возможностью их выгрузки для последующей печати).

7. Заключительные положения

Настоящее Положение подлежит регулярному пересмотру с периодичностью не реже одного раза в три года, а также в случаях изменения требований Законодательства РФ о ПДн.

Приложение:

1. Реестр процессов, в которых осуществляется обработка ПДн
2. Журнал учета мероприятий по контролю за изменениями законодательства в области ПДн
3. Запрос о предоставлении сведений о предоставлении сведений о мерах по защите ПДн
4. Уведомление об осуществлении трансграничной передачи ПДн
5. Уведомление о запрете или ограничении обработки ПДн
6. Лист ознакомления работника с требованиями законодательства о ПДн и ЛНА, регламентирующими обработку и защиту ПДн
7. Обязательство о неразглашении конфиденциальной информации
8. Уведомление работника о факте обработки ПДн без использования средств автоматизации
9. Информация, предоставляемая Субъекту ПДн и/или его Представителю
10. Раздел, подлежащий включению в договор с третьим лицом, условиями которого предусмотрена обработка ПДн
11. Акт приема-передачи материальных носителей, содержащих ПДн
12. Поручение на обработку ПДн
13. Анкета проведения оценки соблюдения третьим лицом, осуществляющим обработку ПДн по поручению Организации, требований по обеспечению конфиденциальности и безопасности обрабатываемых ПДн
14. Согласие на распространение ПДн
15. Акт об уничтожении ПДн