АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ГРАНТЫ ЯМАЛА»

ПРИКАЗ

19 декабря 2025 года

№ 72од

г. Салехард

О вводе в действии, утверждении и признанию утратившим силу некоторых нормативно-правовых актов автономной некоммерческой организации «Гранты Ямала»

В связи с необходимостью актуализации нормативно-правовой базы в соответствии с положениями Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» **п р и к а з ы в а ю**:

1. Ввести в действие с 19 декабря 2025 года:

- положение по защите конфиденциальной информации (персональных данных) автономной некоммерческой организации «Гранты Ямала» (приложение №1);
- положение об ответственном за организацию обработки персональных данных автономной некоммерческой организации «Гранты Ямала» (приложение №2);
- положение о порядке обработки персональных данных субъектов персональных данных автономной некоммерческой организации «Гранты Ямала» (приложение №3);

2. Утвердить с 19 декабря 2025 года:

- политику использования файлов cookie в автономной некоммерческой организации «Гранты Ямала» (приложение №4);
- политику обработки персональных данных автономной некоммерческой организации «Гранты Ямала» (приложение №5);
- инструкцию по допуску сотрудников автономной некоммерческой организации «Гранты Ямала» в помещения, в которых ведется обработка персональных данных (приложение №6);
-инструкцию об осуществлении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленные Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами,

политике и локальными актами оператора автономной некоммерческой организации «Гранты Ямала» (приложение №7).

3. Признать утратившим силу с 19 декабря 2025 года:

- приказ автономной некоммерческой организации «Гранты Ямала» от 21.11.2022 года № 2од «Об утверждении положения о работе с персональными данными работников автономной некоммерческой организации «Гранты Ямала»;

- приказ автономной некоммерческой организации «Гранты Ямала» от 21.11.2022 года № 3од «Об утверждении положения о порядке уничтожения персональных данных работников автономной некоммерческой организации «Граты Ямала»;

- приказ автономной некоммерческой организации «Гранты Ямала» от 27.11.2022 года № 10од «О назначении ответственного лица по работе с персональными данными»;

- приказ автономной некоммерческой организации «Гранты Ямала» от 23.03.2023 года № 11од «Об утверждении мест хранения персональных данных (материальных носителей данных) в автономной некоммерческой организации «Гранты Ямала»;

- приказ автономной некоммерческой организации «Гранты Ямала» от 08.06.2023 года № 23од «О внесение изменений в приказ от 27 декабря 2022 №10од «О назначении ответственного лица по работе с персональными данными»;

- приказ автономной некоммерческой организации «Гранты Ямала» от 18.07.2023 года № 26од «О внесении изменений в приложение к приказу автономного некоммерческой организации «Граты Ямала».

Директор Х.Н. Алхаматов

Приложение №1

УТВЕРЖДАЮ

Директор АНО «Гранты Ямала»

_____ У.Н. Алхаматов

«19» декабря 2025 г.

Положение
по защите конфиденциальной информации (персональных данных)
автономной некоммерческой организации «Гранты Ямала»

1. Общие положения

1.1. Настоящее Положение разработано на основании требований:

- Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Конфиденциальная информация — любая информация с ограниченным доступом которая становится известной какому-либо лицу в связи с выполнением своих профессиональных обязанностей и которые он не имеет права ни распространять, ни использовать в своих интересах.

Персональные данные (далее — ПДн) относятся к информации ограниченного доступа (далее — информация), так как попадают под действие Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — 152-ФЗ).

Цель данного Положения — определение порядка организации, и проведения работ в автономной некоммерческой организации «Гранты Ямала» (далее — Организация) для построения эффективной системы защиты информации.

1.2. Информационная система (далее — ИС) представляет собой совокупность содержащихся в базе данных информации, и обеспечивающих их обработку информационных технологий и технических средств.

1.3. Положение предназначено для практического использования должностными лицами ответственным за защиту информации.

1.4. Требования настоящего Положения являются обязательными для исполнения всеми должностными лицами Организации.

1.5. За общее состояние защиты информации в Организации отвечает директор автономной некоммерческой организации «Гранты Ямала».

1.6. Персональная ответственность за организацию и выполнение мероприятий по защите информации в Организации возлагается на сотрудника Организации, назначенного приказом.

1.7 Лица, виновные в нарушении установленного законом порядка обработки защищаемой информации, с использованием средств автоматизации или без использования таких средств несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

1.8. При необходимости для оказания услуг по защите информации могут привлекаться специализированные организации, имеющие лицензию ФСТЭК на деятельность по технической защите информации.

1.9. Положение может уточняться и корректироваться по мере необходимости.

2. Охраняемые сведения и объекты, актуальные угрозы

2.1. Защищаемые сведения – информация, обрабатываемая в Организации с использованием средств автоматизации или без использования таких средств определены в соответствии с Приказом «Об утверждении перечня обрабатываемых персональных данных».

2.2. Объекты защиты:

информационные системы защищаемой информации, эксплуатируемые Организацией в целях обеспечения своей деятельности. Перечень ИС утверждается директором автономной некоммерческой организации «Гранты Ямала»;

помещения, где установлены ИС или хранится информация на бумажных носителях.

2.3. В Организации необходимо проведение определение угроз безопасности конфиденциальной информации при их обработке в информационных системах.

3. Организационные и технические мероприятия по защите информации

3.1. Для защиты информации, обрабатываемой в Организации, необходимо применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и/или на бумажных носителях.

3.2. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

Для ИСПДн требуется обеспечить 4-й уровень защищённости персональных данных.

3.3. Состав и содержание мер по обеспечению безопасности ПДн, необходимых для обеспечения 4 уровня защищенности приведены и Приказе ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ № 21).

3.4. Проведение работ по технической защите информации в ИС с использованием сертифицированных средств защиты информации, для выполнения требований настоящего Положения, возлагается на администратора

информационной безопасности (далее – Администратор ИБ ИС) и администратора информационных систем (далее – Администратор ИС).

Администратор ИС исполняет обязанности по обеспечению работоспособности средств вычислительной техники (СВТ) ИС, проводит организационно-технические мероприятия по их обслуживанию согласно утвержденным директором автономной некоммерческой организации «Гранты Ямала» инструкций администратору информационных систем.

Администратор ИБ ИС исполняет обязанности по технической защите информационных ресурсов согласно утвержденным директором автономной некоммерческой организации «Гранты Ямала» инструкций администратору информационной безопасности.

Состав мер по обеспечению безопасности защищаемой информации, реализуемых в рамках системы защиты информации с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, указан в Приказе № 21.

Требованиями по защите информации предусмотрено наличие возможности управления конфигурацией ИС, своевременного выявления инцидентов, способных привести к сбоям в работе ИС, возникновению угроз безопасности защищаемой информации.

Необходимо проводить моделирование угроз безопасности, определение актуальных угроз защищаемой информации при их обработке в информационных системах Организации.

Технические меры защиты ИС реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, сертифицированных на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Ответственность за соблюдением установленных правил обеспечения безопасности информации при работе с программными и техническими средствами ИС, правила работы и порядок регистрации в ИС, доступа к информационным ресурсам ИС возлагается непосредственно на пользователя информационной системы персональных данных в соответствии с «Инструкцией пользователю информационной системы персональных данных», утвержденной директором автономной некоммерческой организации «Гранты Ямала».

3.6. Для защиты информации, обрабатываемой в Организации, также необходимо применение организационных мер в соответствии со ст. 18.1 152-ФЗ.

3.7. При обработке ПДн без использования средств автоматизации организационные меры применяются в соответствии Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4. Особенности обработки информации, содержащей персональные данные

4.1. Все ПДн субъекта Организации следует получать у него самого. Если ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Организации должно сообщить субъекту ПДн о целях,

предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа дать письменное согласие на их получение. Обработка ПДн ведется только с согласия субъекта ПДн.

Организация вправе поручить обработку ПДн другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные действующим законодательством.

4.2. Организация не имеет права получать и обрабатывать данные субъекта ПДн о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни.

4.3. Обработка ПДн возможна без согласия субъекта ПДн в соответствии со ст. 6 152-ФЗ.

4.4. Согласие на обработку защищаемой информации оформляется в письменном виде.

4.5. Обработка защищаемой информации должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка защищаемой информации, несовместимая с целями сбора персональных данных.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.6. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя директора автономной некоммерческой организации «Гранты Ямала».

4.7. Ответственный за организацию обработки персональных данных организовывает сбор обязательств работников о неразглашении персональных данных субъектов персональных данных.

5. Планирование работ по защите информации

5.1. Управление осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

5.2. Порядок проведения организации и осуществления контроля выполнения требований по защите персональных данных в структурных подразделениях Организации определяется Инструкцией, утверждаемой директором автономной некоммерческой организации «Гранты Ямала».

5.3. Контроль осуществляет ответственный за организацию обработки персональных данных Организации. Для участия в проведении контроля решением ответственного за организацию обработки персональных данных могут также привлекаться другие специалисты подразделений Организации (по согласованию с их руководителями). В таких случаях контроль носит комплексный характер.

5.4. Контроль проводится в форме плановых и внеплановых проверок.

Плановые проверки проводятся в соответствии с Планом мероприятий, утверждаемым директором автономной некоммерческой организации «Гранты Ямала».

5.5. Внеплановые проверки могут быть контрольными и по частным вопросам. Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов Организации или нарушения требований по защите персональных данных.

5.6. Результаты проверок отражаются в Актах проверок – при проведении проверки комиссией, служебной запиской – при проведении проверки назначенными специалистами. При необходимости принятия решений по результатам проверок подразделений директором автономной некоммерческой организации «Гранты Ямала» готовятся соответствующие служебные записки.

5.7 По результатам проверок, при выявлении недостатков ответственными сотрудниками по защите персональных данных в десятидневный срок разрабатывается план устранения выявленных недостатков, который доводится до заинтересованных лиц с целью их устранения.

Приложение №2

УТВЕРЖДАЮ
Директор АНО «Гранты Ямала»
_____ Х.Н. Алхаматов
«19» декабря 2025 г.

ПОЛОЖЕНИЕ
об ответственном за организацию обработки персональных данных автономной некоммерческой организации «Гранты Ямала»

1. Общие положения

Ответственный за организацию обработки персональных данных (далее Ответственный) является сотрудником автономной некоммерческой организации «Гранты Ямала» (далее Организация).

Ответственный назначается приказом директора автономной некоммерческой организации «Гранты Ямала».

Ответственный в вопросах организации обработки персональных данных (далее ПДн) подчиняется непосредственно директору автономной некоммерческой организации «Гранты Ямала» и проводит мероприятия по защите ПДн в интересах Организации.

Ответственный в своей деятельности руководствуется:

1) Конституцией Российской Федерации;

2) федеральными законами Российской Федерации и нормативными правовыми актами органов государственной власти по вопросам защиты ПДн;

3) государственными стандартами Российской Федерации в области защиты информации;

4) руководящими и нормативными правовыми документами Федеральной Службы по техническому и экспортному контролю России;

5) локальными нормативными актами Организации по защите ПДн;

6) правилами внутреннего трудового распорядка.

Деятельность Ответственного осуществляется согласно утвержденного директором автономной некоммерческой организации «Гранты Ямала» «Плана мероприятий по защите ПДн Организации» на год. «План мероприятий по защите ПДн Организации» разрабатывается на каждый календарный год.

2. Задачи

На Ответственного возложены следующие задачи:

1) организация внутреннего контроля за соблюдением сотрудниками Организации соответствия обработки ПДн требованиям к защите ПДн, установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О

персональных данных» (далее Федеральный закон № 152-ФЗ), принятыми в соответствии с ним нормативными правовыми актами и локальными актами Организации;

2) разработка, внедрение и актуализация локальных актов по вопросам обработки ПДн;

3) доведение до сведения сотрудников Организации, непосредственно осуществляющих обработку ПДн, положений законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн, и проведение обучения указанных сотрудников;

4) осуществление контроля приёма и обработки обращений или запросов субъектов ПДн или их представителей по вопросам обработки ПДн и внесение предложений по организации приёма и обработки таких обращений или запросов;

5) осуществление рассмотрения обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и организация предоставления субъектам ПДн или их представителям информации, предусмотренной Федеральным законом № 152-ФЗ;

6) организация комплексной защиты объектов информатизации Организации, а именно:

а) информационных ресурсов, представленных в виде документированной информации на магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, содержащих ПДн субъектов Организации;

б) средств и систем информатизации (средств вычислительной техники, информационно-вычислительных комплексов, локальных вычислительных сетей и корпоративных информационных систем), программных средств (операционных систем, систем управления базами данных, другого общесистемного и прикладного программного обеспечения), автоматизированных систем управления информационными, управленческими и технологическими процессами, систем связи и передачи данных, технических средств приёма, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорных устройств и других технических средств обработки графической, смысловой и буквенно-цифровой информации), используемых для реализации процессов ведения деятельности, обработки информации, содержащей ПДн субъектов Организации.

7) организация защиты ПДн субъектов Организации;

8) разработка и проведение организационных мероприятий, обеспечивающих безопасность объектов защиты Организации, своевременное выявление и устранение возможных каналов утечки информации;

9) организация проведения работ по технической защите информации на объектах информатизации, в информационно-вычислительных сетях, системах и средствах связи и телекоммуникаций Организации;

10) реализация технических мер, обеспечивающих своевременное выявление возможных технических каналов утечки информации в структурных подразделениях (отделах) Организации;

11) методическое руководство системой обеспечения информационной безопасности Организации;

12) организация контроля состояния и проведение оценки эффективности системы обеспечения информационной безопасности ПДн, а также реализация мер по её совершенствованию;

13) внедрение в информационную инфраструктуру Организации современных методов и средств обеспечения информационной безопасности.

3. Функции

Для решения поставленных задач Ответственный осуществляет следующие функции:

1) участие в разработке и внедрении правовых, организационных и технических мер по комплексному обеспечению безопасности ПДн;

2) контроль обеспечения соблюдения режима конфиденциальности при обработке ПДн и внесение предложений по соблюдению такого режима;

3) разработка планов по защите ПДн на объектах Организации;

4) контроль выполнения мер по защите ПДн, анализ материалов контроля, выявление недостатков и нарушений. Разработка и реализация мер по их устранению;

5) обеспечение взаимодействия с контрагентами по вопросам организации и проведения проектно-изыскательских, научно-исследовательских, опытно-конструкторских и других работ по защите информации. Участие в разработке технических заданий на выполняемые исследования и работы;

6) контроль выполнения плановых заданий, договорных обязательств, а также сроков, полноты и качества работ по защите ПДн, выполняемых контрагентами;

7) разработка и внесение предложений по обеспечению финансирования работ по защите ПДн, в том числе выполняемых по договорам (контрактам);

8) участие в проведении работ по технической защите информации на объектах информатизации Организации. Оценка эффективности принятых мер по технической защите информации;

9) внесение предложений по обеспечению выбора, установке, настройке и эксплуатации средств защиты информации в соответствии с организационно-распорядительной и эксплуатационной документацией;

10) контроль организации режима обеспечения безопасности помещений, в которых происходит обработка ПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в такие помещения, а также внесение предложений по обеспечению безопасности таких помещений;

11) участие в организации доступа сотрудников Организации к ПДн в соответствии с возложенными на них должностными обязанностями и подготовка предложений по организации такого доступа;

12) разработка и внедрение локальных актов, определяющих перечень сотрудников Организации, имеющих доступ к ПДн;

13) контроль размещения устройств ввода (отображения) информации, исключающего её несанкционированный просмотр;

14) проведение оценки вреда, который может быть причинён субъекту(-ам) ПДн в случае нарушения законодательства по защите ПДн;

15) участие в разработке и реализации политики по работе с инцидентами информационной безопасности в части обработки ПДн;

16) внесение предложений по актуализации внутренней организационно-распорядительной документации по защите ПДн при изменении существующих и выходе новых нормативных правовых документов по вопросам обработки ПДн и подготовка соответствующих необходимых проектов документов.

4. Права

Ответственный имеет право:

1) осуществлять контроль за деятельностью структурных подразделений (отделов) Организации по выполнению ими требований по защите ПДн;

2) составлять акты, докладные записки, отчёты для рассмотрения директором автономной некоммерческой организации «Гранты Ямала», при выявлении нарушений порядка обработки ПДн;

3) принимать необходимые меры при обнаружении несанкционированного доступа к ПДн, как сотрудниками Организации, так и третьими лицами, и докладывать о принятых мерах директору автономной некоммерческой организации «Гранты Ямала» с предоставлением информации о субъектах, нарушивших режим доступа;

4) вносить на рассмотрение директору автономной некоммерческой организации «Гранты Ямала» предложения, акты, заключения о приостановлении работ, в случае обнаружения каналов утечки (или предпосылок к утечке) информации ограниченного доступа;

5) давать структурным подразделениям (отделам) Организации, а также отдельным специалистам обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственного;

6) запрашивать и получать от всех структурных подразделений (отделов) Организации сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного;

7) составлять акты и другую техническую документацию о степени защищённости объекта(-ов) информатизации;

8) готовить и вносить предложения: на проведение работ по защите ПДн; о привлечении к проведению работ по оценке эффективности защиты ПДн на объекте(-ах) Организации (на договорной основе) учреждений и организаций, имеющих лицензию на соответствующий вид деятельности; о закупке необходимых технических средств защиты и другой спецтехники, имеющих в обязательном порядке сертификат соответствия;

9) осуществлять визирование договоров (контрактов) с контрагентами с целью правового обеспечения передачи им ПДн субъектов Организации в ходе выполнения работ по этим договорам (контрактам);

10) представлять интересы Организации при осуществлении государственного контроля и надзора за обработкой ПДн Уполномоченным органом по защите прав субъектов ПДн.

5. Взаимоотношения (служебные связи)

Ответственный выполняет свои задачи осуществляя взаимодействие со всеми структурными подразделениями (отделами) Организации.

Для выполнения своих функций и реализации предоставленных прав, Ответственный взаимодействует с территориальными и региональными подразделениями Федеральной службы по техническому и экспортному контролю России, Федеральной службы безопасности России, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерства внутренних дел Российской Федерации и другими представителями исполнительной власти Российской Федерации и организациями, предоставляющие услуги и работы в области защиты ПДн на законном основании.

6. Ответственность

Ответственный несёт ответственность за надлежащее и своевременное выполнение возложенных задач и функций по организации обработки ПДн Организации, в соответствии с положениями законодательства Российской Федерации в области обращения и защиты ПДн.

Приложение №3

УТВЕРЖДАЮ

Директор АНО «Гранты Ямала»

Х.Н. Алхаматов

«19» декабря 2025 г.

ПОЛОЖЕНИЕ
о порядке обработки персональных данных субъектов персональных данных автономной некоммерческой организации «Гранты Ямала»

1. Основные понятия

Для целей настоящего Положения используются следующие основные понятия:

автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники;

безопасность персональных данных — состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

несанкционированный доступ (несанкционированные действия) — доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам;

обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение

персональных данных;

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных;

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2. Общие положения

2.1. Цель разработки настоящего Положения – обеспечение защиты прав и свобод человека и гражданина, при обработке его персональных данных, в том числе права на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным

данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2.2. Положение разработано в соответствии со следующими нормативно-правовыми документами Российской Федерации:

1) Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года с поправками, одобренными Комитетом министров Совета Европы 15 июня 1999 года, ратифицированная Федеральным законом Российской Федерации от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» в рамках, определяемых данным Федеральным законом, заявлений;

2) Конституция Российской Федерации;

3) Гражданский кодекс Российской Федерации;

4) Кодекс об Административных Правонарушениях Российской Федерации;

5) Трудовой кодекс Российской Федерации;

6) Уголовный кодекс Российской Федерации;

7) Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее Федеральный закон № 152-ФЗ);

8) Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

9) Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 года № 188;

10) Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённое постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687;

11) Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119.

2.3. Под обработкой персональных данных понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.4. Положение определяет необходимый минимальный объем мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.

Состав целей обработки, категорий персональных данных, и способов обработки персональных данных определены в «Политике обработки персональных данных». Также «Политика обработки персональных данных» устанавливает перечень третьих лиц, которым передаются персональные данные или поручается их обработка.

Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных

данных, несовместимая с целями сбора персональных данных. Обработке подлежат только те персональные данные, которые отвечают целям их обработки и не должны быть избыточными по отношению к заявленным целям.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

2.5. Деятельность по организации обработки и защиты персональных данных в соответствии с требованиями законодательства Российской Федерации о персональных данных осуществляет работник автономной некоммерческой организации «Гранты Ямала» (далее – Организация, Оператор).

Деятельность по администрированию средств и механизмов защиты осуществляет работник, назначенный администратором информационной безопасности.

Техническое обслуживание информационных систем персональных данных осуществляет работник, назначенный ответственным за техническое обслуживание информационных систем персональных данных.

Ответственный за организацию обработки персональных данных, администратор информационной безопасности и ответственный за техническое обслуживание информационных систем персональных данных назначаются приказом директора автономной некоммерческой организации «Гранты Ямала».

2.6. Оператор может поручить обработку персональных данных третьим лицам с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – Поручение). Лицо, осуществляющее обработку персональных данных по поручению Организации, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ. В поручении Организации должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ.

Лицо, осуществляющее обработку персональных данных по поручению Организации, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случаях, когда Организация поручает обработку персональных данных третьему лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Организация. Лицо, осуществляющее обработку персональных данных по поручению Организации, несет ответственность перед Организацией.

Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.7. В случаях, непосредственно связанных с вопросами трудовых

отношений, в соответствии со статьей 24 Конституции Российской Федерации, Оператор вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

2.8. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

2.9. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законодательством.

2.10. Настоящее Положение вступает в силу с момента его утверждения и действует до замены его новым Положением.

2.11. Все изменения в Положение вносятся приказом директора автономной некоммерческой организации «Гранты Ямала».

3. Порядок обработки персональных данных

3.1. Все персональные данные субъектов Оператор получает от них самих либо от их законных представителей.

3.2. Обработка персональных данных осуществляется на законной и справедливой основе, а также с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ на основании согласия субъекта персональных данных на обработку его персональных данных, кроме случаев, предусмотренных Федеральным законом № 152-ФЗ. Форма согласия утверждается приказом директора автономной некоммерческой организации «Гранты Ямала». Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например, анкеты, бланки).

3.3. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Организация вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются в порядке установленным законодательством.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

3.4. Получение персональных данных субъекта у третьих лиц, возможно только при уведомлении субъекта об этом заранее и с его письменного согласия. Форма согласия утверждается приказом директора автономной некоммерческой организации «Гранты Ямала». Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например, анкеты, бланки).

Персональные данные могут быть получены Оператором от лица, не являющегося субъектом персональных данных, при условии предоставления подтверждения наличия оснований, указанных в Федеральном законе № 152-ФЗ.

3.5. Персональные данные субъектов обрабатываются в структурных подразделениях в соответствии с исполняемыми ими функциями и обязанностями.

3.6. Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии со списком допущенных лиц, утверждённом в порядке, определяемом Организацией.

3.7. Доступ к персональным данным, обрабатываемым в информационных системах персональных данных (далее ИСПДн), осуществляется в соответствии со списком допущенных лиц, утверждённом в порядке, определяемом Организацией.

3.8. Уполномоченные лица, допущенные к персональным данным субъектов Организации, имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностной инструкцией уполномоченных лиц.

3.9. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687.

Персональные данные при такой их обработке должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

3.10. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

3.11. Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются приказом об утверждении мест хранения материальных носителей персональных данных Организации.

3.12. Персональные данные могут подлежать блокированию, уточнению, уничтожению либо обезличиванию в одном из следующих случаев:

1) выявления неправомерной обработки персональных данных при

обращении субъекта персональных данных или его законного представителя либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных;

2) выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных;

3) выявления неправомерной обработки персональных данных, осуществляемой Организацией или лицом, действующим по поручению Оператора невозможности обеспечить правомерную обработку персональных данных;

4) достижения целей обработки или в случае утраты необходимости в их достижении;

5) отзыва согласия субъекта персональных данных на обработку его персональных данных;

6) представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными, неактуальными (устаревшими), незаконно полученными или не являются необходимыми для заявленной цели обработки.

3.13. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению) с момента такого обращения или получения указанного запроса на период проверки.

3.14. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его законного представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных на основании сведений, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, Оператор уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению) в течение 7 рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

3.15. В случае выявления неправомерной обработки персональных данных, осуществляемой Организацией или лицом, действующим по поручению Оператора, в срок, не превышающий 3-х рабочих дней с даты этого выявления, осуществляет прекращение неправомерной обработки персональных данных или обеспечивает

прекращение неправомерной обработки персональных данных лицом, действующим по поручению.

В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, осуществляет уничтожение таких персональных данных или обеспечивает их уничтожение. Решение о неправомерности обработки персональных данных и необходимости уничтожения персональных данных принимает ответственный за организацию обработки персональных данных, который доводит соответствующую информацию до руководства. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение субъекта персональных данных или его законного представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.16. В случае достижения цели обработки персональных данных Оператор прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению) в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

3.17. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

3.18. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор вносит в них необходимые изменения.

В срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор уничтожает такие персональные данные. При этом Оператор уведомляет субъекта персональных данных или его законного представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.19. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанные в пунктах 3.15 – 3.18, Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению) и обеспечивает уничтожение персональных данных в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

3.20. Уничтожение персональных данных осуществляет комиссия в составе руководителя и работников структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого структурного подразделения.

3.21. Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

1) сжигание;

2) шредирование (измельчение носителей);

3) передача на специализированные полигоны (свалки);

4) химическая обработка.

При этом составляется акт, подписываемый председателем комиссии, проводившей уничтожение материальных носителей персональных данных.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия Оператора должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

3.22. Уничтожение полей баз данных, содержащих персональные данные субъекта, выполняется по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

3.23. Уничтожение осуществляет комиссия, в состав которой входят лица, ответственные за администрирование автоматизированных систем, которым принадлежат базы данных, работники структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

3.24. Уничтожение достигается путем затирания информации на носителях информации (в том числе и резервных копиях) или путем механического нарушения целостности носителя информации, не позволяющего произвести считывание или восстановление персональных данных. При этом составляется «Акт уничтожения

полей баз данных, содержащих персональные данные субъекта». Форма акта утверждается отдельным приказом.

3.25. Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами.

3.26. При отсутствии технической возможности осуществить уничтожение персональных данных, содержащихся в базах данных, допускается проведение обезличивания путем перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта персональных данных была невозможна.

3.27. Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных.

3.28. Особенности обработки специальных категорий персональных данных, а также сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные), установлены соответственно статьями 10 и 11 Федерального закона № 152-ФЗ.

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 статьи 10 Федерального закона № 152-ФЗ. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона № 152-ФЗ.

Форма согласия утверждается приказом директора автономной некоммерческой организации «Гранты Ямала». Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например, анкеты, бланки).

3.29. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

3.30. Работники должны быть ознакомлены под подпись с настоящим Положением и другими документами Организации, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

4. Правила работы с обезличенными данными

4.1. Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как уполномоченным органом по защите прав субъектов персональных данных в Российской Федерации, установлены требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, утверждены Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

Методические рекомендации содержат анализ процессов автоматизированной обработки обезличенных данных, требования к обезличенным данным и методам обезличивания, позволяющей выделить основные свойства обезличенных данных и методов обезличивания и оценить возможность их применения при решении задач обработки персональных данных с учетом вида деятельности Оператора и необходимых действий с персональными данными.

4.2. К наиболее перспективным и удобным для практического применения относятся один из следующих методов обезличивания:

1) метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

2) метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

3) метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

4) метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности обезличенных персональных данных в информационных системах и целесообразность их применения определяются ответственным за организацию обработки персональных данных Оператора для каждой информационной системы персональных данных индивидуально.

4.3. Обезличивание должно проводиться таким образом, чтобы определить принадлежность персональных данных конкретному субъекту персональных данных было невозможно без использования дополнительной информации.

4.4. В случае, если обезличенные персональные данные используются в статистических или иных исследовательских целях, сроки обработки и хранения персональных данных устанавливаются руководством Оператора исходя из служебной необходимости, и получение согласия субъекта на обработку его персональных данных не требуется на основании пункта 9 части 1 статьи 6 Федерального закона № 152-ФЗ.

4.5. Если обезличенные персональные данные используются в целях продвижения товаров, работ, услуг на рынке, или в целях политической агитации, Оператор обязан получить согласие субъекта персональных данных на подобную обработку.

5. Передача персональных данных третьим лицам

5.1. При обработке персональных данных субъекта должны соблюдаться следующие требования:

1) не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта;

2) предупреждать лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных.

5.2. При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, Оператор запрашивает согласие субъекта в письменной форме. Форма согласия утверждается приказом директора автономной некоммерческой организации «Гранты Ямала». Допускается совмещение формы согласия субъекта с типовой формой документов, содержащих персональные данные субъекта (например, анкеты). Допускается совмещение формы согласия субъекта с другими формами согласий.

6. Права субъектов персональных данных

6.1. В целях обеспечения своих законных интересов субъекты персональных данных или его представители имеют право:

1) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

2) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ;

3) требовать уточнение его персональных данных, их блокирование или уничтожение в случаях, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Субъект персональных данных при отказе Оператора исключить или исправить, блокировать или уничтожить его персональные данные имеет право заявить в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения;

4) требовать от Оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные, устаревшие, неточные, незаконно полученные или не являющиеся необходимыми для заявленной цели обработки персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них, в том числе блокирование или уничтожение этих данных третьими лицами;

5) обжаловать в суде или в уполномоченном органе по защите прав субъектов персональных данных любые неправомерные действия или бездействие Оператора

при обработке и защите персональных данных субъекта персональных данных, если субъект персональных данных считает, что осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы.

6.2. В случае, если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Организацию или направить ей повторный запрос в целях получения сведений, и ознакомления с персональными данными не ранее, чем через 30 дней после первоначального обращения или направления первоначального запроса, 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 персональных данных.

Субъект персональных данных вправе обратиться повторно до истечения тридцатидневного срока в случае, если сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

6.3. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренные частями 4 и 5 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Организации.

6.4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами Российской Федерации.

7. Порядок обработки обращений и запросов субъектов

7.1. При обращении либо письменном запросе субъекта персональных данных или его законного представителя, на доступ к своим персональным данным Оператор руководствуется требованиями статей 14, 18 и 20 Федерального закона № 152-ФЗ;

7.2. Доступ субъекта персональных данных или его законного представителя к своим персональным данным Оператор предоставляет только под контролем ответственного за организацию обработки персональных данных.

7.3. Обращение субъекта персональных данных или его законного представителя фиксируются в журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных.

7.4. Письменный запрос субъекта персональных данных или его законного представителя фиксируются в журнале регистрации письменных запросов граждан на доступ к своим персональным данным.

7.5. Ответственный за организацию обработки персональных данных принимает решение о предоставлении доступа субъекту персональных данных или его законному представителю к персональным данным указанного субъекта.

7.6. В случае, если данные предоставленные субъектом персональных данных или его законным представителем недостаточны для установления его личности,

или предоставление персональных данных нарушают конституционные права и свободы других лиц, ответственный за организацию обработки персональных данных подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 10 рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо от даты получения запроса субъекта персональных данных или его законного представителя.

7.7. Для предоставления доступа субъекта персональных данных или его законного представителя к персональным данным субъекта ответственный за организацию обработки персональных данных привлекает работника (работников) структурного подразделения, обрабатывающего персональные данные субъекта по согласованию с руководителем этого структурного подразделения.

Организация предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор осуществляет в них необходимые изменения. В срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор уничтожает такие персональные данные. Оператор уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

7.8. Сведения о наличии персональных данных Оператор предоставляет субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Контроль предоставления сведений субъекту или его законному представителю осуществляет ответственный за организацию обработки персональных данных.

7.9. Сведения о наличии персональных данных должны быть предоставлены субъекту при ответе на запрос в течение 10 дней от даты получения запроса субъекта персональных данных или его законного представителя.

8. Порядок действий в случае запросов надзорных органов

8.1. В соответствии с частью 4 статьи 20 Федерального закона № 152-ФЗ Оператор сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 10 дней с даты получения такого запроса.

8.2. Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных при необходимости с привлечением работников Организации.

8.3. В течение установленного законодательством срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

9. Защита персональных данных субъекта

9.1. Защиту персональных данных субъектов от неправомерного их использования или утраты Оператор обеспечивает за счет собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

1) руководящим документом ФСТЭК России «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года;

2) внутренними документами Оператора, действующими в сфере обеспечения информационной безопасности.

9.2. Защита персональных данных предусматривает ограничение к ним доступа.

9.3. Руководитель структурного подразделения Организации, осуществляющего обработку персональных данных:

1) несет ответственность за организацию защиты персональных данных в подчиненном структурном подразделении;

2) закрепляет за работниками, уполномоченными обрабатывать персональные данные, конкретные материальные носители, на которых допускается хранение персональных данных в случае, если такие носители необходимы для выполнения возложенных на работников функций и задач;

3) организовывает изучение подчинёнными работниками, в чьи обязанности входит обработка персональных данных, нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

4) обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном подразделении (отделе);

5) контролирует порядок доступа к персональным данным в соответствии с функциональными обязанностями работников подразделения.

9.4. Работники Оператора, допущенные к персональным данным, дают письменное обязательство о неразглашении таких данных в установленном порядке.

10. Обязанности лиц, допущенных к обработке персональных данных

Лица, допущенные к работе с персональными данными, обязаны:

1) знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы Оператор по обработке и защите персональных данных;

2) сохранять конфиденциальность персональных данных;

3) обеспечивать сохранность закрепленных за ними носителей персональных

данных;

4) контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;

5) докладывать своему непосредственному руководителю отдела (структурного подразделения) обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

Ответственный за организацию обработки персональных данных Оператора организует проведение инструктажа и ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

11. Ответственность работника за нарушение норм, регулирующих обработку и защиту персональных данных субъектов

11.1. Лица, виновные в нарушении норм, регулирующих получение, обработку, передачу и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности.

11.2. К данным лицам могут быть применены следующие дисциплинарные взыскания:

1) замечание;

2) выговор;

3) предупреждение о неполном должностном соответствии;

4) освобождение от занимаемой должности;

5) увольнение.

11.3. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

11.4. Копия приказа о применении к работнику дисциплинарного взыскания с указанием оснований его применения вручается работнику под расписку в течение пяти дней со дня издания приказа.

11.5. Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. До истечения года со дня издания приказа о применении дисциплинарного взыскания работодатель имеет право снять его с работника по собственной инициативе, по письменному заявлению работника или по ходатайству его непосредственного руководителя.

Приложение № 4

УТВЕРЖДАЮ

Директор АНО «Гранты Ямала»

_____ Х.И. Алхаматов

«19» 12 2025 г.

ПОЛИТИКА
использования файлов cookie в автономной некоммерческой организации «Гранты Ямала»

1. Общие положения

1.1. Назначение политики

Настоящий документ (далее – Политика) определяет условия и порядок обработки файлов cookie, собранных и обрабатываемых автономной некоммерческой организацией «Гранты Ямала» (далее – Организация) при посещении и использовании Пользователями Интернет-сайта https://грантыямала.рф/. Организация является оператором персональных данных. Политика является общедоступным документом Организации и предусматривает возможность ознакомления с ней любых лиц.

1.2. Основные понятия

пользователь – физическое лицо, посетившее и использующее Сайт;

файл cookie – текстовый файл небольшого размера, который направляется веб-сервером и сохраняется на компьютере, мобильном телефоне или любом другом устройстве, имеющем доступ в сеть Интернет, при посещении Сайта. Каждый раз при открытии страницы соответствующего интернет-сайта веб-клиент (веб-браузер) Пользователя пересылает указанный текстовый файл веб-серверу в составе HTTP-запроса, чтобы предоставить такому веб-серверу информацию о действиях или предпочтениях Пользователя в Интернете. При этом для обеспечения безопасности и сохранности данных Пользователя веб-клиент (веб-браузер) Пользователя, как правило, не передает файлы cookie, предназначенные для одного веб-сайта, другим ресурсам;

Сайт – Интернет-сайт, имеющий доменное имя «грантыямала.рф»;

2. Цели и виды используемых файлов cookie

2.1. Организация может осуществлять обработку файлов cookie для реализации следующих целей:

1) обеспечение корректной работы сайта и его функциональных возможностей;
2) анализ посещаемости и поведения пользователей для улучшения качества сервиса;
3) персонализация контента и предоставление релевантной рекламы.

2.2. Виды используемых файлов cookie:

1) обязательные файлы cookie — обязательные файлы cookie необходимы для обеспечения корректной работы Сайта предоставления услуг, запрошенных Пользователем. Такие услуги могут включать выбор страны и языка, сохранение статуса входа в систему, обеспечение безопасности и предотвращение мошенничества, сохранение корзины с товарами и элементов списка желаний во время просмотра сайта, сохранение настроек громкости и получение доступа к защищенным областям Сайта. Эта категория файлов cookie не может быть отключена.
2) аналитические (эксплуатационные) файлы cookie — файлы cookie, необходимые для сбора информации о том, каким образом Пользователь использует Сайт (например, информация об используемом Пользователем веб-браузере, при использовании Сайта и т.д.). Данные файлы cookie позволяют улучшать качество и потребительские свойства Сайта: улучшать навигацию на Сайте, чтобы сделать Сайт более удобным и отвечающим потребностям Пользователя, а также исправлять технические ошибки по мере их возникновения и обеспечивать безопасность Сайта.
3) маркетинговые файлы cookie — эти файлы cookie используются для сбора информации о поисковых предпочтениях Пользователя и для показа наиболее подходящей интересам такого Пользователя рекламы и контента. Кроме того, такие файлы cookie могут использоваться для ограничения числа показов рекламы и уникальных предложений для Пользователя, а также для оценки эффективности проводимых Организацией рекламных кампаний (оценка конверсии).

3. Обработка файлов cookie в АНО «Гранты Ямала»

3.1. Организация вправе обрабатывать файлы cookie с использованием средств автоматизации посредством осуществления следующих действий (операций) — сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение. Организация будет обрабатывать файлы cookie со дня принятия Пользователем настоящей Политики / начала использования Пользователем Сайта и до момента достижения заявленных целей обработки файлов cookie или до момента отказа Пользователя от обработки файлов cookie, с учетом сроков действия («сроков жизни») файлов cookie.

4.Отказ пользователя от обработки файлов cookie

4.1. Напоминаем, что обязательные файлы cookie необходимы для обеспечения корректной работы Сайта, а также для обеспечения безопасности Сайта, к сожалению, данный тип файлов cookie нельзя отключить, однако Пользователь может удалить их после завершения использования Сайта. Для управления файлами cookie с помощью используемых веб-браузера или устройства

необходимо воспользоваться инструкцией, предоставляемой разработчиком браузера или производителем устройства, которые использует Пользователь (для удобства Пользователя некоторые из инструкции веб-браузеров приведены далее).

4.2. Файлы cookie размещаются на устройстве Пользователя, иными словами, Организация не может удалить их за него. Пользователь может самостоятельно управлять файлами cookie, действуя по инструкции, применимой для устройства Пользователя и его веб-браузера. Если Пользователь находится на Сайте, работой которого управляет Организация, то Пользователь также может избежать размещения файлов cookie на устройстве Пользователя, задав соответствующие настройки веб-браузера. Срок хранения «браузерных» файлов cookie ограничен. Однако аналогичные технологические решения, такие как локальное хранилище на устройстве Пользователя, не имеют встроенной системы самостоятельного удаления по истечении времени, и соответственно, файлы должны быть удалены Пользователем самостоятельно.

4.3. Примеры руководств по блокировке и удалению файлов cookie в различных браузерах:

Google Chrome https://support.google.com/chrome/answer/95647?hl=ru;

Mozilla Firefox https://support.mozilla.org/ru-ru/kb/delete-cookies-remove-infowebsites-stored;

Microsoft Edge https://support.microsoft.com/ru-ru/help/4468242/microsoft-edgebrowsing-data-and-privacy-microsoft-privacy.

5. Изменения в политике

5.1. Организация оставляет за собой право вносить изменения в настоящую Политику без предварительного уведомления пользователей.

5.2. Актуальная версия Политики размещается на странице https://грантыямала.рф/.

Приложение №5

УТВЕРЖДАЮ

Директор АНО «Гранты Ямала»

Х.Н. Алхаматов

«19» мая 2025 г.

ПОЛИТИКА
обработки персональных данных автономной некоммерческой организации «Гранты Ямала»

1. Общие положения

1.1. Назначение политики

Настоящий документ (далее – Политика) определяет цели и общие принципы обработки персональных данных, а также реализуемые меры защиты персональных данных автономной некоммерческой организации «Гранты Ямала» (далее – Организация). Организация является оператором персональных данных. Политика является общедоступным документом Организации и предусматривает возможность ознакомления с ней любых лиц.

1.2. Основные понятия

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

безопасность персональных данных – состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий, и технических средств;

конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам;

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение

(обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

персональные данные — любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);

персональные данные, разрешённые субъектом персональных данных для распространения — персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путём дачи согласия на обработку персональных данных, разрешённых субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

предоставление персональных данных — действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц;

распространение персональных данных — действия, направленные на раскрытие персональных данных неопределённому кругу лиц;

технические средства информационной системы персональных данных — средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

угрозы безопасности персональных данных — совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных;

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.3. Основные права Организации

Обработка персональных данных осуществляется на законной и справедливой основе, а также с соблюдением принципов и правил, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) на основании согласия субъекта персональных данных на обработку его персональных данных, кроме случаев, предусмотренных Федеральным законом № 152-ФЗ.

Предприятие оставляет за собой право проверить полноту и точность предоставленных персональных данных (далее также – ПДн), их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. В случае выявления ошибочных или неполных ПДн, Организация имеет право прекратить все отношения с субъектом ПДн.

В случае получения согласия на обработку ПДн от представителя субъекта ПДн, полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Организацией.

Организацией могут быть получены ПДн от лица, не являющегося субъектом ПДн, при условии предоставления Организацией подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ.

В случае отзыва субъектом ПДн согласия на обработку своих ПДн, Организация вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ.

Организация вправе поручить обработку ПДн третьим лицам с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом соглашения (договора), в том числе государственного или муниципального контракта, либо путём принятия государственным или муниципальным органом соответствующего акта (далее – поручение Организации). Лицо, осуществляющее обработку ПДн по поручению Организации, обязано соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом № 152-ФЗ. В поручении Организации должны быть определены перечень ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн, требования, предусмотренные частью 5 статьи 18 и статьёй 18.1 Федерального закона № 152-ФЗ, обязанность по запросу Организации в течение срока действия поручения Организации, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Организации требований, установленных в соответствии с Федеральным законом № 152-ФЗ, обязанность обеспечивать безопасность ПДн при их обработке,

а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьёй 19 Федерального закона № 152-ФЗ, в том числе требование об уведомлении Организации о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона № 152-ФЗ.

Лицо, осуществляющее обработку ПДн по поручению Организации, не обязано получать согласие субъекта ПДн на обработку его ПДн.

В случаях, когда Организация поручает обработку ПДн третьему лицу, ответственность перед субъектом ПДн за действия указанного лица несёт Организация. Лицо, осуществляющее обработку ПДн по поручению Организации, несёт ответственность перед Организацией.

В случае, если Организация поручает обработку ПДн иностранному физическому лицу или иностранному юридическому лицу, ответственность перед субъектом ПДн за действия указанных лиц несёт Организация и лицо, осуществляющее обработку ПДн по поручению Организации.

1.4. Основные обязанности Организации

Организация не собирает, не обрабатывает и не передаёт ПДн субъектов ПДн третьим лицам, без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

В случае выявления неправомерной обработки ПДн, при обращении либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн, Организация осуществляет блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных ПДн, при обращении либо по запросу субъекта ПДн или его представителя либо по запросу уполномоченного органа по защите прав субъектов ПДн, Организация осуществляет блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечивает 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.

В случае подтверждения факта неточности ПДн, Организация на основании сведений, предоставленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов, уточняет ПДн либо обеспечивает их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) в течение 7 рабочих дней со дня представления таких сведений и снимает блокирование ПДн.

В случае выявления неправомерной обработки ПДн, осуществляемой Организацией или лицом, действующим по поручению Организации, Организация в срок, не превышающий 3-х рабочих дней с даты этого выявления, осуществляет

прекращение неправомерной обработки ПДн или обеспечивает прекращение неправомерной обработки ПДн лицом, действующим по поручению Организации.

В случае, если обеспечить правомерность обработки ПДн невозможно, Организация в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки ПДн, осуществляет уничтожение таких ПДн или обеспечивает их уничтожение. Решение о неправомерности обработки ПДн и необходимости уничтожения ПДн принимает ответственный за организацию обработки ПДн Организации, который доводит соответствующую информацию до руководства. Об устранении допущенных нарушений или об уничтожении ПДн Организация уведомляет субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом, также указанный орган.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъекта(-ов) ПДн, Организация с момента выявления такого инцидента Организацией, уполномоченным органом по защите прав субъектов ПДн или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов ПДн:

1) в течение 24-х часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Организацией на взаимодействие с уполномоченным органом по защите прав субъектов ПДн, по вопросам, связанным с выявленным инцидентом;

2) в течение 72-х часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

В случае достижения цели обработки ПДн, Организация прекращает обработку ПДн или обеспечивает её прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) и уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) в срок, не превышающий 30 дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Организацией и субъектом ПДн либо, если Организация не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

В случае отзыва субъектом ПДн согласия на обработку его ПДн, Организация прекращает их обработку или обеспечивает прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) в

срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Организацией и субъектом ПДн либо, если Организация не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

В случае обращения субъекта ПДн к Организации с требованием о прекращении обработки ПДн, Организация в срок, не превышающий 10 рабочих дней с даты получения Организацией соответствующего требования, прекращает их обработку или обеспечивает прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 – 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона № 152-ФЗ. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления Организацией в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

В срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Организация вносит в них необходимые изменения.

В срок, не превышающий 7 рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Организация уничтожает такие ПДн. При этом Организация уведомляет субъекта ПДн или его представителя о внесённых изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

В случае отсутствия возможности уничтожения ПДн в течение срока, указанные выше по тексту, Организация осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) и обеспечивает уничтожение ПДн в срок, не более, чем 6 месяцев, если иной срок не установлен федеральными законами.

Подтверждение уничтожения ПДн осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов ПДн.

1.5. Основные права субъекта ПДн

Субъект ПДн принимает решение о предоставлении своих ПДн и даёт согласие на их обработку свободно, своей волей и в своём интересе. В случаях, предусмотренных федеральным законом, обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

В целях обеспечения своих законных интересов, субъекты ПДн или его представители имеют право:

1) получать полную информацию о своих ПДн и обработке этих данных (в том числе автоматизированной);

2) осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, содержащей ПДн субъекта, за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона № 152-ФЗ;

3) требовать уточнение своих ПДн, их блокирование или уничтожение, в случаях, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Субъект ПДн при отказе Организации исключить или исправить, блокировать или уничтожить его ПДн, имеет право заявить в письменной форме о своём несогласии, обосновав соответствующим образом такое несогласие;

4) требовать от Организации уведомления всех лиц, которым ранее были сообщены неверные или неполные, устаревшие, неточные, незаконно полученные или не являющиеся необходимыми для заявленной цели обработки ПДн субъекта, обо всех произведённых в них изменениях или исключениях из них, в том числе блокирование или уничтожение этих данных третьими лицами;

5) обжаловать в суде или в уполномоченном органе по защите прав субъектов ПДн любые неправомерные действия или бездействие Организации при обработке и защите ПДн субъекта, если субъект ПДн считает, что Организация осуществляет обработку его ПДн с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

1) подтверждение факта обработки ПДн Организацией;

2) правовые основания и цели обработки ПДн;

3) цели и применяемые Организацией способы обработки ПДн;

4) наименование и место нахождения Организации, сведения о лицах (за исключением служащих Организации), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Организацией или на основании федерального закона;

5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки ПДн, в том числе сроки их хранения;

7) порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом № 152-ФЗ;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Организации, если обработка поручена или будет поручена такому лицу;

10) информацию о способах исполнения Организацией обязанностей, установленных статьёй 18.1 Федерального закона № 152-ФЗ;

11) иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

В случае, если обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно в Организацию или направить ему повторный запрос в целях получения сведений, и ознакомления с ПДн не ранее, чем через 30 дней после первоначального обращения или направления первоначального запроса, 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.

Субъект ПДн вправе обратиться повторно или направить ему повторный запрос до истечения 30-дневного срока в случае, если сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

Организация вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренные частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Организации.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе, если:

1) обработка ПДн, включая ПДн, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

3) обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма;

4) доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

5) обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного

комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

2. Цели сбора персональных данных

Обработка ПДн ограничивается достижением конкретных, заранее определённых и законных целей. Обработке подлежат только ПДн, которые отвечают целям их обработки. Содержание и объём обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки. Не допускается обработка ПДн, несовместимая с целями сбора ПДн. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

При обработке ПДн Организация обеспечивает точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Организация принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

Целями обработки ПДн в Организации являются:

1) Обеспечение соблюдения трудового законодательства РФ;
2) Ведение кадрового и бухгалтерского учета;
3) Размещение информации для всеобщего сведения на сайте конкурса, других сайтах в сети Интернет и в средствах массовой информации;
4) Рассмотрение заявок на участие в конкурсах на предоставление грантов, проведение отбора победителей, заключение и исполнение грантовых договоров, а также информационное сопровождение данных процессов.

3. Правовые основания обработки персональных данных

Обработка персональных данных в Организации осуществляется на следующих основаниях:

1) письменное согласие субъекта персональных данных;
2) согласие субъекта персональных данных;
3) ст. 86-90 Трудового кодекса РФ.

4. Объём и категории обрабатываемых персональных данных, категории субъектов персональных данных

Организация осуществляет на законной и справедливой основе обработку ПДн следующих физических лиц (субъектов ПДн):

Цель «ведение кадрового и бухгалтерского учета» достигаются посредством обработки ПДн следующих категорий для следующих субъектов ПДн:

1) сотрудники:

Иные категории ПДн: фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, место рождения, семейное положение, социальное положение, пол, адрес места жительства, адрес регистрации, номер телефона, СНИЛС, ИНН, гражданство, данные документа, удостоверяющего личность,

данные водительского удостоверения, реквизиты банковской карты, номер расчетного счета, номер лицевого счета, должность, сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации),отношение к воинской обязанности, сведения о воинском учете, сведения об образовании.

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

2) уволенные сотрудники:

Иные категории ПДн: фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, место рождения, семейное положение, социальное положение, пол, адрес места жительства, адрес регистрации, номер телефона, СНИЛС, ИНН, гражданство, данные документа, удостоверяющего личность, данные водительского удостоверения, реквизиты банковской карты, номер расчетного счета, номер лицевого счета, должность, сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации),отношение к воинской обязанности, сведения о воинском учете, сведения об образовании.

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

3) контрагенты:

Иные категории ПДн: фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, пол, адрес места жительства, адрес регистрации, номер телефона, СНИЛС, ИНН, гражданство, данные документа, удостоверяющего личность, номер расчетного счета, номер лицевого счета, должность, сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации).

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

4) представители контрагентов:

Иные категории ПДн: фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, пол, адрес места жительства, адрес регистрации, номер телефона, СНИЛС, ИНН, гражданство, данные документа, удостоверяющего личность, номер расчетного счета, номер лицевого счета, должность, сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации).

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

5) выгодоприобретатели по договорам:

Иные категории ПДн: фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, место рождения, семейное положение, социальное положение, пол, адрес места жительства, адрес регистрации, номер телефона, СНИЛС, ИНН, гражданство, данные документа, удостоверяющего личность, данные водительского удостоверения, реквизиты банковской карты, номер расчетного счета, номер лицевого счета, должность, сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации),отношение к воинской обязанности, сведения о воинском учете, сведения об образовании.

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Цель «обеспечение соблюдения трудового законодательства РФ» достигаются посредством обработки ПДн следующих категорий для следующих субъектов ПДн:

1) сотрудники:

Иные категории ПДн: фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, место рождения, пол, адрес места жительства, адрес регистрации, номер телефона, СНИЛС, ИНН, данные документа, удостоверяющего личность, должность, отношение к воинской обязанности, сведения о воинском учете.

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

2) уволенные сотрудники:

Иные категории ПДн: фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, место рождения, пол, адрес места жительства, адрес регистрации, номер телефона, СНИЛС, ИНН, данные документа, удостоверяющего личность, должность, отношение к воинской обязанности, сведения о воинском учете.

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Цель «персональные данные руководителей НКО для размещения информации для всеобщего сведения на сайте конкурса, других сайтах в сети Интернет и в средствах массовой информации» достигаются посредством обработки ПДн следующих категорий для следующих субъектов ПДн:

1) контрагенты:

Иные категории ПДн фамилия, имя, отчество, адрес электронной почты, профессия.

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, удаление, уничтожение.

2) представители контрагентов:

Иные категории ПДн: фамилия, имя, отчество, адрес электронной почты, профессия.

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, удаление, уничтожение.

3) выгодоприобретатели по договорам:

Иные категории ПДн: фамилия, имя, отчество, адрес электронной почты, профессия.

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, удаление, уничтожение.

Цель «рассмотрение заявок на участие в конкурсах на предоставление грантов, проведение отбора победителей, заключение и исполнение грантовых договоров, а также информационное сопровождение данных процессов.» достигаются посредством обработки ПДн следующих категорий для следующих субъектов ПДн:

1) физических лиц участников конкурса:

Иные категории ПДн: фамилия, имя, отчество, контактная информация (адрес электронной почты), данные документа, удостоверяющего личность, иные данные, предоставленные в рамках заявки на грант.

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, удаление, уничтожение.

2) физических лиц представителей и руководителей организаций-участников:

Иные категории ПДн: фамилия, имя, отчество, контактная информация (адрес электронной почты), данные документа, удостоверяющего личность, иные данные, предоставленные в рамках заявки на грант.

Способ обработки персональных данных: смешанный.

Перечень действий с персональными данными: распространение, сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, удаление, уничтожение.

5. Порядок и условия обработки персональных данных

5.1. Перечень действий с ПДн субъектов, осуществляемых Организацией.

Организацией осуществляются следующие действия с ПДн: распространение, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

5.2. Способы обработки ПДн

Организацией применяются смешанные способы обработки ПДн с передачей по внутренней сети юридического лица, с передачей по сети Интернет.

5.3. Передача ПДн третьим лицам:

1) Инспекция Федеральной налоговой службы по г. Салехарду

Условия передачи персональных данных: поручение Оператора.

Местонахождение третьего лица: 629001, Ямало-Ненецкий АО, г. Салехард, ул. Подшибякина, д. 51.

Трансграничная передача персональных данных не осуществляется.

Цели передачи персональных данных: в соответствии с действующим законодательством.

Перечень действий, разрешенных третьему лицу: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение).

Способы обработки ПДн третьим лицом: смешанная обработка персональных данных с передачей по внутренней сети и сети интернет.

2) Региональное отделение Фонда социального страхования Российской Федерации по Ямало-Ненецкому автономному округу

Условия передачи персональных данных: поручение Оператора.

Местонахождение третьего лица: 629008, Ямало-Ненецкий АО, г. Салехард, ул. Республики, д. 117а.

Трансграничная передача персональных данных не осуществляется.

Цели передачи персональных данных: в соответствии с законодательством о социальном страховании граждан РФ.

Перечень действий, разрешенных третьему лицу: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, передача (распространение, предоставление, доступ), извлечение.

Способы обработки ПДн третьим лицом: смешанная обработка персональных данных с передачей по внутренней сети и сети интернет.

3) Отделение Пенсионного фонда Российской Федерации по Ямало-Ненецкому автономному округу

Условия передачи персональных данных: поручение Оператора.

Местонахождение третьего лица: 629008, Ямало-Ненецкий АО, г. Салехард, ул. Республики, д. 47.

Трансграничная передача персональных данных не осуществляется.

Цели передачи персональных данных: в соответствии с законодательством о пенсионном обеспечении граждан России.

Перечень действий, разрешенных третьему лицу: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование.

Способы обработки ПДн третьим лицом: смешанная обработка персональных данных с передачей по внутренней сети и сети интернет.

Кроме того, Организация вправе передавать ПДн органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

5.4. Меры по обеспечению безопасности ПДн при их обработке

Организация, при обработке ПДн, принимает необходимые правовые, организационные и технические меры, и обеспечивает их принятие 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.

Обеспечение безопасности ПДн достигается Организацией, в частности, следующими мерами:

1) оценка вреда, в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинён субъектам персональных данных в случае нарушения закона «О персональных данных», соотношение указанного вреда и принимаемых защитных мер, направленных на обеспечение выполнения обязанностей, предусмотренных законом «О персональных данных»;

2) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных закону «О персональных данных» и внутренним документам Организации по вопросам обработки персональных данных;

3) ознакомление служащих, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, политикой Организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных служащих;

4) издание политики Организации в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

5) учёт машинных носителей персональных данных;

6) назначение ответственного за организацию обработки персональных данных;

7) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

9) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

10) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

11) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учёта всех действий, совершаемых с персональными данными в информационной системе персональных данных;

12) обнаружение фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

13) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищённости информационных систем персональных данных;

14) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищённости персональных данных;

15) обеспечение взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерные доступ, представление, распространение, передачу персональных данных.

5.5. Базы ПДн Организации находятся полностью в пределах территории Российской Федерации.

5.6. Сроки обработки ПДн

Персональные данные субъектов, обрабатываемые Организацией, подлежат уничтожению либо обезличиванию в случае:

1) достижения целей обработки ПДн или утраты необходимости в достижении этих целей;

2) отзыва субъектом ПДн согласия на обработку его ПДн;

3) истечение срока действия согласия субъекта ПДн на обработку его ПДн;

4) отсутствия возможности обеспечить правомерность обработки ПДн;

5) прекращения деятельности Организации.

5.7. Условия обработки ПДн без использования средств автоматизации

При обработке ПДн, осуществляемой без использования средств автоматизации, Организация выполняет требования, установленные

постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Персональные данные при такой их обработке обособляются от иной информации, в частности, путём фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

6. Регламент реагирования на запросы обращения субъектов персональных данных и их представителей

При устном обращении либо письменном запросе субъекта ПДн или его представителя на доступ к ПДн субъекта, Организация руководствуется требованиями статей 14, 18 и 20 Федерального закона № 152-ФЗ и требованиями по соблюдению мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Субъект ПДн или его представитель может воспользоваться формами запросов (заявлений) или отзывом согласия, приведенные в приложениях к настоящей Политике.

Сведения о наличии и обработке ПДн предоставляются субъекту ПДн или его представителю Организацией при обращении либо при получении запроса от субъекта ПДн или его представителя. Запрос 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 Организацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Организацией, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Доступ субъекта ПДн или его представителя к ПДн субъекта Организация предоставляет только под контролем ответственного за организацию обработки ПДн (далее Ответственный) Организации.

Ответственный Организации принимает решение о предоставлении доступа субъекту ПДн или его представителю к ПДн указанного субъекта.

В случае, если данные, предоставленные субъектом ПДн или его представителем не достаточны для установления его личности или предоставление ПДн нарушают конституционные права и свободы других лиц, Ответственный Организации подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющийся основанием для такого отказа, в срок, не превышающий 10 рабочих дней со дня обращения субъекта ПДн или его представителя либо от даты получения запроса субъекта ПДн или его

представителя. Указанный срок может быть продлён, но не более чем на 5 рабочих дней в случае направления Организацией в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Сведения предоставляются субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

Для предоставления доступа субъекту ПДн или его представителя к ПДн субъекта, Ответственный Организации привлекает служащих структурного подразделения (отдела), обрабатывающих ПДн субъекта, по согласованию с руководителем этого структурного подразделения (отдела).

Организация предоставляет безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящиеся к этому субъекту ПДн.

Сведения о наличии ПДн Организация предоставляет субъекту ПДн или его представителю в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Контроль предоставления сведений субъекту ПДн или его представителю осуществляет Ответственный Организации.

Сведения о наличии ПДн должны быть предоставлены субъекту ПДн или его представителю при ответе на запрос или при обращении в течение 10 рабочих дней от даты получения запроса (обращения) субъекта ПДн или его представителя. Указанный срок может быть продлён, но не более чем на 5 рабочих дней в случае направления Организацией в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Сведения предоставляются субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

В случае отказа Организацией в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя, Организация предоставляет в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 10 рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлён, но не более чем на 5 рабочих дней в случае направления Организацией в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе, если:

1) обработка ПДн, включая ПДн, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

3) обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма;

4) доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

5) обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

7. Регламент реагирования, в случае запроса уполномоченного органа по защите прав субъектов персональных данных

В соответствии с частью 4 статьи 20 Федерального закона № 152-ФЗ, Организация сообщает в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 10 дней с даты получения такого запроса. Указанный срок может быть продлён, но не более чем на 5 рабочих дней в случае направления Организацией в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет Ответственный Организации, при необходимости с привлечением служащих Организации.

В течение установленного срока Ответственный Организации подготавливает и направляет в уполномоченный орган по защите прав субъектов ПДн мотивированный ответ и другие необходимые документы.

Приложение 1
к Политике обработки персональных данных АНО «Гранты Ямала»

Директору АНО «Гранты Ямала»

Х.Н. Алхаматову

от _____
(Ф.И.О., номер основного документа, удостоверяющего личность

_____
субъекта или его законного представителя, сведения о дате

выдачи

_____
указанного документа и выдавшем органе, адрес,

_____
контактные данные)

ЗАЯВЛЕНИЕ
на уточнение/блокирование/уничтожение персональных данных, в связи с выявлением недостоверных или неправомерных действий с персональными данными

Прошу:

☐ уточнить

☐ заблокировать

☐ уничтожить

мои персональные данные, обрабатываемые в АНО «Гранты Ямала», в связи с выявлением следующих недостоверных сведений или неправомерных действий:

_____

_____
(перечислить)

_____ _____ _____
(дата) (подпись) (И.О. Фамилия)

Приложение 2
к Политике обработки персональных данных АНО «Гранты Ямала»

Директору АНО «Гранты Ямала»

Х.Н. Алхаматову

от _____
(Ф.И.О., номер основного документа, удостоверяющего личность

_____
субъекта или его законного представителя, сведения о дате

выдачи

_____
указанного документа и выдавшем органе, адрес,

_____
контактные данные)

ЗАЯВЛЕНИЕ
на прекращение обработки персональных данных

Прошу прекратить обработку моих персональных данных в связи с:

☐ отсутствием согласия

☐ неправомерной обработкой

☐ достижения цели обработки

☐ Иное:

_____

_____

_____

_____

(описать причину)

_____ _____ _____
(дата) (подпись) (И.О. Фамилия)

Приложение 3
к Политике обработки персональных данных АНО «Гранты Ямала»

Директору АНО «Гранты Ямала»

Х.Н. Алхаматову

от _____
(Ф.И.О., номер основного документа, удостоверяющего личность

_____
субъекта или его законного представителя, сведения о дате

выдачи

_____
указанного документа и выдавшем органе, адрес,

_____
контактные данные)

ЗАЯВЛЕНИЕ
на получение доступа к персональным данным

Прошу предоставить мне для ознакомления следующую информацию (в том числе документы), составляющую мои персональные данные:

_____

_____

_____

_____

_____
(описать причину)

_____ _____ _____
(дата) (подпись) (И.О. Фамилия)

Приложение 4
к Политике обработки персональных данных АНО «Гранты Ямала»

Директору АНО «Гранты Ямала»

Х.И. Алхаматову

от _____
(Ф.И.О., номер основного документа, удостоверяющего личность

_____
субъекта или его законного предетавителя, сведения о дате

выдачи

_____
указанного документа и выдавшем органе, адрес,

_____
контактные данные)

ЗАЯВЛЕНИЕ
на отзыв согласия обработки персональных данных

Прошу Вас прекратить обработку моих персональных данных в связи с:

_____

_____

_____

_____

_____
(описать причину)

_____ _____ _____
(дата) (подпись) (И.О. Фамилия)

Приложение №6

УТВЕРЖДАЮ

Директор АНО «Гранты Ямала»

_____ Х.Н. Алхаматов

«19» 09 2025 г.

ИНСТРУКЦИЯ
по допуску сотрудников автономной некоммерческой организации «Гранты Ямала» в помещения, в которых ведётся обработка персональных данных

1. Общие положения

Настоящая инструкция разработана в целях обеспечения безопасности персональных данных (далее — ПДн), средств вычислительной техники информационных систем, обрабатывающие ПДн, материальных носителей ПДн, а также обеспечения режима внутри объектового.

Документ устанавливает правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях.

Объектами охраны автономной некоммерческой организации «Гранты Ямала» (далее — Организация) являются:

1) помещения, в которых происходит обработка ПДн как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;

2) помещения, в которых хранятся материальные носители ПДн и резервные копии ПДн;

3) помещения, в которых установлены средства криптографической защиты информации (далее — СКЗИ), предназначенные для шифрования ПДн, в том числе носители ключевой информации (далее — спецпомещения).

Бесконтрольный доступ посторонних лиц в указанные помещения исключён.

Посторонними лицами считаются сотрудники Организации, не допущенные к обработке ПДн и лица, не являющиеся сотрудниками Организации.

К спецпомещениям предъявляются дополнительные требования по безопасности, указанные в разделе 4.

Ответственность за соблюдение положений настоящего порядка несут сотрудники структурных подразделений (отделов) Организации, допущенные в помещения, являющиеся объектами охраны, а также их непосредственные руководители.

Контроль соблюдения требований, описанных в данном документе, обеспечивает должностное лицо, назначенное ответственным за организацию обработки ПДн Организации.

Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению. Например, металлические решётки на окнах, металлическая дверь, система контроля и управления доступом и так далее.

2. Правила доступа в помещения, в которых ведётся обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведётся обработка ПДн, а также хранятся материальные носители ПДн и (или) их резервные копии, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица, из числа сотрудников Организации, допущенных к обработке ПДн. При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с ПДн. Например, мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

При возникновении чрезвычайных ситуаций природного или техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в помещения, в которых ведётся обработка ПДн, лиц, из числа сотрудников Организации, не допущенных к обработке ПДн.

В нерабочее время все окна и двери в помещениях (в том числе в смежных помещениях), в которых ведётся обработка ПДн, должны быть надёжно закрыты, материальные носители ПДн должны быть убраны в запираемые шкафы (сейфы) или тумбочки, компьютеры выключены либо заблокированы.

Доступ сотрудников Организации в помещения, в которых ведётся обработка ПДн в нерабочее время, в том числе в выходные и праздничные дни, допускается только по письменному распоряжению директора автономной некоммерческой организации «Гранты Ямала» на основании предоставленных на его имя заявок (служебных записок) с перечнем сотрудников Организации от руководителей структурных подразделений (отделов), доступ которым крайне необходим (с обоснованием, датой и временем выполняемых работ).

3. Правила доступа в серверные помещения

Доступ посторонних лиц в серверные помещения, в которых ведётся обработка ПДн, допускается по согласованию с ответственным за обеспечение безопасности информационных систем ПДн Организации.

Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций,

которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за обеспечение безопасности информационных систем ПДн Организации.

Доступ сотрудников Организации в серверные помещения в нерабочее время, в том числе в выходные и праздничные дни, допускается только по письменному распоряжению директора автономной некоммерческой организации «Гранты Ямала» на основании предоставленных на его имя заявок (служебных записок) с перечнем сотрудников Организации от руководителей структурных подразделений (отделов), доступ которым крайне необходим (с обоснованием, датой и временем выполняемых работ).

4. Правила доступа в спецпомещения

Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений и устройствами опечатывания в нерабочее время. Окна спецпомещений, расположенные на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Расположение спецпомещения, специальное оборудование и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами осуществляемых в помещении работ.

Для предотвращения просмотра спецпомещений извне их окна должны быть защищены.

Спецпомещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей спецпомещений на замок и открытие только для санкционированного прохода, а также опечатывание спецпомещений по окончании рабочего дня или оборудование спецпомещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии спецпомещений.

Доступ в спецпомещения осуществляется в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, утверждённый приказом директора автономной некоммерческой организации «Гранты Ямала».

Доступ иных лиц в спецпомещения может осуществляться под контролем лиц, имеющих право допуска в спецпомещения.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в спецпомещения иных лиц из числа сотрудников Организации.

Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения (отдела) и (или) ответственного пользователя СКЗИ Организации.

При утрате ключа от входной двери в спецпомещение, необходимо заменить замок или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

Доступ сотрудников в спецпомещения в нерабочее время, в том числе в выходные и праздничные дни, допускается только по письменному распоряжению директора автономной некоммерческой организации «Гранты Ямала» на основании предоставленных на его имя заявок (служебных записок) с перечнем сотрудников Организации от руководителей структурных подразделений (отделов), доступ которым крайне необходим (с обоснованием, датой и временем выполняемых работ).

Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается.

Приложение №7

УТВЕРЖДАЮ

Директор АНО «Гранты Ямала»

_____ Х.Н. Алхаматов

«31» 01 2025 г.

Инструкция об осуществлении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленные Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами, политике и локальными актами оператора автономной некоммерческой организации «Гранты Ямала»

1. Общие положения

Настоящая инструкция разработана в соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и требованиями по соблюдению мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», и определяют порядок организации и осуществления контроля выполнения соответствия обработки персональных данных требованиям к защите персональных данных в автономной некоммерческой организации «Гранты Ямала» (далее Организация).

Инструкция обязательна для исполнения всеми должностными лицами Организации, осуществляющими контроль состояния защиты персональных данных.

Контроль выполнения соответствия обработки персональных данных требованиям к защите персональных данных Организации осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, правильности обработки персональных данных ответственными лицами в структурных подразделениях, а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных Организации.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов Организации или нарушения требований по обработке и защите персональных данных.

Проверки осуществляются ответственным за организацию обработки персональных данных Организации либо комиссией, образуемой директором автономной некоммерческой организации «Гранты Ямала».

Сроки проведения контрольных проверок доводятся руководителям

проверяемых структурных подразделений не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых подразделений (отделов).

Периодичность и сроки проведения плановых проверок подразделений Организации устанавливаются планом, утверждаемым директором автономной некоммерческой организации «Гранты Ямала». Сроки проведения плановых проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании приказа директора автономной некоммерческой организации «Гранты Ямала» и утвержденного плана проверок. Ответственный за организацию обработки персональных данных Организации подготавливает предложения по составу комиссии. Проект приказа о проверке подготавливает ответственный за организацию обработки персональных данных Организации.

Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения.

3. Порядок проведения проверки

По прибытию в структурное подразделение для проведения проверки председатель комиссии прибывает к руководителю проверяемого структурного подразделения Организации, представляется ему и представляет других прибывших на проверку лиц.

Руководитель проверяемого структурного подразделения обязан оказывать содействие комиссии по проверке и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите персональных данных, выявление ответственных за обработку и защиту персональных данных и установление факта ознакомления сотрудников проверяемого структурного подразделения со своей ответственностью;

2) получение при содействии сотрудников проверяемого структурного подразделения документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;

3) анализ полученной документации;

4) непосредственная проверка выполнения установленного порядка

обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проведения проверки, а также каких должностных лиц структурного подразделения необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по обработке и защите персональных данных в проверяемом структурном подразделении Организации рассматриваются, в частности, следующие показатели:

1) в части общей организации работ по обработке персональных данных:

а) соответствие информации, указанной в уведомлении об обработке персональных данных Организации, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (персональных данных), их полнота, в соответствии с нормативными правовыми актами и локальными актами, принятыми Организацией;

в) наличие нормативных документов по защите персональных данных;

г) знание нормативных документов сотрудниками (служащими), имеющими доступ к персональным данным;

д) полнота и правильность выполнения требований нормативных документов Организации сотрудниками (служащими), имеющими доступ к персональным данным;

е) наличие документов, определяющих состав сотрудников, ответственных за организацию защиты персональных данных в подразделении, соответствие этих документов реальному штатному составу подразделения, а также подтверждение факта ознакомления ответственных сотрудников с данными документами;

ж) уровень подготовки сотрудников, ответственных за организацию защиты персональных данных в подразделении;

з) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных.

2) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к персональным данным;

б) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о структурных подразделениях Организации, должностных инструкциях сотрудников (служащих) и трудовых договорах;

в) порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

г) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

д) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих персональные данные;

е) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

ж) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

Во время проведения проверки выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

1) актом при проведении проверки комиссией (Приложение № 1);

2) служебной запиской при проведении проверки назначенными специалистами.

Акт и/или служебная записка составляется в двух экземплярах и подписывается членами комиссии.

Один экземпляр хранится у ответственного за организацию обработки персональных данных Организации. Второй экземпляр хранится в Организации в установленном порядке. Копия акта о проверке остается в проверяемом структурном подразделении.

Результаты проверок структурных подразделений периодически обобщаются ответственным за организацию обработки персональных данных Организации и доводятся до руководителей структурных подразделений. При необходимости принятия решений по результатам проверок структурных подразделений на имя директора автономной некоммерческой организации «Гранты Ямала» готовятся соответствующие служебные записки.

Приложение № 1

УТВЕРЖДАЮ
Должность

ФИО

« » 202 г.

ОТЧЕТ (заключение)
по результатам контроля выполнения принятых организационных и технических мер по обработки персональных данных

В соответствии со статьей 18.1 Федерального закона от № 152-ФЗ «О персональных данных» и Планом внутренних мероприятий состояния защиты персональных данных на 20 год, комиссией автономной некоммерческой организации «Гранты Ямала», в период с « » 20 г. по « » 20 г. проведена проверка соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях автономной некоммерческой организации «Гранты Ямала».
В ходе проведения проверки установлено:

;
(указываются сведения о выполнении в автономной некоммерческой организации «Гранты Ямала» требований, установленных ФЗ-152 «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, организационно-распорядительных документов автономной некоммерческой организации «Гранты Ямала»)

В ходе проведения проверки:
- выявлены нарушения требований по обеспечению безопасности:

;
(описание выявленных нарушений)

Рекомендации:

Прилагаемые к акту документы:

;
;
Примечание: к отчету могут прилагаться необходимые документы, схемы, иллюстрации и другие поясняющие материалы.

Председатель комиссии:
Члены комиссии: