Приложение
к приказу ООО «НЦРДО»
от 27 сентября 2022 г. № 332

Общество с ограниченной ответственностью
«Национальный центральный институт развития
дополнительного образования»
(ООО «НЦРДО»)

ИНН/КПП 7726462390/772601001, ОГРН 1207700047103
117556, г. Москва, ул. Фруктовая, д. 7, к. 1, комната 12
тел. +7 (499) 288-00-36, e-mail: help@ncrdo.ru, веб-сайт: https://ncrdo.ru

УТВЕРЖДАЮ
Генеральный директор
ООО «НЦРДО»

_____ А.И. Зотов

ПОЛИТИКА
В ОБЛАСТИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «НАЦИОНАЛЬНЫЙ ЦЕНТРАЛЬНЫЙ ИНСТИТУТ РАЗВИТИЯ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ» (ООО «НЦРДО»)

Москва, 2022 г.

1. Общие положения

1.1. Обработка персональных данных осуществляется Обществом с ограниченной ответственностью «Национальный центральный институт развития дополнительного образования» (далее – Организация, оператор) на законной и справедливой основе, основными правовыми основаниями для обработки являются:

- Конституция РФ;
- Гражданский кодекс РФ;
- Трудовой кодекс РФ;

в соответствии с требованиями:

- Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федеральный закон РФ от 07.07.2003 № 126-ФЗ «О связи»;
- Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Устав Организации;
- Договоры и соглашения Организации;
- Согласия субъектов персональных данных.

1.2. Цель настоящей Политики в области обработки и защиты персональных данных в Обществе с ограниченной ответственностью «Национальный центральный институт развития дополнительного образования» (далее - Политика) – обеспечение прав граждан при обработке их персональных данных, и принятие мер от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных субъектов.

1.3. Содержание и объем обрабатываемых персональных данных определяются исходя из целей обработки. Не обрабатываются персональные данные, избыточные или несовместимые по отношению к следующим основным целям:

а) предоставления образовательных услуг и услуг содействия в трудоустройстве;

б) организации обучения с применением электронного обучения и дистанционных образовательных технологий;

в) оказания информационно-консультационных услуг в сфере образования;

г) заключение трудовых отношений с физическими лицами, подбор персонала;

д) заключение, продление договорных отношений;

е) идентификация сторон договоров, соглашений, сделок;

ж) выполнение договорных обязательств, включая оказание услуг, предоставление прав на использование информационных ресурсов Организации в соответствии с правилами использования, лицензионными соглашениями, а также регистрация, идентификация лиц, являющихся пользователями информационных ресурсов, предоставление доступа к ресурсам и функциям, доступным только для зарегистрированных пользователей;

з) организация конференций, семинаров, вебинаров, иных публичных мероприятий в интересах Организации, партнерских организаций, профессиональных сообществ;

и) автоматизации работы библиотеки;

к) проведения мониторинга деятельности Организации;

л) осуществление связи с физическими и юридическими лицами для направления им уведомлений, ответов на запросы, рассылок и информационных сообщений, а также сообщений маркетингового характера для продвижения продуктов и услуг Организации, как с использованием собственных программных продуктов, так и на основании договоров с партнерскими организациями;

м) участие лиц в акциях и бонусных программах Организации;

н) защита законных интересов Организации, их партнеров и клиентов;

о) противодействие незаконным или несанкционированным действиям, мошенничеству при использовании потребителями и предоставлении потребителям продуктов и услуг Организации, обеспечение информационной безопасности.

1.4. К основным категориям субъектов персональных данных, чьи данные обрабатываются Оператором, относятся:

1.4.1. физические лица, состоящие или состоявшие в трудовых и гражданско-правовых отношениях с Организацией, а также лица, имеющие намерения вступить в такие отношения, например, кандидаты на замещение вакантных должностей;

1.4.2. физические лица, состоящие или состоявшие в трудовых и гражданско-правовых отношениях с контрагентами Организации, а также лица, имеющие намерения вступить в такие отношения;

1.4.3. физические лица, указанные в различных государственных реестрах, базах данных, общедоступных и иных источниках, которые получены законным способом и используются при оказании услуг и в продуктах Организации в качестве источников данных;

1.4.4. физические лица, обратившиеся в Организацию с запросами, сообщениями, заявлениями, жалобами, предложениями с использованием контактной информации или средств сбора обратной связи;

1.4.5. физические лица, обратившиеся за содействием в трудоустройстве после окончания образовательных программ;

1.4.6. физические лица, участвующие в интервью, опросах, аналитических и маркетинговых исследованиях по тематике деятельности Организации;

1.4.7. участники мероприятий, организованных Организацией или организациями партнерами.

1.5. Передача третьим лицам персональных данных без письменного согласия не допускается. Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законом.

1.6. Работники, в обязанность которых входит обработка персональных данных субъекта, обязаны обеспечить каждому возможность ознакомления с документами и материалами,

непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом, а также настоящей Политикой.
1.7. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
1.8. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
1.9. Настоящая Политика утверждается руководителем Организации и является обязательной для исполнения всеми работниками, имеющими доступ к персональным данным субъекта.
1.10. Оператор имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.
1.11. Действующая редакция хранится в месте нахождения Оператора по адресу: 117556, г. Москва, ул. Фруктовая, д. 7, к. 1, комната 12; электронная версия Политики – на сайте по адресу: http://ncrdo.ru/

2. Термины и принятые сокращения

2.1. 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.
2.2. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.
2.3. Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
2.4. Персональные данные, сделанные общедоступными субъектом персональных данных – ПД, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.
2.5. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
2.6. 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.

2.7. Оператор – организация, обрабатывающая персональные данные.

3. Понятие и состав персональных данных

3.1. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (далее – субъекту). К персональным данным субъекта, которые обрабатывает Организация, относятся:

а) фамилия, имя, отчество;

б) адрес места жительства;

в) данные документа, удостоверяющего личность;

г) данные о составе семьи;

д) контактный телефон;

е) адрес электронной почты;

ж) данные страхового свидетельства;

з) данные о трудовой деятельности;

и) документы подтверждающие уровень образования (квалификации);

к) результаты успеваемости и тестирований;

л) иная необходимая информация, которую субъект добровольно сообщает о себе для получения услуг предоставляемых Организацией, если ее обработка не запрещена законом.

4. Условия и основные принципы обработки, передачи и хранения персональных данных

4.1. Организация ведет обработку персональных данных субъекта с использованием средств автоматизации (автоматизированная обработка), и без использования таких средств (неавтоматизированная обработка).

4.2. Обработка персональных данных должна осуществляться на основе принципов:

а) законности целей и способов обработки персональных данных и добросовестности;

б) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям организации;

в) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

г) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

д) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

е) уничтожения персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;

ж) личной ответственности работников организации за сохранность и конфиденциальность персональных данных, а также носителей этой информации.

4.3. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПД, характере подлежащих получению ПД, перечне действий с ПД,

сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта предоставить его персональные данные и (или) дать согласие на их обработку, если в соответствии с федеральным законом предоставление персональных данных и (или) получение оператором согласия на обработку персональных данных являются обязательными.

4.4. Документы, содержащие ПД, создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

б) внесения сведений в учетные формы;

в) получения оригиналов необходимых документов (трудовая книжка, характеристика и др.);

г) получения копий документов по установленным между оператором и субъектом ПД каналам связи.

4.5. Обработка персональных данных осуществляется:

а) с согласия субъекта персональных данных на обработку его персональных данных;

б) в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

в) в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).

5. Сведения о третьих лицах, участвующих в обработке персональных данных

5.1. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:

а) Министерству образования и науки Российской Федерации;

б) Федеральной налоговой службе Российской Федерации;

в) Пенсионному фонду России;

г) Фонду социального страхования Российской Федерации;

д) Федеральной службе государственной статистики Российской Федерации;

е) Фонду обязательного медицинского страхования Российской Федерации;

ж) Банкам для начисления заработной платы (на основании договора);

з) Правоохранительным органам (в случаях, установленных законодательством);

и) Кредитным организациям (с согласия субъекта);

к) Лицензирующим и (или) контролирующим органам государственной власти и местного самоуправления.

5.2. Оператор может поручать обработку персональных данных другим лицам на основании договора с согласия субъекта персональных данных.

6. Обязанности оператора

6.1. В целях обеспечения прав и свобод человека и гражданина организации при обработке персональных данных субъекта обязано соблюдать следующие общие требования:

6.1.1. Обработка персональных данных субъекта может осуществляться исключительно в целях оказания законных услуг субъектам.

6.1.2. Персональные данные субъекта следует получать у него самого. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работники Организации должны сообщить субъектам о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта предоставить его персональные данные и (или) дать согласие на их обработку, если в соответствии с федеральным законом предоставление персональных данных и (или) получение оператором согласия на обработку персональных данных являются обязательными.

6.1.3. Организация не обрабатывает специальные категории персональных данных о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных законом.

6.1.4. Оператор обязан в течение десяти рабочих дней с момента обращения либо получения Оператором запроса субъекта предоставлять ему или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.1.5. Хранение и защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается учреждением, за счет его средств в порядке, установленном действующим законодательством Российской Федерации.

6.1.6. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта либо уполномоченного органа по защите прав субъектов персональных данных Организация обязана осуществить блокирование персональных данных на период проверки.

6.1.7. В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

6.1.8. В случае достижения цели обработки персональных данных Организация обязана незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий десяти рабочих дней.

6.1.9. В случае отзыва субъектом согласия на обработку своих персональных данных, Организация обязана в срок, не превышающий десяти рабочих дней с даты получения Оператором соответствующего требования, прекратить их обработку или

обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных) и уничтожить персональные данные.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, то известить указанный орган.

6.1.10. Оператор обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

6.2. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор обязан с момента выявления им такого инцидента, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

6.2.1. в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

6.2.2. в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

7. Особенности обработки сотрудниками / дистанционными работниками персональных данных и меры защиты ПД

7.1. Организация предпринимает необходимые меры защиты при обработке персональных данных (правовые, организационные и технические).

7.2. Меры по организации работы с персональными данными в организации и порядок общения по каналам связи между должностными лицами (в том числе лицами, осуществляющими трудовые обязанности удаленно или лицами, осуществляющими обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации на основании заключенных договоров) предпринимаются для решения вопросов, связанных с использованием персональных данных.

7.2.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы

создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

7.2.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица. Информация и связанные с ней ресурсы должны быть доступны только для авторизованных пользователей.

7.2.3. Основными мерами защиты ПД, используемыми оператором, являются:

а) назначение приказом лиц ответственных за обработку ПД, которое осуществляет организацию обработки ПД, внутренний контроль за соблюдением оператором и его работниками требований к защите ПД;

б) разработка настоящей Политики в отношении обработки и защиты персональных данных;

в) установление правил доступа к ПД, а также обеспечения учета действий, совершаемых с ПД;

г) установление индивидуальных паролей доступа сотрудников в информационную систему и в аккаунт электронного почтового ящика в соответствии с производственными обязанностями;

д) применение сертифицированного антивирусного программного обеспечения с регулярно обновляемыми базами;

е) соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ посторонних лиц;

ж) обнаружение фактов несанкционированного доступа к персональным данным и принятия мер к его устранению;

з) осуществление внутреннего контроля и аудита.

7.3. Перечень адресов электронной почты, а также иные корпоративные каналы связи, которые используются для передачи любых персональных данных, включая файлы, их содержащие, устанавливаются отдельным локальным актом Организации. Указанный в таком акте перечень адресов и каналов содержит данные, необходимые для доступа в аккаунт, которые являются конфиденциальными и выдаются сотруднику под личную подпись ГПХ – на эл. почту.

7.4. Организация предоставляет доступ к информационным системам средств связи с использованием технологии удаленного доступа (сервер провайдера 1dedic (по адресу - https://1dedic.ru/), в том числе к корпоративному чату Whatsapp Messenger, LMS Moodle (по адресу: https://sdo.ncrdo.ru/), к сайту оператора (по адресу - https://ncrdo.ru/), аккаунту электронной почты, необходимого для выполнения сотрудниками своих служебных (трудовых) обязанностей.

7.4.1. Допущенному к персональным данным удаленному сотруднику необходимо использовать в работе только компьютерную технику со следующим рекомендованным сертифицированным антивирусным программным обеспечением:

1) ESET NOD32;

2) AVIRA ANTIVIRUS;

3) Стандартный защитник Windows (начиная с Windows 10).

7.4.2. В качестве электронного канала связи используется только предоставленный оператором для этих целей канал, в соответствии с п.7.3. настоящей Политики.

7.5. В случае выявления несанкционированного доступа к персональным данным следует немедленно сообщить непосредственному руководителю, для привлечения IT-специалистов с целью нейтрализации угрозы безопасности ПД.

7.6. Обязанность по организации возможности удаленной работы и (или) допуска работника к защищенной информации в организации, предупреждения и нейтрализации угроз безопасности ПД и информационных систем возлагается на IT-специалистов. В

рамках реализации указанных функций IT-специалисты предпринимают следующие действия:

7.6.1. Идентификация и аутентификация субъектов доступа и объектов доступа;

7.6.2. Управление доступом субъектов доступа к объектам доступа;

7.6.3. Ограничение программной среды;

7.6.4. Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные сотрудниками, допущенными в соответствии с п.7.3., и осуществляющими служебную деятельность по месту нахождения оператора;

7.6.5. Регистрация событий безопасности;

7.6.6. Антивирусная защита персональных компьютеров по месту нахождения оператора;

7.6.7. Обнаружение (предотвращение) вторжений;

7.6.8. Контроль (анализ) защищенности персональных данных;

7.6.9. Обеспечение целостности информационной системы и персональных данных;

7.6.10. Обеспечение доступности персональных данных;

7.6.11. Защита среды виртуализации;

7.6.12. Защита технических средств;

7.6.13. Защита информационных систем, их средств, систем связи и передачи данных собственными мерами оператора либо на основании заключенных договоров;

7.6.14. Выявление инцидентов, которые могут привести к сбоям или нарушению функционирования собственных информационных систем и (или) к возникновению угроз безопасности персональных данных, и реагирование на них.

8. Права субъекта

8.1. Право на доступ к информации о самом себе.

8.2. Право на определение форм и способов обработки персональных данных.

8.3. Право на отзыв согласия на обработку персональных данных.

8.4. Право ограничивать способы и формы обработки персональных данных, запрет на распространение персональных данных путём не предоставления его согласия.

8.5. Право требовать изменение, уточнение, уничтожение информации о самом себе.

8.6. Право обжаловать неправомерные действия или бездействия по обработке персональных данных и требовать соответствующей компенсации в суде.

8.7. Право на дополнение персональных данных оценочного характера заявлением, выражающим его собственную точку зрения.

8.8. Право определять представителей для защиты своих персональных данных.

8.9. Право требовать от организации уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них.

9. Порядок доступа к персональным данным субъекта

9.1. Персональные данные субъекта могут быть предоставлены третьим лицам только с письменного согласия субъекта.

9.2. Доступ субъекта к своим персональным данным предоставляется в течение десяти рабочих дней с момента обращения либо получения Оператором запроса субъекта. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Оператором в адрес субъекта персональных данных мотивированного

уведомления с указанием причин продления срока предоставления запрашиваемой информации. Оператор обязан сообщить субъекту информацию о наличии персональных данных о нем.

9.3. Запрос должен содержать номер основного документа, удостоверяющего личность Субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

9.4. Субъект имеет право на получение при обращении или при отправлении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных Оператором;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые оператором способы обработки персональных данных;

г) наименование и место нахождения Оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

е) сроки обработки персональных данных, в том числе сроки их хранения;

ж) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

з) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

и) информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 настоящего Федерального закона.

9.5. Сведения о наличии персональных данных должны быть предоставлены субъекту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

9.6. Право субъекта на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает конституционные права и свободы других лиц.

10. Ответственность за разглашение персональных данных

10.1. Оператор несет ответственность за персональную информацию, которая находится в его распоряжении и закрепляет персональную ответственность работников за соблюдением, установленных в организации принципов уважения приватности.

10.2. Каждый работник Организации, получающий для работы доступ к материальным носителям персональным данных, несет ответственность за сохранность носителя и конфиденциальность информации.

10.3. За нарушение режима конфиденциальности персональных данных виновные лица несут административную, уголовную, гражданско-правовую, а также дисциплинарную

ответственность в случаях, предусмотренных действующим законодательством Российской Федерации.

10.4. В случае если нарушение режима конфиденциальности персональных данных повлекло убытки для работодателя, виновный обязан возместить данные убытки в размерах и порядке, определяемых действующим законодательством Российской Федерации.

10.5. Привлечение к ответственности осуществляется в соответствии с приказом руководителя организации, выносимым на основании отчета специально созываемой для расследования каждого факта нарушения режима конфиденциальности персональных данных комиссии.

10.6. Организация обязуется поддерживать систему приема, регистрации и контроля рассмотрения жалоб субъектов, доступную с помощью телефонной, телеграфной или почтовой связи.

10.7. Любое лицо может обратиться к работнику Организации с жалобой на нарушение данной Политики. Жалобы и заявления по поводу соблюдения требований обработки данных рассматриваются в течение тридцати рабочих дней с момента поступления.

10.8. Работники Организации обязаны на должном уровне обеспечивать рассмотрение запросов, заявлений и жалоб субъектов, а также содействовать исполнению требований компетентных органов. Лица, виновные в нарушении требований настоящей Политики, привлекаются к установленной законодательством Российской Федерации ответственности.