

Муниципальное бюджетное дошкольное образовательное учреждение «Детский сад № 2 «Рябинка» 964760 Россия Сахалинская область с.Горнозаводск, ул. Кольцевая, 31, тел (424 36) 96-517 факс (424 36) 96-517. Регистрационный № 74-009-001115; ИНН 6505009920; КПП 650501001

Утверждено приказом заведующей
МБДОУ «Детский сад № 2 «Рябинка»
от 17.04.2017 г. № 10



Положение об организации обработки и защиты персональных данных третьих лиц в МБДОУ «Детский сад №2 «Рябинка»

Содержание

1	Общие положения	3
2	Понятие и состав ПДн	5
3	Обработка персональных данных третьих лиц.....	7
3.1	Правила получения и обработки персональных данных третьих лиц	7
3.2	Организация работы с ПДн третьих лиц	7
3.3	Организация хранения документов, содержащих ПДн третьих лиц	8
3.4	Уничтожение документов, содержащих ПДн третьих лиц	8
4	Распространение ПДн третьих лиц	10
4.1	Доступ третьих лиц к своим персональным данным	10
4.2	Доступ служащих Управления к ПДн	10
4.3	Передача ПДн третьих лиц	10
4.4	Порядок рассылки документов, содержащих ПДн третьих лиц.....	11
5	Права Субъектов ПДн в отношении своих персональных данных	12
6	Обязанности Управления при обработке ПДн третьих лиц	13
7	Ответственность	14
8	Взаимодействие с уполномоченными органами в области защиты персональных данных.....	16
9	Нормативные документы	17
10	Заключительные положения	17
	Приложение 1 Форма журнала учета выдачи / передачи персональных данных третьих лиц.....	20
	Приложение 2 Соглашение о конфиденциальности с третьей стороной получающей персональные данные третьих лиц.....	21
	Приложение 3 Обязательство о неразглашении персональных данных третьих лиц	25

1. Общие положения

Настоящее Положение разработано в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», распорядительными и методическими документами ФСТЭК России, и определяет порядок обработки персональных данных третьих лиц, права и обязанности сторон трудовых отношений в связи с представлением, получением, хранением, комбинированием, передачей или любым другим использованием ими персональных данных (далее – ПДн), а также порядок защиты персональных данных третьих лиц, в том числе при их обработке в информационных системах персональных данных (далее – ИСПДн).

Положение является внутренним нормативным документом, регламентирующим деятельность МБДОУ «Детский сад №2 «Рябинка» (далее – Учреждение) в сфере обработки ПДн. Положение является обязательным для выполнения всеми работниками, состоящими с Учреждением в трудовых отношениях.

Обработка ПДн в Учреждении осуществляется на основе следующих принципов:

- законности целей и способов обработки ПДн;
- соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям оператора;
- соответствия объема и характера обрабатываемых ПДн, а также способов их обработки заявленным целям;
- достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем ПДн.

Обработка ПДн работников других организаций и сторонних организаций (далее – ПДн третьих лиц) может осуществляться исключительно в целях обеспечения защиты прав и свобод субъекта ПДн при обработке его ПДн или выполнения требований нормативно-правовых актов Российской Федерации. Целью настоящего Положения является обеспечение соблюдения законов и иных нормативных правовых актов Российской Федерации, а также установления ответственности должностных лиц Учреждения, имеющих доступ к ПДн третьих лиц, за невыполнение требований и норм, регулирующих обработку и защиту ПДн.

Обработка и хранение ПДн третьих лиц осуществляются на бумажных и магнитных носителях, в электронном виде, а также с использованием ИСПДн различного назначения.

Защита ПДн третьих лиц от неправомерного их использования или утраты обеспечивается Учреждением в порядке, установленном законодательством Российской Федерации, а также организационно-распорядительными документами Учреждения, за счет своих средств.

2. Понятие и состав ПДн

Под ПДн третьих лиц понимается информация, необходимая Учреждению в связи с договорными или иными отношениями, выполнением требований законодательства Российской Федерации и касающимися конкретного лица.

Субъектами ПДн, обработка ПДн которых осуществляется Учреждением, в соответствии с принципами работы, определенными в настоящем положении, являются:

- третьи лица – физическое лицо, с которым Учреждение имеет договорные или иные отношения, чьи ПДн обрабатываются Учреждением для выполнения требований законодательства Российской Федерации;

- третьи лица – юридическое лицо, с которым Учреждение имеет договорные отношения, соглашения, иные взаимоотношения, предусмотренные законодательными актами Российской Федерации.

Обработка ПДн третьих лиц может осуществляться только с целями, не выходящими за рамки обеспечения деятельности, указанной в Уставе Учреждения.

Таковыми целями могут быть:

- договорные и иные отношения;
- требования и положения законодательства Российской Федерации.

Цель обработки ПДн третьих лиц после расторжения или окончания срока действия договора (в случае его наличия) определяется как обеспечение конституционного права оператора и субъекта на судебную защиту, прохождение оператором налоговой проверки, успешная сдача аудиторской отчетности.

При определении объема и содержания, обрабатываемых ПДн третьих лиц, Учреждение должно руководствоваться целями получения и обработки ПДн.

Информационные ресурсы, содержащие ПДн третьих лиц, создаются путём:

- внесения сведений в учётные формы на бумажных носителях (журнал оказанных услуг, дневной реестр оплаты и т.п.);
- внесения сведений в базы данных.

К ПДн третьих лиц относятся:

1. Информация, содержащаяся в трудовом договоре и дополнительных соглашениях;

2. Информация, содержащаяся в базе данных ИСПДн, ГИС Учреждения, необходимая для выполнения Учреждением требований законодательства Российской Федерации:

- фамилия, имя, отчество;
- дата рождения;
- пол;
- паспортные данные или данные иного документа, удостоверяющего личность (номер документа, сведения о дате выдачи указанного доку-

мента и выдавшем его органе);

- контактный адрес места жительства;
- номер контактного телефона;
- иные, требуемые законодательством.

Состав обрабатываемых ПДн третьих лиц утверждается Приложением «Об организации работы и назначении ответственных за организацию обработки персональных данных».

3. 3. Обработка персональных данных третьих лиц

Правила получения и обработки ПДн третьих лиц

Учреждение получает ПДн третьих лиц в рамках выполнения условий договора с третьими лицами или при выполнении требований законодательства Российской Федерации (в соответствии со статьей 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

В случае получения ПДн третьего лица не от самого, уполномоченный работник Учреждения, должен убедиться в наличии письменного согласия третьего лица на передачу его ПДн стороннему лицу, организации. При отсутствии письменного согласия, уполномоченный работник Учреждения уведомляет третье лицо о начале обработки его ПДн с указанием следующей информации:

- наименование и адрес Учреждения;
- цель обработки ПДн и ее правовое основание в соответствии с п. 3 настоящего Положения;
- предполагаемые пользователи ПДн;
- установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» права Субъекта ПДн в соответствии с п.8.1 настоящего Положения.

Учреждение не имеет права получать и обрабатывать ПДн о политических, религиозных и иных убеждениях и частной жизни третьих лиц. Учреждение не имеет права получать и обрабатывать ПДн о членстве третьих лиц в общественных объединениях и/или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

Учреждение не имеет права запрашивать информацию о состоянии здоровья третьих лиц, за исключением случаев, когда это необходимо для защиты жизни, здоровья или иных жизненно важных интересов третьих лиц, если получение его согласия невозможно.

Организация работы с ПДн третьих лиц:

Учреждение обязано обеспечивать безопасность ПДн третьих лиц, осуществлять их защиту от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Документы, содержащие ПДн третьих лиц, могут создаваться:

- в виде записей баз данных, ведущихся с использованием технических и программных средств ИСПДн, ГИС;
- в виде отдельных файлов (doc, xls и т.п.), создаваемых ответственными лицами.

Доступ работников Учреждения к техническим и программным средствам ИСПДн, ГИС предоставляется на основании решения руководителя Учреждения.

Создание и хранение документов с ПДн третьих лиц в виде отдельных файлов (doc, xls и т.п.) допускается только в ИСПДн, ГИС, а также съемных (машинных), бумажных носителях информации, с реализацией механизма разграничения доступа.

Организация хранения документов, содержащих ПДн третьих лиц

Бумажные документы, содержащие ПДн третьих лиц, обязаны храниться в местах хранения, запирающихся на ключ, сейфах, металлических шкафах и т.п.

При работе с документами, содержащими ПДн третьих лиц, запрещается:

- хранить документы в ящиках стола, оставлять без присмотра;
- брать документы для работы и на хранение домой;
- выносить документы из офиса без разрешения начальника соответствующего подразделения;
- держать документы вне сейфа без необходимости в процессе работы;
- передавать документы на хранение лицам, не имеющим права доступа к данным документам.

Текущее хранение документов, содержащих ПДн третьих лиц, организуют ответственные лица, определяемые приказом.

Правовое регулирование порядка и сроков хранения документов осуществляется на основании требований законодательства Российской Федерации, определивших требования по обработке ПДн третьих лиц.

Организация текущего хранения документов определяется номенклатурой дел, утверждаемой приказом руководителя Учреждения.

Порядок хранения ПДн в электронном виде определяется постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Подготовка документов к последующему хранению включает экспертизу практической ценности документов, оформление и описание дел, составление актов о выделении к уничтожению документов и передачу их в архив организации.

Экспертизу документов проводит комиссия, определяемая приказом руководителя Учреждения. Передача дел в архив осуществляется по графику, утвержденному руководителем Учреждения не реже, чем один раз в три года.

Уничтожение документов, содержащих ПДн третьих лиц

Документы, содержащие ПДн третьих лиц, временного хранения, как правило, в архив Учреждения не передаются, а по истечении срока хранения уничтожаются.

К документам, содержащим ПДн третьих лиц, временного характера относятся документы, которые не должны храниться в архиве в обязательном порядке.

Для решения вопроса об уничтожении такого рода документов один раз в год собирается экспертная комиссия, определяемая приказом руководителя Учреждения.

Итоги работы комиссии оформляются актами об уничтожении документов, содержащих ПДн.

Уничтожение документов, содержащих ПДн третьих лиц, производится любым способом, исключающим ознакомление посторонних лиц с уничтожаемыми материалами и возможность восстановления их текста. Акты составляются и подшиваются в дело.

4. Распространение ПДн третьих лиц

4.1. Доступ третьих лиц к своим ПДн

В случае получения от третьих лиц запроса установленной формы на предоставление его ПДн, Учреждение в течение 10 (десяти) рабочих дней обязано предоставить такие ПДн. Сроки и порядок предоставления ПДн третьих лиц может быть дополнительно уточнен, согласно требованиям законодательства Российской Федерации.

4.2. Доступ работников Учреждения к ПДн третьих лиц

Доступ для работников Учреждения к ПДн третьих лиц, осуществляется при строгом соблюдении требований «Положения об организации обработки и о защите персональных данных третьих лиц» в Учреждении. Доступ для работников Учреждения, кроме работников, утвержденных приказом руководителя Учреждения, к ПДн третьих лиц осуществляется в случаях крайней необходимости. Доступ предоставляется по письменному запросу руководителя структурного подразделения Учреждения на имя руководителя Учреждения, с указанием цели предоставления и перечня ПДн.

Обо всех запросах, о предоставлении ПДн должен быть уведомлен ответственный специалист Административно-правового отдела, который регистрирует их в журнале учета выдачи/передачи ПДн третьих лиц.

4.3. Передача ПДн третьих лиц

При передаче ПДн третьей стороне должны соблюдаться следующие требования:

- передача ПДн третьей стороне осуществляется на основании договора (соглашения) на основании действующего законодательства Российской Федерации;

- существенным условием договора (соглашения) является обеспечение третьей стороной конфиденциальности и безопасности ПДн третьих лиц при их обработке. Форма Соглашения о конфиденциальности приведена в Приложении № 2 к настоящему Положению;

- наличие письменного согласия третьего лица при необходимости.

Обо всех запросах, о предоставлении ПДн должен быть уведомлен административный отдел (ответственный специалист), который регистрирует их в журнале учета выдачи/передачи ПДн третьих лиц (форму журнала см. в Приложении № 1 к настоящему Положению).

При передаче ПДн третьих лиц Учреждение должно соблюдать следующие требования:

- не сообщать ПДн третьего лица кому-либо без письменного его согласия, за исключением случаев, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– предупредить третью сторону, использующую ПДн третьих лиц, 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 от Учреждения ПДн третьих лиц, обязаны соблюдать конфиденциальность полученных ПДн.

Порядок действий с запросами от третьих лиц или их законных представителей на подтверждение наличия, ознакомление, уточнение, уничтожение или отзыв согласия на обработку ПДн дополнительно определен в Регламенте обработки запросов субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных.

4.4. Порядок рассылки документов, содержащих ПДн третьих лиц

Рассылка документов, содержащих ПДн третьих лиц, осуществляется аналогично рассылке документов, содержащих информацию ограниченного доступа, а именно:

– отправка документов осуществляется ответственным специалистом административного отдела Учреждения;

– при получении от исполнителей документов, предназначенных к отправке, ответственный специалист административного отдела Учреждения проверяет наличие всех экземпляров и листов документа, приложений к нему, правильность оформления и адресации;

– перед отправкой необходимо выяснить способ отправки документа (пакет может быть доставлен адресату ценным, заказным письмом, либо лично исполнителем, при наличии такой возможности).

Сведения о способе отправки заносятся в журнал учета исходящих и внутренних документов ограниченного доступа.

Отправлять электронные письма, содержащие информацию ограниченного доступа, допускается только с использованием сертифицированных средств криптографической защиты информации по согласованию с ответственным сотрудником по информационной безопасности Учреждения в соответствии с Политикой информационной безопасности Учреждения.

Основное требование настоящей политики заключается в использовании электронной почты, с криптографическим преобразованием информации при пересылке электронных писем, содержащих ПДн и ограничение круга лиц, которым такие данные могут быть отправлены.

5. Права третьих лиц в отношении своих персональных данных

Третьи лица в отношении своих ПДн имеют право на:

- получение от Учреждения полной информации о своих ПДн и обработке этих данных;
- бесплатный доступ к своим ПДн;
- определение законных представителей для защиты своих ПДн;
- требование уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

6. Обязанности Учреждения при обработке ПДн третьих лиц

При обработке ПДн третьих лиц Учреждение обязано:

- обеспечить защиту ПДн от их неправомерного использования или утраты в порядке, установленном законодательством Российской Федерации и требованиями регулирующих органов;
- ознакомить третье лицо или его законных представителей с его правами в области защиты ПДн;
- осуществлять передачу ПДн третьих лиц только в соответствии с настоящим Положением и законодательством Российской Федерации;
- обеспечить третьему лицу доступ к своим ПДн.

Защита ПДн третьих лиц в ИСПДн, ГИС Учреждения осуществляется на основании постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн», нормативно-методических документов ФСТЭК России, ФСБ России, в соответствии с требованиями Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных.

Доступ в помещения, где осуществляется обработка ПДн третьих лиц, ограничивается организационно-техническими мероприятиями и организационно-распорядительными мерами.

Подразделением (специалистом), ответственным за предоставление доступа к ИСПДн, ГИС Учреждения, является отдел (специалист) по информационной безопасности.

Право внутреннего доступа к ПДн третьих лиц имеют только те работники Учреждения, которым это необходимо для выполнения своих должностных обязанностей в рамках трудового договора с Учреждением. Список таких работников отражен в Разрешительной системе доступа работников Учреждения к ИСПДн, ГИС. Ответственным за ведение Разрешительной системы допуска работников Учреждения к ИСПДн является администратор (специалист) информационной безопасности.

Работниками Учреждения, получающими доступ к ПДн третьих лиц, должна обеспечиваться конфиденциальность этих данных. Форма соглашения о соблюдении конфиденциальности ПДн третьих лиц работниками Учреждения, получающими доступ к этим данным в рамках своих должностных обязанностей, приведена в Приложении № 2 к настоящему Положению.

При обнаружении нарушений порядка предоставления ПДн третьих лиц, работник Учреждения незамедлительно приостанавливает предоставление ПДн до выявления причин нарушений и устранения этих причин.

7. Ответственность

Пункты настоящего Положения обязательны для исполнения работниками Учреждения, в должностные обязанности которых входит обработка и обеспечение безопасности ПДн.

Ознакомление работников Учреждения с настоящим Положением организует руководитель Учреждения.

Принципы работы с ПДн третьих лиц в Учреждении:

- постоянный контроль за состоянием работы с ПДн третьих лиц;
- минимальная уязвимость ПДн третьих лиц;
- персональная ответственность работников Учреждения.

Обязанность по исполнению требований по нераспространению сведений, содержащих ПДн третьих лиц, сохраняется за бывшими работниками Учреждения в течение всего срока действия конфиденциальности сведений.

Ответственным за общее руководство по организации обработки ПДн третьих лиц в Учреждении является руководитель Учреждения, как гарант соблюдения законодательства Российской Федерации.

Ответственность за учет, техническое обслуживание и эксплуатацию средств защиты информации в составе системы защиты ИСПДн, ГИС возложена на отдел (специалиста) информационной безопасности Учреждения.

Учреждение при обработке ПДн третьих лиц предпринимает необходимые организационные и технические меры для их защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

На руководителя Учреждения возлагается:

- принятие мер по предотвращению разглашения и утечки ПДн третьих лиц;
- учет фактов утраты документов и разглашения ПДн третьих лиц, анализ причин и разработка мер по предупреждению таких инцидентов;
- обеспечение учета сейфов, металлических шкафов, специальных хранилищ и помещений (а также ключей к ним), в которых осуществляется хранение и работа с документами, содержащими ПДн третьих лиц.

На руководителей структурных подразделений Учреждения, допущенных к обработке ПДн третьих лиц, возлагается:

- организация и ведение работы с информацией, содержащей ПДн третьих лиц;
- контроль за выполнением правил обращения с документами, содержащими ПДн третьих лиц;
- контроль за соблюдением установленного порядка копирования документов, содержащих ПДн третьих лиц; их учетом, хранением и использованием;
- ведение журнала учета выдачи, передачи ПДн третьих лиц (форму журнала см. в Приложении № 1 к настоящему Положению);

– обеспечение соблюдения правил рассылки третьей стороне документов, содержащих ПДн третьих лиц.

На администратора информационной безопасности Учреждения возлагается:

– обеспечение функционирования средств защиты информации в составе системы защиты ИСПДн, ГИС;

– выборочный периодический контроль за соблюдением порядка обмена электронными копиями файлов, содержащими ПДн третьих лиц;

На руководителей структурных подразделений возлагается:

– персональная ответственность за организацию работы с информацией, содержащей ПДн третьих лиц, во вверенных структурных подразделениях.

Работники Учреждения, в обязанности которых входит обработка и защита ПДн третьих лиц, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, могут быть привлечены к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации и административно-правовыми нормами, установленными в Учреждении.

8. Взаимодействие с уполномоченными органами в области защиты персональных данных

В соответствии с законодательством Российской Федерации в области обеспечения безопасности ПДн функции контроля и надзора за соответствием порядка обработки ПДн требованиям действующего законодательства возлагаются на федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности, противодействия техническим разведкам и технической защиты информации, контроля и надзора в сфере информационных технологий и связи.

Взаимодействие с уполномоченными органами организуется в пределах их полномочий.

С территориальными органами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) по вопросам:

- предоставления информации, необходимой для реализации полномочий;
- осуществления проверочных и контрольных мероприятий в пределах предоставленных полномочий;
- выполнения требований об уточнении, блокировании, уничтожении недостоверных или полученных незаконным путем ПДн;
- принятия в установленном законодательством Российской Федерации порядке мер по приостановлению или прекращению обработки ПДн.

С территориальными органами ФСТЭК России по вопросам:

- предоставления информации, необходимой для реализации полномочий и осуществления проверочных и контрольных мероприятий;
- организации и проведения мероприятий, направленных на обеспечение безопасности ПДн при их обработке в ИСПДн, ГИС.

С территориальными органами ФСБ России по вопросам:

- предоставления информации, необходимой для реализации полномочий и осуществления проверочных и контрольных мероприятий;
- организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для обеспечения безопасности ПДн при их обработке в ИСПДн, ГИС.

Организация взаимодействия с уполномоченными органами в области обеспечения безопасности ПДн третьих лиц возлагается на отдел (специалиста) информационной безопасности Учреждения.

9. Нормативные документы

Настоящее Положение разработано в соответствии с требованиями следующих документов:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральный закон Российской Федерации от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Указа Президента Российской Федерации от 6 марта 1997 года «Об утверждении перечня сведений конфиденциального характера»;
- Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановление Правительства Российской Федерации от 21 марта 2012 года № 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 и муниципальными органами»;
- приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 18 февраля 2013 года № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ «Об утверждении административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных

технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных». Утвержден приказом Роскомнадзора от 14 ноября 2011 года № 312;

– методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 года «Об утверждении требований и методов по обезличиванию персональных данных»;

– приказ ФСБ России от 09 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 года, ДСП;

– методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 года.

10. Заключительные положения

Настоящее Положение доводится до работников Учреждения, занимающих вакантные должности, в должностные обязанности которых входит обработка ПДн третьих лиц, под роспись при приеме на работу.

11. Приложение № 1

Журнала учета выдачи / передачи персональных данных третьих лиц

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи / отказа в передаче персональных данных	Подпись запрашивающего лица	Подпись ответственного работника

12. Приложение № 2

СОГЛАШЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ № _____

Настоящее Соглашение о Конфиденциальности (в дальнейшем именуемое «Соглашение») заключено «___» _____ 20__ года между:

Учреждением, юридическим лицом, организованным и действующим в соответствии с законодательством Российской Федерации, зарегистрированным по адресу: _____, в лице руководителя Учреждения Фамилия Имя Отчество, действующего на основании _____

И

«_____», юридическим лицом, организованным и действующим в соответствии с законодательством Российской Федерации, зарегистрированным по адресу: г. _____, ул. _____ д. ____, в лице _____ действующего на основании _____.

(если контекстом Соглашения не подразумевается иное, стороны здесь и далее индивидуально именуются «Сторона» и совместно «Стороны»)

ПРИНИМАЯ ВО ВНИМАНИЕ, ЧТО

Стороны в настоящее время имеют намерение вступить в переговоры и провести оценку возможности установления потенциальных взаимоотношений на взаимовыгодной основе с целью выполнения договорных работ (далее «**Взаимоотношения**»).

СТОРОНЫ ДОГОВОРИЛИСЬ О СЛЕДУЮЩЕМ:

1. В рамках настоящего Соглашения принимается следующая терминология:

Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Конфиденциальная информация – документированная информация, составляющая ключевую информацию, конфиденциальную информацию, служебную тайну, ПДн или прочие сведения, доступ к которым ограничивается в соответствии с законодательством Российской Федерации, за исключением информации, составляющей государственную тайну. К конфиденциальной информации нет свободного доступа на законном основании и в отношении нее введен режим ограничения доступа. Конфиденциальная информация имеет гриф ограничения доступа и не включает в себя уже разглашен-

ную информацию или информацию, полученную из сторонних источников или от третьих лиц.

Обладатель конфиденциальной информации – лицо (Сторона), которое владеет конфиденциальной информацией на законном основании, установило в отношении этой информации режим конфиденциальности (ограничения доступа) или коммерческой тайны.

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

Режим ограничения доступа к информации – правовые, организационные, технические и иные принимаемые обладателем конфиденциальной информации меры по охране ее конфиденциальности.

Контрагент – Сторона настоящего соглашения, которой Обладатель конфиденциальной информации передал эту информацию.

Разглашение конфиденциальной информации – действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации.

2. Документированная информация, передаваемая между Сторонами в рамках выполнения договорных обязательств, помеченная грифом «Конфиденциально», «Персональные данные» считается Конфиденциальной информацией.

3. Стороны обязуются обеспечить защиту Конфиденциальной информации, ставшей доступной в рамках выполнения настоящего Соглашения, от несанкционированного использования, распространения или публикации, в соответствии с требованиями нормативно-правовых актов Российской Федерации, а также не разглашать Конфиденциальную информацию какой-либо третьей стороне, как организациям, так и частным лицам, за исключением случаев, определенных законодательством РФ и п. 5 настоящего Соглашения в течение срока действия настоящего Соглашения и в течение 5 (пяти) лет после его окончания.

4. Несанкционированным использованием Конфиденциальной информации считается любое ее использование не в интересах Сторон, определенных действующими договорами Сторон.

5. Стороны обязуются не разглашать Конфиденциальную информацию, ставшую им известной в рамках выполнения договорных обязательств какой-либо третьей стороне, как организациям, так и частным лицам, за исключением случаев, определенных законодательством РФ и п. 6 настоящего Соглашения.

6. Стороны могут передавать полученную по настоящему Соглашению Конфиденциальную информацию третьим лицам, только с письменного разрешения Обладателя (Контрагента) данной информации на следующих условиях:

– третьи лица используют полученную Конфиденциальную информа-

цию только в рамках работ, проводимых на договорной основе между Сторонами;

– Стороны гарантируют соблюдение третьими лицами условий конфиденциальности в соответствии с настоящим Соглашением;

– Обладатель (Контрагент) и привлекаемые к работам третьи лица заключили соглашение о конфиденциальности;

– Стороны несут ответственность за несанкционированное использование, распространение или публикацию третьими лицами Конфиденциальной информации ставшей им известной в рамках выполнения договорных обязательств.

7. Любой ущерб, вызванный нарушением условий конфиденциальности, определяется и возмещается в соответствии с действующим законодательством Российской Федерации и настоящим Соглашением.

8. В случае невозможности разрешения споров и разногласий путем переговоров они подлежат разрешению судом в соответствии с действующим законодательством Российской Федерации в Арбитражном суде Сахалинской области.

9. Настоящее Соглашение вступает в силу с момента его подписания уполномоченными представителями обеих Сторон и будет действовать в течение 5 (пяти) лет после вступления в силу. («Срок действия Соглашения»).

10. Вся Конфиденциальная информация оставшиеся у Сторон после окончания срока действия настоящего Соглашения должна быть возвращена Обладателю (Контрагенту).

11. Положения, изложенные в настоящем Соглашении, должны иметь обязательственную силу для любых дочерних или аффилированных компаний обеих Сторон, а также для их правопреемников.

12. Любые уведомления по данному Соглашению должны быть оформлены Сторонами в письменной форме и будут считаться доставленными надлежащим образом в случае:

– отправки по факсу и/или электронной почте, за подписью уполномоченного представителя отправляющей Стороны с подтверждением о получении;

– отправки с привлечением своих работников, общепризнанной круглосуточной курьерской службы или оплаченным заказным письмом, с запросом подтверждения получения, по адресам, приведенным на титульном листе настоящего Соглашения.

13. Настоящее Соглашение составлено в 2 (двух) идентичных экземплярах имеющих одинаковую силу.

В ПОДТВЕРЖДЕНИЕ ИЗЛОЖЕННОГО

Стороны заключили настоящее Соглашение, подписываемое их уполномоченными представителями:

От Учреждения

От имени _____

Руководитель Учреждения

_____ /Фамилия И.О./
подпись

МП

Должность

_____ /Фамилия И.О./
подпись

МП

13. Приложение № 3

ОБЯЗАТЕЛЬСТВО О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИХ ЛИЦ

Я,

(Фамилия Имя Отчество)

в качестве работника Учреждения в период трудовых отношений с Учреждением (его правопреемником) и в течение пяти лет после их окончания обязуюсь не разглашать сведения, составляющие ПДн третьих лиц (юридических и физических лиц), которые будут мне доверены или станут мне известны по работе.

До моего сведения доведено с разъяснениями действующее Положение о защите персональных данных третьих лиц.

Мне известно, что нарушение данного Положения может повлечь дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

« ____ » _____ 20 ____ г.

(Должность)

(Подпись)

(Фамилия И.О.)