Приложение к Приказу
от 6 марта 2017г. № 4-ИБ/17

Положение
«О порядке обработки персональных данных в ЗАО «Аладдин Р.Д.»

Москва

Содержание

1. Термины, определения и сокращения

1.1. Термины и определения

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

Инструкция - Инструкция «Об обеспечении безопасности персональных данных при их обработке в ЗАО «Аладдин Р.Д.»

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;

Персональные данные - любая информация, относящаяся прямо или косвенно, к определенному или определяемому физическому лицу (субъекту персональных данных)

Показатель эффективности Системы защиты персональных данных - количественная мера оценки качества решения частных задач по защите персональных данных. В качестве частных показателей используются:

- количество предписаний о нарушениях в защите персональных данных, полученных от регуляторов;
- количество претензий от партнеров, связанных с нарушением договорных отношений по защите персональных данных;
- количество мотивированных обращений субъектов персональных данных на обжалование действий и/или бездействия Компании как оператора персональных данных;
- количество положительных решений суда по обращениям субъектов персональных данных;
- количество необработанных инцидентов, выявленных при обработке персональных данных;

Пользователь - работник Компании, осуществляющий трудовую деятельность в соответствии с трудовым договором, или специалист, оказывающий услуги (выполняющий работы) для Компании на основании гражданско-правового договора, или представитель юридического лица, имеющего с Компанией договорные отношения (подрядчики, аудиторы и т.п.), зарегистрированные в информационной среде Компании в установленном порядке и получившие право на доступ к ресурсам информационной среды в соответствии с договором;

Система защиты персональных данных - Совокупность необходимых организационных и технических мер, а также средств защиты информации, используемых для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий;

Уполномоченный обладатель информации – лицо **(**как правило руководитель самостоятельного структурного подразделения), которому обладатель информации делегировал права разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа, передавать информацию другим лицам по договору, а также обязанности при осуществлении им своих прав в соответствии с законодательством РФ и настоящим Положением.

1.2. Сокращения

В настоящем документе используются сокращения, приведенные в таблице 1.

Таблица 1

Сокращение	Определение
ИР	Информационный ресурс
ИС	Информационная система
ИСПДн	Информационная система ПДн
ИТ	Информационные технологии
ИБ	Информационная безопасность
ПДн	Персональные данные
СЗИ	Средства защиты информации
СЗПДн	Система защиты ПДн
ССП	Самостоятельное структурное подразделение
УОИ	Уполномоченный обладатель информации

2. Общие положения

2.1. Область применения и область действия Положения

Настоящее Положение «О порядке обработки персональных данных в ЗАО «Аладдин Р.Д.» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О Персональных данных») и другими федеральными законами и нормативными актами действующего законодательства РФ, а также в соответствии с Уставом ЗАО «Аладдин Р.Д.» (далее - Компания) и внутренними нормативными документами Компании с целью конкретизации мер по защите законных интересов субъектов ПДн, определения принципов защиты ПДн, состава и целей обработки ПДн, назначения системы защиты ПДн и порядка оценки ее эффективности, порядка обработки ПДн, порядка учета работников, допущенных к работе с ПДн, порядка обеспечения конфиденциальности ПДн и обеспечения безопасности при их обработке, организации доступа работников Компании к ПДн, а также обязанностей работников Компании в отношении ПДн и определения порядка взаимодействия структурных подразделений Компании в целях обеспечения указанных требований.

Положение определяет требования к сбору, систематизации, накоплению, хранению, уточнению (обновлению, изменению), использованию, распространению (в том числе передаче), обезличиванию, блокированию, уничтожению ПДн физических лиц, для которых Компания выступает в качестве оператора ПДн только в отношении своих работников, связанных с ней трудовыми отношениями.

Область действия Положения включает:

- все процессы обработки ПДн в Компании без использования средств автоматизации;
- все структурные подразделения Компании;

– все информационные системы Компании, в которых происходит обработка ПДн.

Требования, изложенные в настоящем Положении, являются обязательными для выполнения всеми работниками Компании и иными лицами, имеющими договорные отношения с Компанией, при этом срочность и важность выполняемых ими работ не должны являться основанием для нарушения требований настоящего Положения и других документов, регламентирующих в Компании вопросы обработки и защиты ПДн.

Настоящее Положение доводится до сведения всех работников Компании под роспись в соответствии с перечнем подразделений и работников, допущенных к работе с персональными данными, обрабатываемыми в Компании.

3. Принципы обработки ПДн в СЗПДн

Обработка ПДн в Компании осуществляется на основе принципов, обозначенных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных»:

– обработка ПДн должна осуществляться на законной и справедливой основе;

– обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;

– не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только ПДн, которые отвечают целям их обработки;

– содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки;

– при обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Оператор должен принимать необходимые меры, либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных;

– хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Состав и цели обработки ПДн

Компания осуществляет обработку ПДн в следующих целях:

– содействия в трудоустройстве в Компанию, прохождения работы в Компании, обучения и должностного роста работников, формирования кадрового резерва, учета результатов исполнения работником своих должностных обязанностей, обеспечения работнику установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, информационного обеспечения работы Компании, заключения и исполнения договоров добровольного страхования;

– обеспечения безопасности, связанной с физическим доступом субъектов ПДн на территорию, в здания и помещения Компании;

– статистической обработки информации, при условии обязательного обезличивания ПДн;

В целях информационного обеспечения Компании могут создаваться

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

Сведения о субъекте ПДн должны быть в любое время исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

Порядок обработки информации в системах контроля и управления физическим доступом на территорию (в здания и помещения) Компании, в системах видеонаблюдения и в бюро пропусков, а также порядок обращения с носителями, на которых эта информация размещается, устанавливается соответствующими локальными актами Компании

Состав обрабатываемых в Компании ПДн, а также цели и правовые основания такой обработки определены в законах и иных нормативно-правовых актах, закрепляющих состав и цели обработки, в договорах с субъектом ПДн, а также в других источниках. Состав ПДн должен быть зафиксирован в перечне ПДн, обрабатываемых в Компании.

5. Система защиты ПДн

С целью обеспечения защиты законных интересов субъектов ПДн в Компании разработана, внедрена и поддерживается в работоспособном состоянии система защиты ПДн, которая является частью информационной системы Компании.

В качестве субъектов ПДн, персональные данные которых могут обрабатываться и соответственно защищаться в Компании без использования средств автоматизации, понимаются нижеперечисленные категории физических лиц, условно именуемые далее:

1. **работниками**, в состав которых включаются:

- персонал Компании (работники, имеющие трудовые отношения с Компанией), кандидаты на работу в Компании и лица, имевшие ранее трудовые отношения с Компанией;

- лица, имеющие гражданско-правовой характер договорных отношений с Компанией или находящиеся на этапе преддоговорных отношений подобного характера;

- лица, проходящие различного рода практику (стажировку) в Компании.

2. **посетителями**, в состав которых включаются:

- представители (должностные лица) государственных органов законодательной, исполнительной и судебной власти и управления;

- представители общественных организаций, коммерческих и некоммерческих структур и иных объединений (в т.ч. иностранных).

В Компании в соответствии с ФЗ «О персональных данных» выделяются следующие категории ПДн:

– персональные данные **иные** или **общей** категории, которые не могут быть отнесены к специальным категориям ПДн, к биометрическим ПДн, к общедоступным или обезличенным ПДн;
– обезличенные и/или **общедоступные** ПДн.

Вышеуказанные категории ПДн классифицированы Компанией с учетом степени тяжести последствий потери свойств безопасности ПДн для субъекта ПДн

5.1. Назначение ответственных лиц в сфере организации обработки и защиты ПДН

В целях разграничения обязанностей и функций работников в области обработки и обеспечения безопасности ПДн в Компании вводятся следующие роли:

- менеджер по организации обработки ПДн
- менеджер по защите ПДн;
- администратор систем обработки ПДн;
- руководитель ССП;
- менеджер по правовому сопровождению процессов обработки ПДн;
- пользователь ПДн.

Возложение обязанностей по осуществлению функций указанных ролей утверждается приказом Руководителя Компании.

Описание указанных ролей приведено в таблице 2.

Обязанности, соответствующие определенной роли приведены в таблице 3.

Таблица 2

Роль	Описание
Менеджер по организации обработки ПДн	На данную роль возлагаются задачи по организации выполнения законодательных требований при обработке ПДн в целом в Компании (обработка с использованием средств автоматизации и без них)
Менеджер по защите ПДн	Пользователь - основной операционный исполнитель процессов ИБ, который непосредственно выполняет все основные мероприятия по ИБ, уполномочен обладателем информации принимать решения по обеспечению защиты ПДн в Компании (обработка с использованием средств автоматизации и без них) на основании предложений УОИ - руководителей подразделений, непосредственно обрабатывающих ПДн, а также осуществлять контроль за выполнением мер по защите ПДн и администрирование инцидентов, связанных с нарушением безопасности ПДн.
Администратор систем обработки ПДн	Представитель подразделения, ответственного за обеспечение функционирования ИСПДн Компании, осуществляющий техническую поддержку работы ИСПДн Компании (установка, настройка, обновление и удаление ПО в ИСПДн и на рабочих местах Пользователей ИСПДн в соответствии с внутренними нормативными документами).
Руководитель ССП	Пользователь, являющийся УОИ, содержащей персональные данные. Данную роль выполняют все руководители подразделений, в которых происходит обработка ПДн
Менеджер по правовому сопровождению процессов обработки ПДн	Пользователь, который уполномочен осуществлять правовую поддержку решений по защите ПДн и правовому сопровождению деятельности Компании в области защиты ПДн. Данную роль выполняет основной операционный

Роль	Описание
	руководитель процессов правового сопровождения деятельности Компании.
Пользователь ПДн	Все пользователи, которым предоставлен доступ к информации, содержащей ПДн.

Таблица 3

Роль	Обязанности
Менеджер по организации обработки ПДн	– осуществлять внутренний контроль за соблюдением Компанией, как оператором ПДн, и его работниками законодательства РФ о ПДн, в том числе требований к защите ПДн; – доводить до сведения работников Компании положения законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн; – организовывать прием и обработку обращений и запросов субъектов ПДн или их Представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов; – взаимодействует с менеджером по защите ПДн по вопросам организации и совершенствования защиты процедур обработки ПДн в соответствии с требованиями ФЗ «О персональных данных» и принятым в соответствии с ним нормативно-правовым актам;
Менеджер по защите ПДн	– организовывать разработку и поддержание в актуальном состоянии организационно-распорядительных документов, определяющих требования и порядок обработки и обеспечения безопасности ПДн в Компании; – организовывать контроль за состоянием системы защиты ПДн Компании и за соблюдением работниками установленных норм и требований по обеспечению безопасности ПДн; – взаимодействовать с регулирующими органами по вопросам защиты ПДн при проведении ими плановых и внеплановых проверок; – формировать предложения для руководства Компании по совершенствованию СЗПДн; – утверждать планы проведения контрольных проверок пользователей ПДн на предмет выполнения требований Положения; – согласовывать права доступа работников к ПДн и средствам их обработки в порядке, установленном внутренними нормативными документами; – согласовывать решения о привлечении сторонних организаций (подрядчиков) для обслуживания, настройки и ремонта СЗИ, входящих в состав СЗПДн; – информировать руководство Компании о состоянии СЗПДн, о планируемых мероприятиях, нацеленных на обеспечение безопасности ПДн, а также о результатах проведенных мероприятий; – организовывать расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением

Роль	Обязанности
	безопасности ПДн; – осуществлять контроль эффективности принимаемых мер по выявлению и закрытию возможных каналов неправомерного распространения ПДн; – участвовать в разработке проектов основных направлений работ по обеспечению комплексной безопасности ПДн, целевых программ и соответствующих разделов планов работ в этой области, а также в составлении бюджетных планов на проведение необходимых мероприятий по обеспечению безопасности ПДн.
Администратор систем обработки ПДн	– обеспечивать непрерывное функционирование ИСПДн в целом и ее программных и технических компонентов в отдельности; – предоставлять экспертные консультации и рекомендации по вопросам надежной работы СВТ, участвующих в обработке ПДн в Компании; – хранить эталонные версии ПО; – выполнять процедуры контроля, обслуживания, настройки и ремонта средств обработки ПДн, входящих в состав ИСПДн; – сопровождать и контролировать сторонние организации (подрядчиков) в случае привлечения их для обслуживания, настройки и ремонта средств обработки ПДн, входящих в состав ИСПДн; – устанавливать параметры конфигурации компонентов ИСПДн (параметры конфигурации рабочих мест обработки ПДн, параметры конфигурации средств обработки ПДн); – контролировать настройку параметров конфигурации систем обработки ПДн, средств обработки, входящих в состав ИСПДн; – согласовывать требования по защите ПДн к проектируемым и внедряемым информационным системам Компании; – контролировать права доступа пользователей ПДн к ПДн и средствам их обработки в Компании; – предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении контрольных мероприятий по обеспечению безопасности ПДн
Руководитель ССП	– назначать (при необходимости) из числа имеющихся работников, ответственных за обеспечение безопасности ПДн (в рамках реализуемых бизнес-процессов); – обеспечивать выполнение требований по обработке и соблюдению безопасности ПДн в соответствии с Положением и иными нормативными документами в области обработки и защиты ПДн; – осуществлять контроль за действиями подчиненных при обработке ПДн; – проводить инструктаж подчиненных, разъяснять подчиненным положения нормативных документов в области обработки и защиты ПДн и требовать их выполнение; – участвовать в процессе разработки и согласования организационно-распорядительных документов по СЗПДн Компании; – направлять на обучение работников, назначенных на роли, определенные в соответствии с настоящим документом;

Роль	Обязанности
	– предоставлять консультации пользователям ПДн по вопросам автоматизированной или неавтоматизированной обработки ПДн в рамках своих компетенций; – определять для подчиненных работников права доступа к ПДн и средствам обработки ПДн в рамках своих компетенций; – предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении контрольных мероприятий по обеспечению безопасности ПДн; – сообщать о выявленных нарушениях требований Положения Менеджеру по защите ПДн
Менеджер по правовому сопровождению процессов обработки ПДн	– отслеживать изменения в нормативных актах РФ, касающихся обработки и обеспечения безопасности ПДн; – формировать предложения о необходимости проведения контрольных мероприятий по обеспечению безопасности ПДн для Менеджера по защите ПДн; – формировать предложения по внесению изменений в организационно-распорядительные документы по СЗПДн; – контролировать договоры с третьими лицами на предмет их соответствия требованиям организационно-распорядительных документов Компании по обработке и обеспечению безопасности ПДн; – принимать запросы от субъектов ПДн, осуществлять первичное рассмотрение и распределение запросов между владельцами бизнес-процессов обработки ПДн; – осуществлять взаимодействие с органами власти и регулирующими органами по вопросам обработки и обеспечения безопасности ПДн.
Пользователь ПДн	– соблюдать требования организационно-распорядительных документов по обработке ПДн Компании; – проходить обучение и инструктажи по вопросам обработки и обеспечения безопасности ПДн; – предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении внутренних контрольных мероприятий по защите ПДн; – сообщать о выявленных нарушениях требований Положения своему непосредственному руководителю и Менеджеру по защите ПДн.

В Компании распорядительным порядком (приказом) назначается лицо, ответственное за организацию обработки ПДн с ролью - Менеджер по организации обработки ПДн (далее – Менеджер ПДн), как в информационных системах Компании, в которых обрабатываются ПДн, так и при обработке без использования средств автоматизации.

Менеджер ПДн получает указания непосредственно от единоличного исполнительного органа Компании – Генерального директора (далее - Руководитель) и подотчетен ему.

В соответствии с требованиями ФЗ «О персональных данных» (ч. 4 ст. 22.1) Менеджер ПДн, в частности выполняет обязанности, соответственно своей роли, отраженные в таблице 3.

На Менеджера ПДн возлагается задача по организации выполнения законодательных требований при обработке ПДн в Компании, для осуществления которой:

– назначается распорядительным порядком (приказом) постоянно действующая рабочая группа (далее – Рабочая группа), подчиненная Менеджеру ПДн;
– в состав Рабочей группы включаются представители подразделений Компании роли и обязанности которых в системе обработки ПДн отражены в таблицах 2 и 3 – это Менеджер по защите ПДн; Администратор систем обработки ПДн; Менеджер по правовому сопровождению процессов обработки ПДн
– представители подразделений, входящие в состав Рабочей группы, кроме выполнения текущих поручений Менеджера ПДн, должны осуществлять постоянный контроль по закрепленным за ними направлениями деятельности, за выполнением требований настоящего Положения и других локальных актов Компании по вопросам обработки и защиты ПДн;
– члены Рабочей группы обязаны докладывать через своих непосредственных руководителей Менеджеру ПДн о возникающих вопросах и о случаях, приведших к нарушениям законодательных требований при обработке ПДн в Компании или предпосылках к таким случаям, а также подавать предложения по совершенствованию процедур обработки ПДн в Компании с целью недопущения нарушений законодательных требований и требований локальных актов Компании по вопросам обработки и защиты ПДн.

Ответственными за организацию и выполнение требований локальных актов Компании по вопросам обработки ПДн и их защите в ССП Компании являются руководители этих подразделений (роль – Руководитель ССП таблица 2 и 3). На время отсутствия этих руководителей ответственными являются лица, штатно замещающие их.

Ответственными за выполнение требований локальных актов Компании по вопросам обработки ПДн и их защите на своих рабочих местах в рамках, определенных соответствующими должностными инструкциями являются лица, уполномоченные в установленном порядке обрабатывать в Компании ПДн (роль- Пользователь ПДн таблица 2 и 3).

В должностной инструкции работников, относящихся к руководящему составу, в разделе «Должностные обязанности» должны быть предусмотрены следующие обязанности:

– «Осуществляет в соответствии с требованиями законодательства РФ, Положения «О порядке обработки персональных данных в ЗАО «Аладдин Р.Д.»), обработку ПДн подчиненных работников и посетителей Компании с использованием и без использования средств автоматизации с обязательным применением регламентированных соответствующими локальными актами Компании мер по обеспечению безопасности обрабатываемых ПДн.
– Определяет функциональные обязанности всем подчиненным работникам с учетом соблюдения мер по обеспечению информационной безопасности в соответствии с требованиями локальных актов Компании, эксплуатационной документацией технических средств и систем при работе подчиненных работников в качестве пользователей (операторов) этих средств и систем.
– Планирует и проводит конкретные мероприятия по вопросам обеспечения информационной безопасности, предписанные соответствующими техническими и

распорядительными документами Компании, в том числе определяет порядок действия подчиненных работников по экстренной защите информации при стихийных бедствиях и других нештатных ситуациях.

– Обеспечивает соблюдение подчиненными работниками правил применения штатных средств и систем защиты информации и выполнение установленных правил обращения с машинными носителями информации.

– Организует подготовку и проведение инструктажей подчиненных работников по вопросам обеспечения безопасности информации ограниченного доступа, в том числе ПДн».

Должности работников, непосредственно осуществляющих обработку ПДн в Компании, либо имеющих доступ к ПДн, указываются в утверждаемом в распорядительном порядке «Перечне ролей и должностей работников «ЗАО «Аладдин Р.Д.», введенных в целях разграничения обязанностей и функций в области обработки и обеспечения безопасности персональных данных».

Перечни должностей работников формируются с учетом ролей, исполняемых в соответствующих ИС Компании работниками, назначенными в установленном порядке на должности, указанные в перечнях.

Учитывая, что права по доступу к информационным активам (ресурсам) ИСПДн Компании предоставляются пользователям только в распорядительном порядке, то при необходимости, привязка указанных в Перечнях должностей работников к конкретным работникам, возможна через текущие (действующие) учетные записи этих работников в ИСПДн и соответствующие Перечни ролей.

5.2. Требования к документации по СЗПДн

С целью нормативного обеспечения СЗПДн в Компании разрабатывается, внедряется и поддерживается в актуальном состоянии документация по СЗПДн, которая включает:

– частные политики ИБ Компании, утвержденные в соответствии с установленным в Компании порядком;

– настоящее Положение,

– ПДн, обрабатываемые в Компании (допускается ведение в электронном виде);

– перечень подразделений и работников, допущенных к работе с ПДн, обрабатываемыми в Компании (допускается ведение в электронном виде);

– модель угроз безопасности ПДн при их обработке в ИСПДн Компании;

– техническую документацию на СЗПДн.

Формы всех документов, касающихся взаимодействия Компании с субъектами ПДн, при обработке их ПДн в ИС Компании, включены в Инструкцию в виде приложений к Инструкции.

Согласование документов по СЗПДн с заинтересованными подразделениями, их пересмотр, актуализация, внесение изменений и утверждение производятся в порядке, предусмотренном внутренними нормативными документами.

Ответственность за организацию работ по актуализации документов СЗПДн и ее результативность несет менеджер по защите ПДн.

Каждый из документов СЗПДн в случае необходимости может быть пересмотрен в случаях:

– изменения федерального законодательства;

– изменения бизнес-процессов в Компании (в том числе изменения организационно-штатной структуры Компании).

Внесение изменений и пересмотр документов по СЗПДн осуществляются по мере необходимости в соответствии с Инструкцией. Решение о внесении изменений о пересмотре документов по СЗПДн принимает менеджер по защите ПДн.

Актуальные версии документов СЗПДн размещаются на портале Компании в разделе «Информационная безопасность». Ответственность за актуальность размещенных документов СЗПДн возлагается на менеджера по защите ПДн.

Переписка с внешними организациями, касающаяся вопросов СЗПДн, ведется через подразделение, в функции которого входят организация и обеспечение делопроизводства. Переписка ведется в соответствии с правилами, установленными в Инструкции.

5.3. Оценка эффективности СЗПДн

Оценка эффективности СЗПДн осуществляется в соответствии с показателями эффективности СЗПДн, приведенными в таблице 4.

Таблица 4

Показатель эффективности СЗПДн	**Допустимое значение показателя эффективности СЗПДн**
Количество предписаний о нарушениях в защите ПДн, полученных от регуляторов	0
Доля партнеров, обратившихся с претензиями, связанными с нарушением договорных отношений по защите ПДн	0,01% от общего числа партнеров - 0
Количество мотивированных обращений субъектов ПДн на обжалование действий и/или бездействия Компании как оператора ПДн	0
Количество решений суда, вынесенных в пользу субъектов ПДн по искам, связанным с нарушением прав субъектов ПДн	0
Количество необработанных инцидентов, выявленных при обработке ПДн	0
Рост собственных трудозатрат владельца бизнес-процесса, связанных с СЗПДн	Не более 1% общих трудозатрат процесса

Функционирование СЗПДн считается эффективным, если в течение календарного года не превышены допустимые значения показателей эффективности СЗПДн.

6. Специальные категории ПДн

Правила обработки специальных категорий ПДн в Компании приведены в таблице 5.

Таблица 5

Категория ПДн	**Правила обработки**
Данные, касающиеся расовой принадлежности	Не обрабатываются

Категория ПДн	Правила обработки
Данные, касающиеся национальной принадлежности	Не обрабатываются
Данные, касающиеся политических взглядов	Не обрабатываются
Данные, касающиеся религиозных или философских убеждений	Не обрабатываются
Данные, касающиеся интимной жизни	Не обрабатываются
Данные, касающиеся состояния здоровья	В Компании допускается обработка ПДн, касающихся состояния здоровья. Такими ПДн в Компании признается набор сведений, описанных в определенной форме на бумажном или электронном носителе, а также подтвержденных печатью и подписью (или электронной подписью) ответственного лица, уполномоченного определять отсутствие или нарушение качественных параметров, являющихся сведениями о здоровье субъекта ПДн. Параметры, являющиеся сведениями о здоровье субъекта ПДн, могут быть описаны в ряде документов, принадлежащих субъекту ПДн, а именно в: 1) медицинской карте субъекта ПДн; 2) эпикризе или истории болезни; 3) протоколе с места происшествия, вследствие которого наступила смерть субъекта ПДн; 4) иных документах, содержащих обоснование диагноза, проведенного лечения, медицинский прогноз и лечебно-профилактические рекомендации. В Компании допускается обработка ПДн, касающихся состояния здоровья, только в следующих случаях: – обработка необходима для ведения судебно-претензионной работы с субъектом ПДн; – обработка необходима для урегулирования просроченной задолженности субъекта ПДн перед Компанией; – обработка необходима для оформления социальных компенсаций для работников за счет средств социального фонда; – обработка производится в рамках участия в благотворительной деятельности. Компания прекращает обработку ПДн о здоровье, если устранены причины, вследствие которых они обрабатывались, за исключением случаев, когда федеральным законом установлено иное.
Сведения о судимости	В Компании допускается обработка данных о судимости в трактовке их состава и содержания в рамках приказа МВД РФ от 01 ноября 2001 г. № 965 «Об утверждении Инструкции о порядке предоставления гражданам справок о наличии

Категория ПДн	Правила обработки
	(отсутствии) у них судимости»

7. Биометрические персональные данные

В Компании не ведется обработка биометрических ПДн.

8. Трансграничная передача ПДн

Трансграничная передача ПДн в Компании не производится, но (при необходимости) в рамках выполнения процессов кадрового администрирования в части иностранных работников в Компании может быть реализованы процедуры трансграничной передачи ПДн.

До начала осуществления трансграничной передачи ПДн Компания обязана убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн. При передаче ПДн на территорию государств, подписавших Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке ПДн, получения письменного согласия не требуется.

Трансграничная передача ПДн работников может осуществляться Компанией с согласия субъекта ПДн и с учетом требований статьи 12 ФЗ «О персональных данных».

Перед трансграничной передачей ПДн исполнитель обязан согласовать условия такой передачи с лицом, ответственным за обработку ПДн в Компании.

9. Общедоступные персональные данные

Компания может осуществлять обработку общедоступных ПДн в соответствии с полученным от субъекта согласием. Форма согласия о признании ПДн общедоступными приведена в приложении к Инструкции.

10. Порядок получения доступа к ПДн и учета работников, допущенных к работе с ПДн

Работники, уполномоченные обрабатывать в Компании персональные данные, без использования средств автоматизации, подразделяются на следующие группы:

- обрабатывающие персональные данные только работников;
- обрабатывающие персональные данные только посетителей;

Работники, непосредственно осуществляющие обработку ПДн, должны быть ознакомлены с положениями законодательства РФ о ПДн, в том числе с требованиями к защите ПДн, внутренними нормативно-правовыми документами, определяющими политику в отношении обработки ПДн.

Список работников, имеющих право доступа к работе с персональными данными, должен быть определен в «Перечне ролей и должностей работников «ЗАО «Аладдин Р.Д.», введенных в целях разграничения обязанностей и функций в области обработки и обеспечения безопасности персональных данных

Список работников, имеющих право доступа к работе с ПДн, ведется руководителем ССП - уполномоченным обладателем информации (ПДн).

Допускается ведение данного списка в электронном виде.

Сотрудник Компании допускается к обработке ПДн после ознакомления с настоящим Положением и внутренними нормативными документами, определяющими порядок обработки ПДн.

11. Общий порядок обработки ПДн

11.1. Получение согласия субъекта ПДн

В соответствии с ФЗ «О персональных данных» (ч.1 ст. 9) субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн (далее – Согласие) должно быть конкретным, информированным и сознательным.

Согласие может быть дано субъектом ПДн или его Представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения Согласия от Представителя субъекта ПДн полномочия данного Представителя на дачу Согласия от имени субъекта ПДн проверяются Компанией.

В случаях, предусмотренных действующим законодательством Российской Федерации, 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 действующим законодательством Российской Федерации электронной подписью.

Обработка ПДн допускается в следующих случаях:

- обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;
- обработка ПДн необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на Компанию, как на оператора функций, полномочий и обязанностей;
- обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве;
- обработка ПДн необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта ПДн на едином портале государственных и муниципальных услуг;
- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- обработка ПДн необходима для осуществления прав и законных интересов Компании как оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации, при условии обязательного обезличивания ПДн;

– осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн, либо по его просьбе;

– осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с Федеральным законом.

11.2. Систематизация ПДн

Систематизация ПДн подразумевает под собой инвентаризацию ПДн, в которой определены категория ПДн, состав ПДн, место хранения ПДн и порядок доступа к ПДн в Компании.

11.3. Накопление ПДн

В процессе деятельности Компании происходит накопление ПДн в результате:

- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажные носители и в базы данных автоматизированных систем);
- получения оригиналов документов (трудовая книжка и т.п.).

11.4. Хранение ПДн

Хранение ПДн в Компании осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, за исключением случаев, когда срок хранения установлен Федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.

Компания осуществляет хранение ПДн на машинных и бумажных носителях – при неавтоматизированной обработке ПДн.

Сроки хранения ПДн в Компании должны быть определены в «Перечне информации конфиденциального характера, подлежащей защите в ЗАО «Аладдин Р.Д.»

11.5. Уничтожение ПДн

По достижении целей обработки ПДн или в случае утраты необходимости в достижении этих целей (за исключением случаев, когда федеральным законодательством установлено иное) ПДн уничтожаются или обезличиваются (при необходимости).

Уничтожение ПДн производится в соответствии с требованиями внутренних нормативных документов Компании, описанным в Инструкции.

11.6. Уточнение ПДн

Уточнение (изменение, обновление, блокирование) происходит при выявлении фактов неполноты, неточности или неактуальности обрабатываемых сведений, а также при выявлении неправомерных действий в отношении субъекта ПДн по требованию:

- субъекта ПДн или его законного представителя;
- уполномоченного органа по защите прав субъектов ПДн.

11.7. Предоставление ПДн

Под предоставлением ПДн понимаются действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

11.8. Распространение ПДн

Под распространением ПДн понимаются действия, направленные на раскрытие ПДн неопределенному кругу лиц.

В Компании не производится распространение ПДн, за исключением ПДн, ставших общедоступными благодаря действиям субъекта ПДн, подлежащих обязательному раскрытию в соответствии с федеральным законом, а также случаев добровольного распространения ПДн с согласия субъектов.

11.9. Обезличивание ПДн

Обезличивание ПДн должно производиться способом, исключающим возможность идентифицировать субъекта ПДн по остаточным данным без использования дополнительной информации после проведения соответствующих процедур.

11.10. Взаимодействие с третьими лицами при обработке ПДн

Компания уведомляет субъекта ПДн в случае получения ПДн от третьей стороны, за исключением случаев, предусмотренных в п. 4 ст. 18 ФЗ «О персональных данных». В Компании имеются случаи получения ПДн от третьей стороны, приведенные в таблице 6.

Таблица 6

Бизнес-процесс	**Категория субъектов, чьи ПДн получены от третьей стороны**	**От кого получены ПДн**	**Правила обработки**
Оформление полисов ДМС для родственников работников Компании (по их желанию)	Родственники работников Компании	Работники Компании	Необходимо уведомление, форма которого приведена в Приложении к Инструкции «Об обеспечении безопасности ПДн при их обработке в ЗАО «Аладдин Р.Д.»

В случае если Компания поручает обработку ПДн третьему лицу, в договор включается условие, которое возлагает на указанное лицо обязанность обеспечивать режим конфиденциальности ПДн и безопасность ПДн при их обработке. Компания может при необходимости определять условия и порядок подтверждения третьим лицом соблюдения конфиденциальности и обеспечения безопасности ПДн при их обработке (в т.ч. проверку, мероприятия в рамках аккредитации и другой порядок, если необходимо).

Договор Компании с третьим лицом также включает следующую информацию:

- перечень действий (операций) с ПДн, которые будут совершаться третьим лицом;
- цели обработки ПДн;
- требования к защите обрабатываемых ПДн.

Форма документа находится в Инструкции (в Приложении).

12. Порядок обеспечения безопасности ПДн при их обработке

Обеспечение безопасности ПДн при их обработке осуществляется на всех этапах жизненного цикла ИСПДн Компании путем:

- формулирования требований по защите ПДн к проектируемой и внедряемой информационной системе и согласования их Заказчиком проекта внедрения такой системы;

– согласования технического задания на внедрение ИСПДн подразделением, ответственным за обеспечение ИБ в Компании;

– включения в методику тестирования операций по проверке требований по защите ПДн, сформулированных в техническом задании;

– ведения протоколов тестирования, используемых в качестве свидетельств степени соответствия внедряемой ИСПДн требованиям по защите ПДн;

– назначения администратора информационной безопасности ПДн для каждой ИСПДн, находящейся в эксплуатации;

– актуализации описания бизнес-процессов, достаточных для определения механизмов обработки ПДн (регламент, техническое описание и т.д.) и соблюдения процедуры согласования вносимых изменений с уполномоченным обладателем информации (ПДн);

– доведения до ответственных исполнителей под подпись актуальных версий описаний бизнес-процессов;

– проведения самооценки обеспечения безопасности ПДн в процессе их обработки в соответствии с внутренним нормативным документом Компании.

13. Ответственность

Работники, выполняющие роли, введенные настоящим Положением, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей в пределах, определенных действующим законодательством Российской Федерации.

Руководитель Компании вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

14. Заключительные положения

При работе с ПДн во всех случаях, не урегулированных внутренними нормативными документами Компании, необходимо руководствоваться действующим законодательством РФ.