ИНДИВИДУАЛЬНЫЙ ПРЕДПРИНИМАТЕЛЬ
БАКИНОВСКАЯ ЮЛИЯ МИХАЙЛОВНА

УТВЕРЖДАЮ

__/Бакиновская Ю.М./
«03» сентября 2024 года

ПОЛОЖЕНИЕ О ПОРЯДКЕ ПОЛУЧЕНИЯ, УЧЕТА, ОБРАБОТКИ, ХРАНЕНИЯ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ст-ца Полтавская,

2024 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о порядке получения, учета, обработки, хранения и защиты персональных данных (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности персональных данных (далее – ПДн), при их обработке в информационных системах ПДн (далее – ИСПДн).

1.2. В настоящем Положении используются следующие термины:

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

1.1) *персональные данные, разрешенные субъектом персональных данных для распространения*, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных»;

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

3) *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;

4) *автоматизированная обработка персональных данных* – обработка персональных данных с помощью средств вычислительной техники;

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

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

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

8) *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;

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

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

11) *трансграничная передача персональных данных* – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3. Настоящее Положение определяет порядок и условия обработки ПДн у Индивидуального предпринимателя Бакиновской Юлии Михайловны (далее по тексту – Оператор, ИП), включая порядок передачи ПДн третьим лицам, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн и иные вопросы.

1.4. Действие настоящего Положения распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению, использованию, передачу (в том числе распространению, предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.5. Настоящее Положение вступает в силу с момента его утверждения Оператором и действует бессрочно, до замены его новым Положением.

1.6. Все изменения в Положение вносятся приказом.

1.7. Все сотрудники Оператора должны быть ознакомлены с настоящим Положением под подпись.

2. ЦЕЛИ И ЗАДАЧИ ОБРАБОТКИ ПДН

2.1. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями их сбора.

2.2. Не допускается объединение баз данных содержащих ПДн обработка которых осуществляется в целях несовместимых между собой.

2.3. Содержание и объем, обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

2.4. Обработка ПДн сотрудников Оператора может осуществляться в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Оператора.

2.5. Основными целями обработки ПДн являются:

2.5.1. Обеспечение соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов ИП.

2.5.2. Осуществление функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на ИП, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы.

2.5.3. Регулирование трудовых отношений с сотрудниками ИП (содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества, формирование и хранение документации по личному составу сотрудников Оператора, автоматизированное ведение их учета).

2.5.4. Предоставление сотрудникам ИП и членам их семей дополнительных гарантий и компенсаций или иных видов социального обеспечения.

2.5.5. Подготовка, заключение, исполнение и прекращение договоров с контрагентами ИП.

2.5.6. Формирование и ведение справочников для информационного обеспечения деятельности ИП.

2.5.7. Исполнение судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.

2.5.8. Осуществление прав и законных интересов ИП в рамках осуществления видов деятельности, предусмотренных Уставом.

2.5.9. Организация делопроизводства по вопросам обращения граждан.

2.5.10. Предоставление доступа к сервисам, информации и/или материалам, владельцем которых является ИП, для оказания услуг.

2.5.11. В иных законных целях.

2.6. ИСПДн обеспечивает решение следующих задач:

2.6.1. Защита персональных данных.

2.6.2. Контроль использования персональных данных.

2.6.3. Упрощение процедуры обработки персональных данных, сокращение времени на их обработку.

2.6.4. Обеспечение возможности обмена персональными данными с использованием информационных систем связи.

3. ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ У ИП

3.1. У ИП обрабатываются ПДн следующих категорий субъектов:

3.1.1. Сотрудники Оператора.

3.1.2. Физические лица, получатели услуг ИП, законные представители получателей услуг ИП, ПДн которых обрабатываются Оператором.

3.1.3. Сотрудники контрагентов Оператора.

3.2. Данный перечень может пересматриваться по мере необходимости.

3.3. Полные списки обрабатываемых ПДн формируются в перечне ПДн обрабатываемых в ИСПДн, утверждаемым у Оператора.

4. ДОСТУП К ПДН

4.1. Сотрудники Оператора, которые в силу выполняемых служебных обязанностей работают с ПДн, получают допуск к необходимым категориям ПДн на срок выполнения ими соответствующих должностных обязанностей, на основании перечня должностей ИП, допущенных к работе с ПДн.

4.2. Оператором установлен разрешительный порядок доступа к ПДн. Сотрудникам Оператора, на основании решения ИП, предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

4.3. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником по согласованию с ИП.

4.4. Доступ к ПДн третьих лиц, не являющихся сотрудниками Оператора без согласия субъекта ПДн, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с ведома руководителя Оператора.

4.5. В случае если сотруднику сторонней организации необходим доступ к ПДн Оператора, то необходимо, в договоре с контрагентом зафиксировать условия конфиденциальности ПДн и обязанность по соблюдению требований действующего законодательства в области защиты ПДн. Кроме того, в случае доступа к ПДн лиц, не являющихся сотрудниками Оператора, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Оператором с субъектом ПД.

4.6. Доступ сотрудника Оператора к ПДн прекращается с даты, прекращения трудовых отношений, либо даты изменения должностных обязанностей сотрудника и/или исключения сотрудника из списка лиц, имеющих право доступа к ПДн. В случае увольнения все носители, содержащие ПДн, которые в соответствии с должностными обязанностями

находились в распоряжении сотрудника во время работы, должны быть переданы должностному лицу ответственному за защиту ПДн у ИП.

5. ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ПДН

5.1. При обработке ПДн должно быть обеспечено:

5.1.1. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и/или передачу их лицам, не имеющим права доступа к такой информации.

5.1.2. Формирование и проведение единой политики в области обеспечения информационной безопасности.

5.1.3. Своевременное обнаружение фактов несанкционированного доступа к ПДн.

5.1.4. Недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование.

5.1.5. Возможность восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.1.6. Постоянный контроль над обеспечением соответствующего уровня защищенности ПДн.

5.2. Оператор обязан принимать необходимые правовые, организационные, технические и другие меры для обеспечения безопасности ПДн.

5.3. Оператором используются технические средства и программное обеспечение для обработки и защиты ПДн. Также ведется журнал учета средств защиты ПДн.

5.4. Оператором ведется журнал учета и хранения съемных носителей информации.

5.5. Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн и средств защиты информации, должны быть под подпись ознакомлены с требованиями настоящего Положения.

5.6. Сотрудники обязаны незамедлительно сообщать соответствующему должностному лицу Оператора об утрате или недостаче носителей информации, составляющей ПДн, а также о причинах и условиях возможной утечки ПДн. В случае попытки посторонних лиц получить доступ к ПДн, обрабатываемым Оператором, сотрудник должен незамедлительно известить об этом соответствующее должностное лицо, ответственное за информационную безопасность у ИП.

6. СОГЛАСИЕ НА ОБРАБОТКУ ПДН

6.1. Перед началом любого рода обработки ПДн субъекта, необходимо получение согласия на обработку его ПДн, если иное не предусмотрено законодательством Российской Федерации.

6.2. Субъект ПДн принимает решение о предоставлении своих ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и

сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством Российской Федерации. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Оператором.

6.3. Получение письменного согласия на обработку ПДн осуществляется сотрудником Оператора, при получении ПДн от субъекта ПДн, путем оформления письменного согласия по форме, установленной у Оператора ИСПДн. Получение письменного согласия на обработку ПДн может осуществляется сотрудником контрагента Оператора, путем оформления письменного согласия по форме, установленной у Оператора ИСПДн, в рамках договорных отношений, заключённых с контрагентом.

7. ПРАВА СУБЪЕКТА В ОТНОШЕНИИ ПДН, ОБРАБАТЫВАЕМЫХ ОПЕРАТОРОМ

7.1. На получение информации от Оператора, касающейся обработки его ПДн. Сведения должны быть предоставлены субъекту ПДн Оператором в доступной форме и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Перечень сведений и порядок их получения предусмотрен действующим законодательством Российской Федерации.

7.2. Требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством Российской Федерации меры по защите своих прав (ч. 1 ст. 14 закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

7.3. На условие письменного согласия при принятии на основании исключительно автоматизированной обработки ПДн решений Оператора, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы (ч.2. ст.16 закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

7.4. Заявлять возражения на решения Оператора на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения (ч.3 ст.16 закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

7.5. Обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке (ст. 17 закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

8. ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА ИСПДН

8.1. Оператор ИСПДн вправе:

8.1.1. Поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта (ч.3 ст.6 закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

8.1.2. В случае отзыва субъектом ПДн согласия на обработку его ПДн, продолжить обработку этих ПДн без согласия субъекта при наличии оснований, указанных в законодательстве Российской Федерации (ч.2 ст.9 закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

8.1.3. Отказать субъекту ПДн в выполнении повторного запроса сведений, не соответствующего условиям, предусмотренным законодательством Российской Федерации. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе (ч.6 ст.14 закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

8.1.4. Самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора ИСПДн, предусмотренных законодательством Российской Федерации (ч.1 ст.18.1 закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

8.2. Оператор ИСПДн обязан.

8.2.1. Принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей Оператора ИСПДн, предусмотренных законодательством Российской Федерации.

8.2.2. Назначить лицо, ответственное за обработку ПДн.

8.2.3. Назначить лицо, ответственное за защиту ПДн.

8.2.4. До начала обработки ПДн обязан уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных законодательством Российской Федерации.

8.2.5. При получении доступа к ПДн не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

8.2.6. Представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия законных оснований, обработки ПДн без согласия субъекта ПДн.

8.2.7. До начала осуществления трансграничной передачи ПДн убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн.

8.2.8. При сборе ПДн, предоставить субъекту ПДн по его просьбе информацию, предусмотренную законодательством Российской Федерации.

8.2.9. Если ПДн получены не от субъекта ПДн, Оператор, за исключением случаев, предусмотренных законодательством Российской Федерации, до начала обработки таких ПДн предоставить субъекту ПДн следующую информацию:

- наименование и адрес Оператора или его представителя;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные настоящим Федеральным законом права субъекта ПДн;
- источник получения ПДн.

8.2.10. Опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн. Для осуществления сбора ПДн с использованием информационно-телекоммуникационных сетей, опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки ПДн и сведения о реализуемых требованиях к защите ПДн, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

8.2.11. Представить документы и локальные акты, предусмотренные законодательством Российской Федерации, и/или иным образом подтвердить принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора ИСПДн, по запросу уполномоченного органа по защите прав субъектов ПДн.

8.2.12. При обработке ПДн принимать необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

8.2.13. Сообщить в порядке, предусмотренном законодательством Российской Федерации, субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.

8.2.14. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя Оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение законодательства Российской Федерации, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

8.2.15. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или

его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие ПДн. Оператор обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

8.2.16. Сообщить в уполномоченный орган по защите прав субъектов ПДн, по запросу этого органа, необходимую информацию в течение тридцати дней с даты получения такого запроса.

8.2.17. В случае выявления неправомерной обработки ПДн, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки ПДн невозможно, Оператор в срок, не превышающий семи рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Оператор обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

8.2.18. В случае достижения цели обработки ПДн прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации.

8.2.19. В случае отзыва субъектом ПДн согласия на обработку его ПДн, прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации.

9. ПОРЯДОК ОБРАБОТКИ И ЗАЩИТЫ ПДН

9.1. Обеспечение конфиденциальности ПДн, обрабатывающихся Оператором, является обязательным требованием для всех лиц, которым ПДн стали известны.

9.2. Сотрудники Оператора, обязаны получать в установленных случаях согласие субъектов ПДн на обработку их ПДн.

9.3. В случае нарушения установленного порядка обработки ПДн сотрудники Оператора несут ответственность в соответствии с разделом 13 настоящего Положения.

9.4. ПДн субъектов на бумажных носителях, обрабатываемые Оператором, хранятся в отделах (у сотрудников), имеющих допуск к обработке соответствующих ПДн, а также в архиве ИП. Право допуска сотрудников к неавтоматизированной ИСПДн определяется ИП. Носители ПДн не должны оставаться без присмотра. При покидании рабочего места, сотрудники, осуществляющие обработку ПДн должны, убирать носители ПДн в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям ПДн. При утере или порче ПДн осуществляется по возможности их восстановление.

9.5. Места хранения документов, содержащих ПДн:

9.5.1. ПДн клиентов Оператора – договоры, акты, соглашения, анкеты, копии паспортов, иные документы, носители информации (флеш-карты, CD-диски, и т.п.) хранятся в специально предусмотренных помещениях Оператора, размещаются на полках и запираются на ключ.

9.5.2. ПДн сотрудников Оператора – документы, носители информации (флеш-карты, CD-диски и т.п.) хранятся в специально отведённом месте и запираются на ключ.

9.6. Выдача документов для ознакомления осуществляется лицам, допущенным к соответствующей информации в целях исполнения должностных обязанностей, на срок, не более одного рабочего дня.

9.7. Иные носители информации (флеш-карты, CD-диски и т.п.) могут храниться в помещениях Оператора, размещаются на полках и запираются на ключ или же в сейфах или запираемых шкафах.

9.8. При работе с программными средствами информационной системы Оператора, реализующей функции просмотра и редактирования ПДн, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

9.9. При получении ПДн сотрудником Оператора, который в соответствии с должностными обязанностями получает ПДн от клиента, в обязательном порядке проводится проверка достоверности ПДн. Ввод ПДн, полученных Оператором, в информационную систему осуществляется сотрудниками, имеющими доступ к соответствующим ПДн. Сотрудники, осуществляющие ввод информации, несут ответственность за достоверность и полноту введенной информации.

9.10. Особенности обработки ПДн, содержащихся на бумажных носителях, без использования средств автоматизации установлены в соответствии с Постановлением Правительства Российской Федерации от

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

9.11. При неавтоматизированной обработке различных категорий ПДн должен использоваться отдельный материальный носитель для каждой категории ПДн.

9.12. При неавтоматизированной обработке ПДн на бумажных носителях:

9.12.1. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы.

9.12.2. ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

9.13. 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.

9.14. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление).

9.15. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

9.16. Уничтожение носителей, содержащих ПДн, осуществляется в следующем порядке:

9.16.1. ПДн на бумажных носителях уничтожаются путем использования шредеров (уничтожители документов), установленных в офисе Оператора, а также иным путем полного уничтожения без возможности восстановления.

9.16.2. ПДн, размещенные в памяти автоматизированного рабочего места уничтожаются путем удаления её из памяти АРМ.

9.16.3. ПДн, размещенные на флеш-карте, CD-диске, ином носителе информации уничтожаются путем удаления файла с носителя, при необходимости путем нарушения работоспособности флеш-карты или CD-диска.

9.17. Уничтожение носителей контролируется комиссией, назначенной ИП. Об уничтожении носителя комиссией составляется акт.

9.18. Помещения Оператора, в которых обрабатываются и хранятся ПДн, должны запираться и опечатываться, окна должны быть закрыты. В нерабочее время так же должна быть включена сигнализация (при наличии).

9.19. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

9.20. Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПДн.

9.21. В обязанности администратора информационной безопасности и администратора ИСПДн входит управление учетными записями пользователей ИСПДн, поддержание штатной работы ИСПДн, обеспечение резервного копирования данных, а также установка и конфигурирование аппаратного и программного обеспечения ИСПДн, обеспечение соответствия порядка обработки и обеспечения безопасности ПДн в ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемых к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленных федеральным законодательством.

9.22. В обязанности администратора информационной безопасности также входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации ИСПДн, учет и хранение машинных носителей ПДн, периодический аудит журналов безопасности и анализ защищенности ИСПДн, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

9.23. Квалификационные требования и детальный перечень прав и обязанностей администраторов закрепляются в соответствующих должностных инструкциях или утверждаются соответствующими приказами ИП, с которыми сотрудники, назначаемые на данные роли, должны быть ознакомлены под роспись.

9.24. Организация внутреннего контроля процесса обработки ПДн у Оператора осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

9.25. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

9.25.1. Обеспечение соблюдения сотрудниками Оператора требований настоящего Положения и нормативно-правовых актов, регулирующих обработку и защиту ПДн.

9.25.2. Оценка компетентности персонала, задействованного в обработке ПДн.

9.25.3. Обеспечение работоспособности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн.

9.25.4. Выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений.

9.25.5. Принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн.

9.25.6. Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий.

9.25.7. Осуществление внутреннего контроля за исполнением рекомендаций и указаний по устранению нарушений.

9.26. Результаты контрольных мероприятий оформляются протоколами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств ИСПДн и средств защиты ПДн, по обучению и повышению компетентности персонала, задействованного в обработке ПДн.

10. ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПДН

10.1. Проверки проводятся на основании ежегодного плана, утвержденного руководителем, или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

10.2. В плане по каждой проверке устанавливается объект внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.

10.3. Проверки проводятся комиссией, создаваемой соответствующим приказом ИП.

10.4. Основанием для проведения внеплановой проверки является поступившее ИП письменное обращение субъекта персональных данных или его представителя о нарушении правил обработки персональных данных.

10.5. Проведение внеплановой проверки организуется в течение 5 рабочих дней с момента поступления обращения. Срок проведения проверки не может превышать 30 дней со дня принятия решения о ее проведении.

10.6. Члены комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных субъектов персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.

10.7. По результатам каждой проверки комиссией проводится заседание. Решения, принятые на заседаниях комиссии, оформляются протоколом. По существу, поставленных в обращении (жалобе) вопросов

комиссия в течение 5 рабочих дней со дня окончания проверки дает письменный ответ заявителю.

11. РАБОТА С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ В СЛУЧАЕ ОБЕЗЛИЧИВАНИЯ ПДН

11.1. Обезличивание персональных данных производится с целью устранения возможности определить принадлежность ПДн конкретному субъекту ПДн сотрудниками ИП и в соответствии с законодательством Российской Федерации.

11.2. Обезличенные персональные данные конфиденциальны и не подлежат разглашению.

11.3. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

11.4. При обработке обезличенных персональных данных необходимо соблюдение раздела 9 настоящего Положения.

12. ОСОБЕННОСТИ ОБРАБОТКИ ПДН СОТРУДНИКОВ ОПЕРАТОРА БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

12.1. Персональные данные сотрудников Оператора при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

12.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

12.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на

обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

− типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

− типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

12.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

− при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

− при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

12.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

12.6. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

12.7. При хранении материальных носителей у Оператора соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер,

необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Оператором.

13. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

13.1. Руководство Оператора несет ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

13.2. Сотрудники Оператора несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

13.3. Сотрудник Оператора может быть привлечен к ответственности в случаях:

13.3.1. Умышленного или неосторожного раскрытия ПДн.

13.3.2. Утраты материальных носителей ПДн.

13.3.3. Нарушения требований настоящего Положения и других нормативных документов Оператора в части вопросов доступа и работы с ПДн.

13.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Оператору, его сотрудникам, клиентам и контрагентам материального или иного ущерба, виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.