УТВЕРЖДЕНО
Приказом генерального директора
ООО МКК «БЕСТВЕЙ»
От 17 августа 2026 г. № 08-ПД

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ МИКРОКРЕДИТНОЙ КОМПАНИИ «БЕСТВЕЙ»

г. Москва

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ.....3

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ.....4

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....6

4. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ.....18

5. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ, РАЗРЕШЕННЫХ СУБЪЕКТОМ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ РАСПРОСТРАНЕНИЯ.....19

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ.....20

7. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ.....29

8. ПРАВА И ОБЯЗАННОСТИ ОБЩЕСТВА КАК ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ.....30

9. ВНУТРЕННИЙ КОНТРОЛЬ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.....32

10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ.....33

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.....34

Приложение № 1.....35

1. ОБЩИЕ ПОЛОЖЕНИЯ

Положение о защите персональных данных является локальным нормативным актом ООО МКК «БЕСТВЕЙ» (далее - Общество), устанавливающим порядок получения, обработки, хранения, передачи и защиты персональных данных работников, клиентов, представителей клиентов, контрагентов и иных субъектов персональных данных в Обществе.

Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Главой 14 Трудового кодекса Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлениями Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

В настоящем Положении используются следующие термины и определения:

Актуальные угрозы безопасности — это совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Защита персональных данных – комплекс мер, принимаемых Обществом для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Клиент - физическое лицо, вступившее с Обществом в договорные отношения.

Контрагент - индивидуальный предприниматель или физическое лицо - плательщик налога на профессиональный доход, вступивший с Обществом в договорные отношения.

Конфиденциальная информация – информация, содержащая сведения конфиденциального характера, в том числе получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах, в отношении которой Общество принимает меры по защите от несанкционированного доступа третьих лиц, не имеющих право доступа к такой информации.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Оператор – ООО МКК «БЕСТВЕЙ», вступившее в договорные отношения с работником, клиентом или контрагентом, организующее и осуществляющее, в связи с этим обработки.

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

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 настоящим Положением.

Пользователь сайта - физическое лицо, выступающее от своего имени и в своих интересах или от имени и в интересах представляемого им юридического лица, заполняющее форму обратной связи и (или) подающее заявку на взаимодействие с Обществом на сайте Общества.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Представитель клиента - представитель юридического лица или индивидуального предпринимателя, вступивший с Обществом в договорные отношения.

Работник - физическое лицо, вступившее в трудовые отношения с работодателем.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Реестр определения прав доступа к Конфиденциальной информации (далее – Реестр прав доступа) – внутренний документ Общества, закрепляющий перечень должностей и категории Конфиденциальной информации, ресурсы информационной системы, криптографические ключи, к которым работники Общества имеют доступ.

Режим конфиденциальности – правовые, организационные, технические и иные меры по защите конфиденциальной информации, принимаемые ее обладателем на основании закона.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Субъект персональных данных – физическое лицо, персональные данные которого обрабатываются Обществом в целях, определенных настоящим Положением.

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

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях обеспечения прав и свобод человека и гражданина Обществом и его представителями при обработке персональных данных должны соблюдаться следующие общие требования:

Обработка персональных данных должна осуществляться на законной и справедливой основе, исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия выполнения договорных обязательств в соответствии с законодательством Российской Федерации.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, а также объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой.

Получение Обществом персональных данных может осуществляться как путем представления их самим субъектом персональных данных, так и путем получения их из иных источников. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие.

Общество должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и юридических последствиях отказа предоставления его персональные данные и (или) дать согласие на их обработку, если в соответствии с федеральным законом предоставление персональных данных и (или) получение Обществом согласия на обработку персональных данных являются обязательными.

Согласие на обработку персональных данных должно быть оформлено отдельно от иной информации и (или) документов, которые подтверждает и (или) подписывает субъект персональных данных.

Общество не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его политических, религиозных и иных убеждениях, о частной жизни. В необходимых случаях данные о частной жизни работника или клиента (информация о семейных, бытовых, личных отношениях) могут быть получены и обработаны Обществом только с его письменного согласия.

Общество не имеет право получать и обрабатывать персональные данные субъектов персональных данных об их членстве в общественных объединениях или их профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

Персональные данные субъекта персональных данных не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено действующим законодательством Российской Федерации.

При принятии решений, затрагивающих интересы субъекта персональных данных, Общество не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки без письменного согласия субъекта персональных данных на такие действия.

При идентификации клиента или контрагента Общество может затребовать предъявления документов, удостоверяющих личность и подтверждающих полномочия представителя. При заключении договора и в ходе его выполнения, Общество может затребовать предоставление клиентом или контрагентом иных документов, содержащих информацию о нем.

После принятия решения о заключении договора или предоставления документов, подтверждающих полномочия представителя, а также впоследствии, в процессе выполнения договора, к документам, содержащим персональные данные клиента или контрагента, также будут относиться:

- договоры;
- приказы по основной деятельности;
- служебные записки;

– другие документы, где включение персональных данных клиента или контрагента необходимо согласно действующему законодательству.

Не допускается отвечать на вопросы, связанные с предоставлением персональных данных по телефону или факсу, по электронной почте и иным видам связи.

Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

Период хранения и обработки персональных данных определяется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ОСУЩЕСТВЛЕНИЯ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ, ПРЕДУСМОТРЕННОЙ УСТАВОМ ОБЩЕСТВА

Общество осуществляет обработку персональных данных в целях осуществления предпринимательской деятельности, предусмотренной Уставом Общества.

Для цели осуществления предпринимательской деятельности Общество обрабатывает персональные данные у следующих категорий субъектов персональных данных:

- **представителей клиентов** - представитель юридического лица или индивидуального предпринимателя;
- **контрагентов -** индивидуальный предприниматель или физическое лицо - плательщик налога на профессиональный доход, вступивший с Обществом в договорные отношения;
- **учредителей Общества** – физических лиц.

Общество запрашивает у **контрагентов** следующие персональные данные:

· фамилия, имя, отчество;
· паспортные данные;
· занимаемая должность;
· телефон;
· номер банковского счета;
· адрес электронной почты.

Общество запрашивает у **представителей клиентов** следующие персональные данные:

· фамилия, имя, отчество;
· паспортные данные;
· телефон;
· адрес электронной почты;
· номер банковского счета;
· должность.

Общество запрашивает у **учредителей Общества** следующие персональные данные:

• фамилия, имя, отчество (при наличии);
• год, месяц, дата и место рождения;
• адрес;
• паспортные данные;
• данные страхового свидетельства государственного пенсионного страхования (СНИЛС);

- данные свидетельства о постановке на учет в налоговом органе физического лица (ИНН);
- адрес электронной почты;
- телефон.

Обществом не обрабатываются биометрические персональные данные и специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Общество осуществляет обработку персональных данных следующими способами:

– Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

– Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

– Смешанная обработка персональных данных - обработка персональных данных, как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных начинается с момента поступления персональных данных в Общество и прекращается:

– в случае выявления неправомерных действий с персональными данными;

– в случае достижения цели обработки персональных данных;

– в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;

– в случае получения Обществом требования субъекта персональных данных о прекращении обработки персональных данных;

– в случае прекращения деятельности Общества.

Хранение персональных данных осуществляется в Обществе:

– в течение пяти лет с момента фактического прекращения отношений с клиентом;

– не более 30 дней с даты достижения цели их обработки в случае, если договор оказания услуг не заключен;

– в сейфе на бумажных носителях и на электронных носителях с ограниченным доступом;

– в электронном виде на облачных-серверах\базах данных.

Уничтожение персональных данных осуществляется комиссией, назначаемой приказом руководителя Общества. Лицо, ответственное за организацию обработки персональных данных, назначается председателем комиссии по уничтожению персональных данных.

При наступлении любого из событий, повлекших необходимость уничтожения персональных данных в соответствии с законодательством Российской Федерации, лицо, ответственное за организацию обработки персональных данных, обязано:

– уведомить членов комиссии о дате начала работ по уничтожению персональных данных;

– определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);

– установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению (и/или материальные носители персональных данных);

– руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных): документы, подлежащие уничтожению, измельчаются в шредере, персональные данные клиентов в электронном виде стираются с электронных носителей, либо физически уничтожаются сами материальные носители, на которых хранится информация;

– в случае необходимости уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

В целях подтверждения уничтожения персональных данных составляются следующие документы:

1) В случае если обработка персональных данных осуществляется без использования средств автоматизации - Акт об уничтожении персональных данных.

2) В случае если обработка персональных данных осуществляется с использованием средств автоматизации либо одновременно с использованием средств автоматизации и без использования средств автоматизации - Акт об уничтожении персональных данных и Выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

Формы акта об уничтожении персональных данных и выгрузки из журнала утверждаются приказом руководителя Общества и содержат все обязательные сведения, указанные в Приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

Акт об уничтожении персональных данных может быть составлен как на бумажном носителе, так и в электронном виде и подписан лицом (лицами), уничтожившими персональные данные, собственноручной либо электронной подписью соответственно.

Акт об уничтожении персональных данных и выгрузка из журнала хранятся Обществом в течение 3 лет с момента уничтожения персональных данных.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ЗАКЛЮЧЕНИЯ И ИСПОЛНЕНИЯ ГРАЖДАНСКО-ПРАВОВЫХ ДОГОВОРОВ

Общество осуществляет обработку персональных данных в целях заключения и исполнения гражданско-правовых договоров, в связи с осуществлением хозяйственной деятельности Общества.

Для цели заключения и исполнения гражданско-правовых договоров Общество обрабатывает персональные данные у следующих категорий субъектов персональных данных:

- **контрагентов** – самозанятых / индивидуальных предпринимателей;
- **представителей клиентов** - представитель юридического лица или индивидуального предпринимателя;
- **клиентов** – физических лиц.

Общество запрашивает у **контрагентов** следующие персональные данные:

· фамилия, имя, отчество;
· паспортные данные;
· занимаемая должность;
· телефон;
· адрес электронной почты.

Общество запрашивает у **представителей клиентов** следующие персональные данные:

· фамилия, имя, отчество;
· паспортные данные;
· телефон;
· адрес электронной почты;
· должность.

Общество запрашивает у **клиентов** следующие персональные данные:

• фамилия, имя, отчество;
• паспортные данные;
• телефон.

Обществом не обрабатываются биометрические персональные данные и специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Общество осуществляет обработку персональных данных следующими способами:

– Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

– Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

– Смешанная обработка персональных данных - обработка персональных данных как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных начинается с момента поступления персональных данных в Общество и прекращается:

– в случае выявления неправомерных действий с персональными данными;

– в случае достижения цели обработки персональных данных;

– в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;

– в случае получения Обществом заявления субъекта персональных данных о прекращении обработки персональных данных;

– в случае прекращения деятельности Общества.

Хранение персональных данных осуществляется в Обществе:

– в течение пяти лет с момента фактического прекращения отношений с контрагентом;

– не более 30 дней с даты достижения цели их обработки в случае, если договор с контрагентом не был заключен;

– в сейфе на бумажных носителях и на электронных носителях с ограниченным доступом;

– в электронном виде на облачных-серверах/базах данных.

Уничтожение персональных данных контрагентов Общества осуществляется комиссией, назначаемой приказом руководителя Общества. Лицо, ответственное за организацию обработки персональных данных, назначается председателем комиссии по уничтожению персональных данных.

При наступлении любого из событий, повлекших необходимость уничтожения персональных данных контрагентов Общества в соответствии с законодательством Российской Федерации, лицо, ответственное за организацию обработки персональных данных, обязано:

– уведомить членов комиссии о дате начала работ по уничтожению персональных данных;

– определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);

– установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению (и/или материальные носители персональных данных);

– руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных): документы, подлежащие уничтожению, измельчаются в шредере, персональные данные клиентов в электронном виде стираются с электронных носителей, либо физически уничтожаются сами материальные носители, на которых хранится информация;

– в случае необходимости – уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

В целях подтверждения уничтожения персональных данных составляются следующие документы:

В случае если обработка персональных данных осуществляется без использования средств автоматизации - Акт об уничтожении персональных данных.

В случае если обработка персональных данных осуществляется с использованием средств автоматизации либо одновременно с использованием средств автоматизации и без использования средств автоматизации - Акт об уничтожении персональных данных, и Выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

Формы акта об уничтожении персональных данных и Выгрузки из журнала утверждаются приказом руководителя Общества и содержат все обязательные сведения, указанные в Приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

Акт об уничтожении персональных данных может быть составлен как на бумажном носителе, так и в электронном виде и подписан лицом (лицами), уничтожившими персональные данные, собственноручной либо электронной подписью соответственно.

Акт об уничтожении персональных данных и выгрузка из журнала хранятся Обществом в течение 3 лет с момента уничтожения персональных данных.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ОФОРМЛЕНИЯ ТРУДОВЫХ ОТНОШЕНИЙ

Общество осуществляет обработку персональных данных в целях оформления трудовых отношений, в том числе исполнение обязательств по трудовым договорам; ведение кадрового делопроизводства; содействие работникам в обучении и продвижении по службе; исполнение требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение.

Для цели оформления трудовых отношений Общество обрабатывает персональные данные у следующих категорий субъектов персональных данных:

- **работников** (в том числе уволенных);
- **родственников работника**.

Общество запрашивает у **работников** (в том числе уволенных) следующие персональные данные:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес регистрации по месту жительства (почтовый адрес);
- адрес фактического проживания (почтовый адрес фактического проживания);
- семейное положение;
- паспортные данные;
- адрес электронной почты, телефон;
- данные свидетельства о заключении брака;
- данные свидетельства о расторжении брака;
- данные свидетельства о рождении детей;
- сведения о стаже работы и о местах работы (город, название организации, должность, сроки работы);
- сведения о наградах (поощрениях), почетных званиях;
- данные страхового свидетельства государственного пенсионного страхования (СНИЛС);
- данные свидетельства о постановке на учет в налоговом органе физического лица (ИНН);
- сведения об образовании, повышении квалификации, профессиональной переподготовки и местах обучения (город, образовательное учреждение, сроки обучения, специальность, квалификация, профессия);
- сведения о наличии льгот и гарантий, предоставляемых в соответствии с действующим законодательством;
- номер расчетного счета;
- данные документов воинского учета – для военнообязанных и лиц, подлежащих призыву на воинскую службу.

Общество запрашивает специальные категории персональных данных у некоторых категорий работников:

- сведения о судимости.

Общество запрашивает персональные данные **родственников работника** исключительно в целях заполнения личной карточки работника по унифицированной форме в следующем объеме:

- фамилия, имя, отчество;
- год, месяц, дата рождения;
- данные, содержащиеся в свидетельстве о браке.

Общество осуществляет обработку персональных данных следующими способами:

– Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

– Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

– Смешанная обработка персональных данных - обработка персональных данных как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных начинается с момента поступления персональных данных в Общество и прекращается:

– в случае выявления неправомерных действий с персональными данными;

– в случае достижения цели обработки персональных данных;

– в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;

– в случае получения Обществом требования субъекта персональных данных о прекращении обработки персональных данных;

– в случае прекращения деятельности Общества.

Хранение персональных данных осуществляется в Обществе:

– в течение 75 лет после расторжения с работником трудового договора;

– в электронном виде на облачных серверах базах данных.

Уничтожение персональных данных работников Общества осуществляется комиссией, назначаемой приказом руководителя Общества. Лицо, ответственное за организацию обработки персональных данных, назначается председателем комиссии по уничтожению персональных данных.

При наступлении любого из событий, повлекших необходимость уничтожения персональных данных контрагентов Общества, в соответствии с законодательством Российской Федерации, лицо, ответственное за организацию обработки персональных данных, обязано:

– уведомить членов комиссии о дате начала работ по уничтожению персональных данных;

– определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);

– установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению (и/или материальные носители персональных данных);

– руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных): документы, подлежащие уничтожению, измельчаются в шредере, персональные данные клиентов в электронном виде стираются с электронных носителей, либо физически уничтожаются сами материальные носители, на которых хранится информация;

– в случае необходимости – уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

В целях подтверждения уничтожения персональных данных составляются следующие документы:

- Акт об уничтожении персональных данных.

- Акт об уничтожении персональных данных и Выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

Формы акта об уничтожении персональных данных и Выгрузки из журнала утверждаются приказом руководителя Общества и содержат все обязательные сведения, указанные в Приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

Акт об уничтожении персональных данных может быть составлен как на бумажном носителе, так и в электронном виде, и подписан лицом (лицами), уничтожившими персональные данные, собственноручной либо электронной подписью соответственно.

Акт об уничтожении персональных данных и Выгрузка из журнала хранятся Обществом в течение 3 лет с момента уничтожения персональных данных.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ПОДБОРА ПЕРСОНАЛА

Общество осуществляет обработку персональных данных в целях подбора персонала.

Для цели подбора персонала Общество обрабатывает персональные данные у следующих категорий субъектов персональных данных:

– **соискатели на замещение вакантных должностей**.

Общество запрашивает у соискателей на замещение вакантных должностей следующие персональные данные:

- фамилия, имя, отчество;
- гражданство,
- адрес регистрации по месту жительства (почтовый адрес);
- адрес фактического проживания (почтовый адрес фактического проживания);
- адрес электронной почты, телефон;
- сведения о стаже работы и о местах работы (город, название организации, должность, сроки работы);
- сведения о наградах (поощрениях), почетных званиях;

- сведения об образовании, повышении квалификации, профессиональной переподготовки и местах обучения (город, образовательное учреждение, сроки обучения, специальность, квалификация, профессия).

Общество запрашивает специальные категории персональных данных у некоторых категорий работников:

Общество осуществляет обработку персональных данных следующими способами:

- Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
- Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
- Смешанная обработка персональных данных - обработка персональных данных, как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных начинается с момента поступления персональных данных в Общество и прекращается:

- в случае выявления неправомерных действий с персональными данными;
- в случае достижения цели обработки персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;
- в случае получения Обществом требования субъекта персональных данных о прекращении обработки персональных данных;
- в случае прекращения деятельности Общества.

Хранение персональных данных соискателей на вакантные должности осуществляется в Обществе:

- не более 30 дней с даты достижения цели обработки персональных данных соискателей на замещение вакантных должностей.

Уничтожение персональных данных соискателей на замещение вакантных должностей Общества осуществляется комиссией, назначаемой приказом руководителя Общества. Лицо, ответственное за организацию обработки персональных данных, назначается председателем комиссии по уничтожению персональных данных.

При наступлении любого из событий, повлекших необходимость уничтожения персональных данных контрагентов Общества, в соответствии с законодательством Российской Федерации, лицо, ответственное за организацию обработки персональных данных обязано:

- уведомить членов комиссии о дате начала работ по уничтожению персональных данных;
- определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);
- установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению (и/или материальные носители персональных данных);

- руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных): документы, подлежащие уничтожению, измельчаются в шредере, персональные данные клиентов в электронном виде стираются с электронных носителей, либо физически уничтожаются сами материальные носители, на которых хранится информация;
- в случае необходимости уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

В целях подтверждения уничтожения персональных данных составляются следующие документы:

В случае, если обработка персональных данных осуществляется без использования средств автоматизации – Акт об уничтожении персональных данных.

В случае, если обработка персональных данных осуществляется с использованием средств автоматизации либо одновременно с использованием средств автоматизации и без использования средств автоматизации – Акт об уничтожении персональных данных и Выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

Формы акта об уничтожении персональных данных и Выгрузки из журнала утверждаются приказом руководителя Общества и содержат все обязательные сведения, указанные в Приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

Акт об уничтожении персональных данных может быть составлен как на бумажном носителе, так и в электронном виде и подписан лицом (лицами), уничтожившими персональные данные, собственноручной либо электронной подписью соответственно.

Акт об уничтожении персональных данных и Выгрузка из журнала хранятся Обществом в течение 3 лет с момента уничтожения персональных данных.

Общество осуществляет обработку персональных данных следующими способами:

- Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
- Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
- Смешанная обработка персональных данных - обработка персональных данных, как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных начинается с момента поступления персональных данных в Общество и прекращается:

- в случае выявления неправомерных действий с персональными данными;
- в случае достижения цели обработки персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;

- в случае получения Обществом требования субъекта персональных данных о прекращении обработки персональных данных;
- в случае прекращения деятельности Общества.

Хранение персональных данных соискателей на вакантные должности осуществляется в Обществе:

- не более 30 дней с даты достижения цели обработки персональных данных соискателей на замещение вакантных должностей.

При наступлении любого из событий, повлекших необходимость уничтожения персональных данных соискателей на вакантные должности Общества в соответствии с законодательством Российской Федерации, лицо, ответственное за организацию обработки персональных данных обязано:

- уведомить членов комиссии о дате начала работ по уничтожению персональных данных;
- определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);
- установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению (и/или материальные носители персональных данных);
- руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных): документы, подлежащие уничтожению, измельчаются в шредере, персональные данные клиентов в электронном виде стираются с электронных носителей, либо физически уничтожаются сами материальные носители, на которых хранится информация;
- в случае необходимости – уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

В целях подтверждения уничтожения персональных данных составляются следующие документы:

В случае если обработка персональных данных осуществляется без использования средств автоматизации - Акт об уничтожении персональных данных.

В случае, если обработка персональных данных осуществляется с использованием средств автоматизации либо одновременно с использованием средств автоматизации и без использования средств автоматизации - Акт об уничтожении персональных данных и Выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

Формы акта об уничтожении персональных данных и выгрузки из журнала утверждаются приказом руководителя Общества и содержат все обязательные сведения, указанные в Приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

Акт об уничтожении персональных данных может быть составлен как на бумажном носителе, так и в электронном виде и подписан лицом (лицами), уничтожившими персональные данные, собственноручной либо электронной подписью соответственно.

Акт об уничтожении персональных данных и Выгрузка из журнала хранятся Обществом в течение 3 лет с момента уничтожения персональных данных.

ОБЕСПЕЧЕНИЕ ВЗАИМОДЕЙСТВИЯ С СУБЪЕКТАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОСРЕДСТВОМ САЙТА ОБЩЕСТВА

Общество осуществляет обработку персональных данных в целях обеспечения взаимодействия с субъектами персональных данных посредством сайта Общества.

Для цели обеспечения взаимодействия с субъектами персональных данных посредством сайта Общество обрабатывает персональные данные у следующих категорий субъектов персональных данных:

- **клиенты;**
- **посетители сайта.**

Общество запрашивает следующие персональные данные:

· фамилия, имя, отчество (при наличии);

· телефон;

· адрес электронной почты;

· сведения, собираемые посредством метрических программ, применяемых на сайте Яндекс.Метрика.

Общество может использовать общеотраслевую технологию «куки». Куки – это небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере, который использует пользователь сайта, позволяющий Обществу сохранять персональные настройки и предпочтения пользователя сайта, а также собирать неличную информацию о нем.

Техническая информация, автоматически собираемая программным обеспечением Сайта во время его посещения Пользователем, включает:

- IP-адрес,
- Просмотр страницы,
- Параметры загрузки страницы;
- Время до отрисовки и время ответа сервера;
- Географические данные;
- Браузер и его версия;
- Операционная система и ее версия;
- Визит;
- Переход по внешней ссылке;
- Скачивание файла.

В любое время пользователь сайта может изменить параметры в настройках своего браузера таким образом, чтобы браузер перестал сохранять все файлы куки, а также оповещал об их отправке. В этом случае некоторые сервисы и функции сайта могут перестать работать или работать некорректно.

Общество может использовать метрический сервис «Яндекс.Метрика», формы обратной связи Jivo.

Обществом не обрабатываются биометрические персональные данные и специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Общество осуществляет обработку персональных данных автоматизировано, т.е. с помощью средств вычислительной техники.

Обработка персональных данных начинается с момента поступления персональных данных в Общество и прекращается:

- в случае выявления неправомерных действий с персональными данными;
- в случае достижения цели обработки персональных данных;

- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;
- в случае получения Обществом требования субъекта персональных данных о прекращении обработки персональных данных;
- в случае прекращения деятельности Общества.

Хранение персональных данных осуществляется в Обществе:

- в течение пяти лет с момента фактического прекращения отношений с посетителями сайта;
- не более 30 дней с даты достижения цели их обработки в случае, если договор оказания услуг не заключен;
- в сейфе на электронных носителях с ограниченным доступом;
- в электронном виде в информационной системе персональных данных сайта Общества, а также в архивных копиях баз данных сайта Общества.

Уничтожение персональных данных осуществляется комиссией, назначаемой приказом руководителя Общества. Лицо, ответственное за организацию обработки персональных данных, назначается председателем комиссии по уничтожению персональных данных.

При наступлении любого из событий, повлекших необходимость уничтожения персональных данных, в соответствии с законодательством Российской Федерации, лицо, ответственное за организацию обработки персональных данных, обязано:

- уведомить членов комиссии о дате начала работ по уничтожению персональных данных;
- определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);
- установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению.
- в процессе руководства работой членов комиссии произвести уничтожение персональных данных посетителей сайта в электронном виде стираются с электронных носителей, либо физически уничтожаются сами материальные носители, на которых хранится информация;
- в случае необходимости уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

В целях подтверждения уничтожения персональных данных составляются следующие документы:

1. Акт об уничтожении персональных данных и Выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).
2. Формы Акта об уничтожении персональных данных и Выгрузки из журнала утверждаются приказом руководителя Общества и содержат все обязательные сведения, указанные в Приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».
3. Акт об уничтожении персональных данных может быть составлен как на бумажном носителе, так и в электронном виде и подписан лицом (лицами), уничтожившими персональные данные, собственноручной либо электронной подписью соответственно.
4. Акт об уничтожении персональных данных и Выгрузка из журнала хранятся Обществом в течение трех лет с момента уничтожения персональных данных.

4. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

Общество вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта.

Лицо, осуществляющее обработку персональных данных по поручению Общества, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

В поручении Общества определяется перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели их обработки, и устанавливаются обязанности, запреты:

- соблюдать конфиденциальность персональных данных;
- принимать меры, направленные на обеспечение выполнения обязанностей, предусмотренных локально-нормативными актами Общества;
- при сборе персональных данных в том числе посредством информационно-телекоммуникационной сети «Интернет», запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся за пределами территории Российской Федерации, не допускается;
- предоставлять Обществу документы и информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- уведомлять Общество в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных.

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

В случае, если Общество поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Общество. Лицо, осуществляющее обработку персональных данных по поручению Общества, несет ответственность перед Обществом.

5. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ, РАЗРЕШЕННЫХ СУБЪЕКТОМ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ РАСПРОСТРАНЕНИЯ

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

Общество обеспечивает субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на

обработку персональных данных, разрешенных субъектом персональных данных для распространения.

В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных Обществом неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

Общество в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных публикует информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения. Публикация информации осуществляется в местах распространения персональных данных, разрешенных субъектом персональных данных для распространения.

Общество в любое время по требованию субъекта персональных данных прекращает передачу (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения.

Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления Обществу требования, указанного п. 7.7 настоящего Положения.

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Обществом определено, что на информацию, содержащую персональные данные, распространяется режим конфиденциальности.

Организация работы по защите Конфиденциальной информации, в том числе персональных данных.

Безопасность персональных данных при их использовании и обработке в Обществе обеспечивается с помощью системы защиты Конфиденциальной информации, разработанной самим Обществом (далее – система защиты).

При разработке системы защиты учитывалась обязанность Общества обеспечивать защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, в том числе принимать меры, установленные статьей 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Система защиты реализуется путем проведения нескольких взаимосвязанных процессов. К ним относятся:

– определение актуальных угроз безопасности персональных данных.

Порядок определения актуальных угроз безопасности персональных данных, и ответственный за проведение процедуры определения актуальных угроз безопасности, определяется приказом руководителя Общества. Результатом проведения процедуры определения актуальных угроз безопасности персональных данных является составление акта определения актуальных угроз безопасности;

– оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– определение необходимых правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах, исполнение которых обеспечивает необходимый уровень защищенности;

Необходимый уровень защищенности персональных данных при обработке в информационных системах определяется Обществом при выявлении актуальных угроз безопасности с учетом результатов проведенной оценки вреда, который может быть причинен субъектам персональных данных и фиксируется в акте определения актуальных угроз безопасности;

– надлежащее применение определенных правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах, а также применение прошедших в установленном порядке процедуру оценки соответствия средств защиты персональных данных;

– проведение оценки эффективности принимаемых мер по обеспечению безопасности персональных данных с установленной в настоящем Положении периодичностью;

– обеспечение контроля надлежащей реализации мер по обеспечению безопасности персональных данных.

Порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее в подпункте – вред, оценка вреда).

1) Оценка вреда осуществляется ответственным за организацию обработки персональных данных либо комиссией, образуемой оператором.

2) Общество для целей оценки вреда определяет одну из следующих степеней вреда: высокую, среднюю или низкую, в зависимости от критериев, установленных в Приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 октября 2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее в подпункте – Требования).

При этом в случае, если по итогам проведенной оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

Результаты оценки вреда оформляются актом оценки вреда, форма которого утверждается приказом руководителя и содержит все обязательные сведения, указанные в Требованиях.

Акт оценки вреда может быть составлен как на бумажном носителе, так и в электронном виде и подписан лицом (лицами), проводившими оценку вреда, собственноручной либо электронной подписью соответственно.

В целях обеспечения функционирования системы защиты руководитель выполняет следующие функции:

– организация разработки проектов и утверждение внутренних документов Общества по вопросам обеспечения режима конфиденциальности, определения режима порядка обращения с персональными данными с привлечением иных работников Общества;

– организация взаимодействия с органами государственной власти, правоохранительными и надзорными органами по вопросам обеспечения и соблюдения режима конфиденциальности;

– утверждение Реестра прав доступа, в том числе при внесении изменений и дополнений;

– рассмотрение вопроса о передаче персональных данных третьим лицам;

– определение требований к техническому оснащению помещений, в которых осуществляется работа с персональными данными;

– осуществление контроля за обеспечением режима безопасности помещений;

– принятие решений о необходимости проведения обучений для работников Общества;

– проведение плановых и внезапных проверок на предмет соблюдения режима конфиденциальности в Обществе работниками Общества;

– принятие решений о необходимости отстранения от работы с конфиденциальной информации работников Общества, нарушающих режим конфиденциальности в Обществе;

– рассмотрение иных вопросов обеспечения и соблюдения режима конфиденциальности.

Защите подлежат все персональные данные, определенные в разделе 2 настоящего Положения, в том числе:

– персональные данные субъекта, содержащиеся в копиях документов;

– персональные данные субъекта, содержащиеся в документах, созданных Обществом;

– персональные данные субъекта, занесенные в учетные формы;

– записи, содержащие персональные данные субъекта;

– персональные данные субъекта, содержащиеся на электронных носителях;

– персональные данные субъекта, обрабатываемые в информационных системах персональных данных;

– персональные данные субъекта, разрешенные субъектом для распространения.

Правовые меры защиты персональных данных.

К правовым мерам защиты персональных данных относится:

1) Разработка и утверждение локальных нормативных актов Общества: Политики в отношении обработки и защиты персональных данных, Положения о защите персональных данных, иных документов, которыми регламентируется порядок организации системы защиты в Обществе (далее – Регламентирующие документы).

2) Обязанность Общества осуществлять мониторинг действующего законодательства.

Регламентирующие документы разрабатываются самим Обществом или с привлечением третьих лиц и утверждаются руководителем Общества.

Регламентирующие документы должны пересматриваться на предмет их актуальности и необходимости внесения изменений не реже одного раза в год, а также:

– в случае изменения законодательства, регламентирующего порядок обращения организаций с Конфиденциальной информацией и устанавливающего требования к защите информации, в том числе законодательства о персональных данных;

– в случае установления фактов несанкционированного доступа к персональным данным, грубого нарушения работниками Общества режима конфиденциальности, разглашения и утечки информации, содержащей персональные данные;

– на основании заключения, сформированного по результатам проведения очередной оценки достаточности принятых мер по защите персональных данных.

Организационные меры защиты персональных данных.

К организационным мерам защиты персональных данных относятся:

Определение правил доступа к информации, содержащей персональные данные.

К работе с информацией, содержащей персональные данные, могут быть допущены работники Общества при одновременном выполнении следующих условий:

– должность работника указана в Реестре прав доступа;

– работник ознакомлен под подпись с Реестром прав доступа и настоящим Положением;

– работником Общества подписано Обязательство о неразглашении конфиденциальной информации.

Приказом руководителя Общества с целью определения перечня лиц, доступ которых к информации, содержащей персональные данные, необходим для выполнения ими своих должностных обязанностей, и определения необходимого объема информации, содержащей персональные данные, с которым вправе работать каждый из таких работников, утверждается Реестр прав доступа.

1) При утверждении Реестра прав доступа Общество руководствуется правилом о том, что доступ к персональным данным должен предоставляться только тем лицам, которым персональные данные необходимы для выполнения возложенных на них должностных обязанностей и только в том объеме (к той ее части), который необходим для выполнения определенных функций.

2) Реестр прав доступа Общества содержит следующую информацию:

– должности работников Общества, допущенных к работе с информацией, содержащей персональные данные;

– категории информации, к которым работники имеют доступ;

– ресурсы информационной системы, к которым работники имеют доступ;

– криптографические ключи, к которым работники имеют доступ.

3) Реестр прав доступа подлежит обязательному пересмотру не реже одного раза в год, а также в случае:

– изменения штатного расписания Общества;

– изменения функционала определенной должности;

– изменения перечня ресурсов информационной системы;

– приобретения или уничтожения Криптографических ключей.

4) Правом предоставления, ограничения, прекращения доступа ко всей информации, содержащей персональные данные, создаваемой, хранимой и обрабатываемой в Обществе, включая информацию, полученную от третьих лиц, обладает руководитель Общества.

До начала работы с персональными данными работник должен подписать Обязательство о неразглашении конфиденциальной информации.

Обязательство о неразглашении конфиденциальной информации, подписанное работником Общества, приобщается к личному делу работника.

Определение обязанностей для работников Общества при работе с персональными данными.

Работник Общества, допущенный к работе с информацией, содержащей персональные данные, обязан:

– знать и выполнять требования настоящего Положения, иных внутренних документов по защите информации;

– соблюдать ограничения, установленные Реестром прав доступа: работать только с теми сведениями и использовать только те ресурсы информационной системы, которые определены Реестром прав доступа;

– соблюдать порядок работы и меры по защите ставших ему известными сведений конфиденциального характера;

– соблюдать правила работы с носителями информации, содержащей персональные данные, порядок их учета и хранения, обеспечивать в процессе работы сохранность сведений, содержащихся в них от посторонних лиц;

– незамедлительно в письменной форме, информировать руководителя Общества о попытках несанкционированного доступа к информационным ресурсам и сведениям, содержащим персональные данные, о попытках подкупа, угроз, шантажа другими лицами с целью получения доступа к указанной информации;

– давать письменные объяснения о допущенных личных нарушениях установленного порядка работы, учета и хранения документов, содержащих персональные данные, и машинных съемных носителей информации, а также о фактах их утраты, передачи другим лицам.

Определение ограничений для работников Общества при работе с персональными данными.

Работнику, допущенному к работе с информацией, содержащей персональные данные, запрещается:

– передавать сведения конфиденциального характера и документы (в устной форме, по телефону, на бумажных и машинных носителях, в электронной виде и т.д.) другим лицам;

– использовать информацию, содержащую персональные данные, в открытой переписке, статьях и выступлениях, а также в личных интересах;

– передавать по незащищенным техническим каналам связи, в том числе сообщать (обсуждать) по телефону сведения, содержащие персональные данные;

– снимать копии с документов, содержащих персональные данные, или производить выписки из них;

– копировать документы Общества, содержащие персональные данные, и хранить их на машинных съемных носителях информации, а также использовать различные технические средства, способные накапливать и хранить информацию в электронном виде (фото, видео и звукозаписывающую аппаратуру, сотовые телефоны и т.п.), за исключением случаев, описанных в настоящем Положении;

– выполнять работы с материальными и машинными носителями, содержащими персональные данные, вне служебных помещений (помещений, где размещены подразделения Общества);

– выносить из служебных помещений документы и машинные носители с информацией, содержащей персональные данные.

Назначение лица, ответственного за информационную безопасность.

Приказом руководителя Общества назначается лицо, ответственное за информационную безопасность. В число его обязанностей входят:

– организация процесса реализации норм, установленных настоящим Положением, в том числе обеспечение работы системы защиты информации, содержащей персональные данные;

– обеспечение применения в Обществе определенных мер защиты информации, содержащей персональные данные;

– контроль за соблюдением работниками Общества требований настоящего Положения;

– проведение обучений для работников Общества в целях ознакомления с требованиями настоящего Положения;

– сбор и анализ статистических данных об Актуальных угрозах безопасности, характерных для Общества;

– внесение предложений руководителю Общества о необходимости проведения оценки достаточности принятых мер по защите информации, содержащей персональные данные, предложений по внесению изменений во внутренние документы Общества, регламентирующие деятельность Общества по защите информации, содержащей персональные данные, предложений по иным вопросам, связанным с деятельностью Общества по защите информации, содержащей персональные данные.

Определение порядка передачи персональных данных:

1) Информация, содержащая персональные данные, может быть передана третьим лицам по письменному запросу третьего лица и только с письменного разрешения руководителя Общества, при условии соблюдения требований действующего законодательства:

– по требованию органов государственной власти и местного самоуправления, государственных, надзорных и контролирующих органов, а также участников Общества в соответствии с действующим законодательством;

– работникам Общества в соответствии с учредительным документом Общества;

– другим физическим и юридическим лицам на основании гражданско-правовых договоров, заключенных между ними и Обществом, при условии наличия в этих договорах обязательств по соблюдению режима конфиденциальности в отношении информации, ответственности за разглашение этой информации или заключения с ними отдельного договора о конфиденциальности.

2) При передаче персональных данных Общество должно соблюдать следующие требования:

– не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных за исключением случаев, когда это необходимо в целях

предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных законодательством Российской Федерации;

– предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они получены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

– передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций;

Обеспечение сохранности носителей информации.

Режим сохранности материальных носителей информации.

1) Доступ к материальным носителям информации, содержащей персональные данные, имеют только те работники Общества, которым такая информация необходима для выполнения должностных обязанностей.

2) Доступ к материальным носителям информации, содержащей персональные данные, посторонним лицам запрещен.

3) Рабочие места работников размещаются таким образом, чтобы исключить возможность обозрения находящихся на столе документов, а также мониторов компьютеров посторонними лицами.

4) Материальные носители, содержащие персональные данные должны храниться в специальных сейфах или запирающихся металлических шкафах.

5) Персональные данные, обработка, которых осуществляется в различных целях, хранятся раздельно.

Режим сохранности машинных носителей информации.

Учет машинных носителей информации осуществляется лицом, ответственным за информационную безопасность, путем ведения журнала учета машинных носителей информации. В журнале учета машинных носителей информации каждый машинный носитель информации Общества закрепляется за ответственным работником, который не вправе передавать закрепленный за ним машинный носитель информации третьим лицам.

Запрещается копирование файлов с информацией, содержащей персональные данные, и хранение их на жестких дисках рабочих станций (компьютеров, ноутбуков), съемных машинных носителях информации, других устройствах, способных накапливать и хранить информацию в электронном виде, за исключением случаев, описанных в настоящем Положении.

Общество приобретает съемные машинные носители информации, способные накапливать и хранить информацию, для использования работниками Общества в рабочих целях. Такие машинные носители должны проверяться на наличие вирусов и вредоносных программ на регулярной основе.

Установление режима использования Криптографических ключей.

Общество осуществляет учет Криптографических ключей путем закрепления права их использования за определенным должностным лицом в Реестре прав доступа. При этом каждый Криптографический ключ используется только руководителем Общества или работником, должность которого определена в Реестре прав доступа.

Передача Криптографических ключей, в случае если Криптографический ключ размещен на материальном носителе, не допустима.

Криптографические ключи должны использоваться Обществом в соответствии с технической документацией.

Установление режима обеспечения безопасности помещений.

В целях исключения возможности неконтролируемого проникновения или пребывания в помещениях, в которых обрабатывается и (или) хранится информация, содержащая персональные данные, посторонних лиц Общества устанавливает режим обеспечения безопасности этих помещений.

Требования к помещениям, в которых обрабатывается и (или) хранится информация, содержащая персональные данные, устанавливаются в локальном нормативном акте по обеспечению безопасности помещений, которое утверждается руководителем.

Порядок доступа в помещения, в которых ведется обработка персональных данных.

1) Для помещений, в которых обрабатываются персональные данные (далее - Помещения), обеспечивается режим безопасности, при котором исключается возможность неконтролируемого проникновения и пребывания в этом помещении посторонних лиц.

2) Доступ в Помещения имеют работники, непосредственно работающие в этих помещениях.

3) Руководитель и замещающие лица могут находиться в Помещениях в любое время, в том числе в нерабочие и праздничные дни.

4) Помещения в нерабочее время должны закрываться на ключ.

5) Вскрытие и закрытие Помещений производится лицами, имеющими право доступа.

6) Уборка Помещений должна производиться в присутствии лиц, имеющих право доступа.

7) Перед открытием Помещений лица, имеющие право доступа в помещения, обязаны:

- провести внешний осмотр с целью установления целостности двери и замка;
- открыть дверь и осмотреть Помещение, где хранятся материальные носители.

8) Перед закрытием Помещений по окончании рабочего дня лица, имеющие право доступа в помещения, обязаны:

- убрать материальные носители персональных данных в шкафы или сейфы и закрыть их;
- отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;
- закрыть окна.

9) Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, проводится руководителем Общества.

Обнаружение фактов несанкционированного доступа к персональным данным, а также фактов нарушения работниками режима конфиденциальности и принятие мер.

Общество принимает меры по обнаружению фактов несанкционированного доступа путем:

– установления обязанности работников сообщать о фактах, свидетельствующих о несанкционированном доступе к информации, содержащей персональные данные, в том числе о фактах несанкционированного проникновения в помещения, в которых обрабатывается и(или) хранится информация, содержащая персональные данные;

– применения технических средств обнаружения фактов несанкционированного доступа в информационную систему.

Каждый факт несанкционированного доступа фиксируется лицом, ответственным за информационную безопасность, в определенном им порядке.

По всем фактам нарушений работниками режима конфиденциальности должны быть проведены расследования, в ходе которых определен круг лиц, виновных в этих нарушениях и причастных к ним, а также причины и условия, способствовавшие совершению данных нарушений. К проведению расследования привлекается лицо, ответственное за информационную безопасность.

По каждому факту несанкционированного доступа к персональным данным, а также факту нарушения работниками режима конфиденциальности проводится анализ причин и условий, совершению указанных фактов, по результатам которого составляется заключение, содержащее дополнительные меры по защите персональных данных, а также план по реализации данных мер, включающий сроки их реализации и ответственных лиц.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, с момента выявления такого инцидента самим Обществом или уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом, Общество уведомляет уполномоченный орган по защите прав субъектов персональных данных:

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

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

Уведомление направляется одним из следующих способов:

– на бумажном носителе по адресу Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций;

– в форме электронного документа посредством заполнения специализированной формы, размещенной на Портале персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в информационно-телекоммуникационной сети «Интернет», после прохождения процедуры идентификации и аутентификации посредством федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» и подписывается электронной подписью в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Технические меры по защите персональных данных:

Приобретение и установка антивирусного программного обеспечения. Обязательным условием для приобретения антивирусного программного обеспечения является наличие лицензии. Антивирусное программное обеспечение должно регулярно обновляться в соответствии с последней версией. Антивирусное программное обеспечение устанавливается на все персональные компьютеры информационной системы Общества.

Создание учетных записей для работников Общества. Каждому пользователю информационной системы Общества, работающему с информацией, содержащей персональные данные, присваиваются личная учетная запись, для входа в которую устанавливается пароль. Пароль для входа в учетную запись не может совпадать с паролем для входа в учетные записи иных работников Общества. Пароль для входа в учетную запись не может передаваться третьим лицам, за исключением случаев, установленных настоящим Положением.

Установление режима защиты сетевого взаимодействия. Обмен данными между элементами информационной системы Общества и другими компьютерами (рабочими станциями, серверами) должен быть организован через защищенные соединения, организованные с использованием протоколов IPSec с проверкой подлинности и шифрованием IP-пакетов.

Осуществление Резервного копирования информации, содержащей персональные данные.

Ограничение доступа к Информационно-коммуникационной сети Интернет.

Пользователям информационной системы Общества (учетным записям пользователей), работающим с информацией, содержащей персональные данные, может быть ограничен доступ к сети Интернет и средствам электронной почты.

Применение технических средств, обеспечивающих восстановление модифицированной или уничтоженной вследствие несанкционированного доступа информации, содержащей персональные данные.

Проведение оценки эффективности принятых мер по защите информации, содержащей персональные данные.

Оценка эффективности принятых мер по защите информации, содержащей персональные данные, может проводиться Обществом самостоятельно или с привлечением сторонней организации.

Оценка эффективности принятых мер по защите информации, содержащей персональные данные, проводится по результатам внутренней проверки, проводимой лицом, ответственным за информационную безопасность.

Приказом руководителя утверждаются периодичность проведения проверок (но не реже одного раза в год), сроки проведения плановых проверок, а также их содержание.

По результатам проведения проверок составляется письменный отчет, который должен содержать:

– сведения обо всех фактах несанкционированного доступа к информации, содержащей персональные данные, нарушения работниками режима конфиденциальности;

– предложения по внесению изменений в систему защиты информации, содержащей персональные данные, и представляет руководителю Общества заключение о проведении оценки достаточности принятых мер по защите информации, содержащей персональные данные.

В случае подтверждения недостаточности принятых мер по защите информации, содержащей персональные данные, руководитель Общества принимает решение о необходимости применения дополнительных мер по изменению системы защиты информации, содержащей персональные данные, в целях приведения ее к достаточному уровню.

Контроль за соблюдением работниками Общества требований, предъявляемых к ним и установленных настоящим Положением, осуществляется лицом, ответственным за информационную безопасность.

7. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях защиты персональных данных, хранящихся у Общества, субъект персональных данных имеет право на:

- требовать от Общества уточнения его персональных данных, 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 законом меры по защите своих прав;
- требовать перечень своих персональных данных, обрабатываемых Обществом и информацию об источнике их получения;
- получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.
- в любое время отозвать свое согласие на обработку персональных данных, представив оператору письменный отзыв согласия на обработку по адресу: 143006, Московская область, Одинцовский городской округ, г. Одинцово, ул. Маковского, д. 26, помещ. 39 или на адрес электронной почты: info@mkkbestway.ru.

Для реализации вышеуказанных прав субъект персональных данных, может в порядке, установленном ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», обратиться в Общество с соответствующим запросом. Для выполнения таких запросов представитель Общества устанавливает личность субъекта персональных данных и при необходимости запрашивает дополнительную информацию.

Если субъект персональных данных считает, что Общество осуществляет обработку его персональных данных с нарушением требований законодательства о персональных данных или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Общества в порядке, предусмотренном законодательством Российской Федерации.

В целях обеспечения достоверности персональных данных субъект персональных данных обязан при заключении договора предоставить Обществу полные и достоверные данные о себе.

8. ПРАВА И ОБЯЗАННОСТИ ОБЩЕСТВА КАК ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

Общество в соответствии с Законом о персональных данных в том числе, но не исключительно, исполняет следующие обязанности:

- предоставляет субъекту персональных данных или его представителю по их просьбе информацию, предусмотренную Законом о персональных данных, в том числе о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с этими персональными данными;

– в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя дает в письменной форме мотивированный ответ, содержащий ссылку на положение Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», являющееся основанием для такого отказа;

– разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку, если в соответствии с федеральным законом предоставление персональных данных и (или) получение Обществом согласия на обработку персональных данных являются обязательными;

– в случае получения персональных данных не от субъекта персональных данных предоставляет субъекту персональных данных (за исключением установленных Законом о персональных данных случаев) до начала обработки таких персональных данных информацию, предусмотренную Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся за пределами территории Российской Федерации, не допускаются, за исключением случаев, указанных в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– вносит необходимые изменения в персональные данные в случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, а также уведомляет об этом субъекта персональных данных или его представителя и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

– уничтожает персональные данные в случае представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, а также уведомляет об этом субъекта персональных данных или его представителя и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

– прекращает обработку персональных данных при достижении целей их обработки;

– осуществляет обезличивание и передачу обезличенных персональных данных по требованию Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации о предоставлении обезличенных данных в порядке, установленном Постановлением Правительства Российской Федерации от 1 августа 2025 г. № 1154 "Об утверждении требований к обезличиванию персональных данных, методов обезличивания персональных данных и Правил обезличивания персональных данных".

Общество в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в том числе, но не исключительно, имеет право:

– поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора;

– продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в случае отзыва субъектом персональных данных согласия на обработку персональных данных;

– мотивированно отказать субъекту персональных данных в выполнении повторного запроса на предоставление необходимой информации и ознакомления с обрабатываемыми персональными данными, не соответствующего условиям, предусмотренным Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– осуществлять обработку персональных данных в форме обезличивания в порядке, установленном локальным нормативным актом Общества.

9. ВНУТРЕННИЙ КОНТРОЛЬ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящий раздел устанавливает основания, порядок и формы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным в Обществе.

Целями осуществления внутреннего контроля являются:

- оценка общего состояния выполнения требований по защите персональных данных, закрепленных в нормативно-правовых актах, в том числе в локальных актах Общества;

- соответствие обработки персональных данных Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Общества в отношении обработки персональных данных, локальным актам Общества;

- выявление и предотвращение нарушений в сфере персональных данных.

Порядок осуществления внутреннего контроля.

Внутренний контроль соответствия обработки персональных данных установленным требованиям осуществляется путем проведения проверок. Проверки проводятся лицом, ответственным за организацию обработки персональных данных.

В Обществе выделяют два типа проверок: плановые и внеплановые.

Плановые проверки проводятся не реже одного раза в год. Лицо, ответственное за проведение проверки, проверяемый период, срок проведения проверки устанавливается приказом руководителя Общества. Общий срок проверки не должен превышать 20 (двадцать) рабочих дней, при необходимости может быть продлен приказом руководителя, но не более чем на 10 (десять) рабочих дней.

Непосредственно перед проведением плановой проверки, за пять рабочих дней лицо, ответственное за проведение проверки, направляет уведомление структурным подразделениям Общества, в которых планируется проведение внутреннего контроля.

Внеплановые внутренние проверки проводятся в следующих случаях:

- по результатам расследования выявленных нарушений требований законодательства в сфере персональных данных;

- по результатам контрольно-надзорных мероприятий, проводимых уполномоченными органами в сфере защиты персональных данных.

Внутренние проверки представляют собой комплекс мероприятий, состоящий из следующих этапов:

- подготовка к проведению внутренней проверки;
- сбор информации, свидетельств проверки;
- анализ соответствия полученной в ходе проверки информации контрольным параметрам (приложение № 1);
- подготовка и формирование заключения по проверке.

В ходе подготовки к проведению проверки лицо, ответственное за проведение проверки, определяет границу и область, подвергающиеся проверке, перечень контрольных параметров, объекты контроля (подразделения, процессы, информационные системы персональных данных и т.п.), состав сотрудников/участников, привлекаемых для проведения проверки, сроки и этапы проведения проверки.

Сбор информации, свидетельств проверки включает в себя анализ организационно-распорядительных и регламентирующих документов по обработке и защите персональных данных, опрос сотрудников, участвующих в процессах обработки персональных данных, обслуживании и эксплуатации информационных систем персональных данных, наблюдение процедур обработки персональных данных. В результате происходит сопоставление с контрольными параметрами для формирования заключения по проверке.

Внутренние проверки проводятся непосредственно на месте обработки персональных данных путем опроса, осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

Лицо, ответственное за проведение проверки, вправе:

- привлекать к проведению проверки сотрудников Общества;
- запрашивать у сотрудников Общества всю необходимую информацию;
- принимать меры по устранению выявленных нарушений выполнения требований к защите персональных данных;
- вносить предложения о совершенствовании организационно-правового регулирования обеспечения безопасности персональных данных при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в сфере обработки персональных данных.

Фиксирование результатов внутренних проверок осуществляется в Журнале проведения проверок.

10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Лица, виновные в нарушении порядка обращения с персональными данными, несут предусмотренную законодательством Российской Федерации ответственность.

Дисциплинарная ответственность:

Разглашение персональных данных субъекта персональных данных Общества, то есть передача посторонним лицам, не имеющим к ним доступа; публичное раскрытие; утрата документов и иных носителей, содержащих персональные данные работника; иные нарушения обязанностей по их защите, обработке и хранению, установленных настоящим Положением, а также иными локальными нормативными актами Общества, лицом,

ответственным за получение, обработку и защиту персональных данных работника, влекут наложение на него дисциплинарного взыскания - выговора, увольнения (пп. «в» п.6 ч. 1 ст. 81 Трудового кодекса РФ).

В случае причинения ущерба Обществу работник, имеющий доступ к персональным данным сотрудников и совершивший указанный дисциплинарный поступок, несет полную материальную ответственность в соответствии с п. 7 ч. 1 ст. 243 Трудового кодекса РФ.

Административная ответственность:

За нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11 КоАП РФ).

За разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

Уголовная ответственность – за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящее Положение вступает в силу с момента его утверждения приказом руководителя Организации и действует без ограничения срока, до утверждения Положения в новой редакции.

Настоящее Положение является обязательным для исполнения всеми работниками Общества, имеющими доступ к персональным данным, и доводится до их сведения персонально под подпись.

Приложение № 1

ПЕРЕЧЕНЬ

контрольных параметров проверок в области обработки и обеспечения безопасности персональных данных

№ п/п	Контрольные параметры и объекты проверок
1	Соответствие установленных в перечне персональных данных категорий персональных данных фактически обрабатываемым в Обществе
2	Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников
3	Подтверждение факта ознакомления с локальными актами Общества в сфере обработки и обеспечения безопасности персональных данных
4	Наличие в договорах с третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных
5	Наличие законных целей и оснований обработки всех категорий персональных данных
6	Актуальность перечня должностей работников, замещение которых предусматривает осуществление обработки персональных данных
7	Актуальность перечня мест хранения материальных носителей персональных данных
8	Выборочные проверки сотрудников на предмет знания организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных
9	Соблюдение сроков хранения и порядка уничтожения персональных данных
10	Соблюдение процедур и сроков подготовка ответов на обращения субъектов персональных данных
11	Необходимость актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных.