УТВЕРЖДАЮ
Генеральный директор
ЗАО «ПармаТел»
В.Н. Алексеевич

«29» декабря 2011 г.

Приказ ЗАО «ПармаТел» от
«29» декабря 2011г. № 70

ПОЛОЖЕНИЕ
Об обработке персональных данных в ЗАО «ПармаТел»

Сыктывкар 2011 г.

Содержание

1. Основные понятия и сокращения

В настоящем положении используются следующие основные понятия и сокращения:

- ПДн — персональные данные
- ИСПДн — информационная система персональных данных
- информация - сведения (сообщения, данные) независимо от формы их представления.
- документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.
- персональные данные работника - любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;
- обработка персональных данных - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников Организации;
- конфиденциальность персональных данных - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;
- распространение персональных данных - действия, направленные на передачу персональных данных работников определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным работников каким-либо иным способом;
- использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом Организации в целях принятия решений или совершения иных

действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, в том числе их передачи;

- уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников или в результате которых уничтожаются материальные носители персональных данных работников;

- обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику;

- общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

- «клиент/контрагент» - физическое или юридическое лицо, пользующееся услугами или заключившее договор с организацией.

- 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.

2. Общие положения

2.1. Настоящее Положение по обработке персональных данных (далее - Положение) ЗАО «ПармаТел» (далее - «Общество») разработано в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Правилами внутреннего трудового распорядка Общества.

2.2. Цель разработки Положения:

- определение порядка обработки персональных данных работников, клиентов/контрагентов Общества, персональные данные которых подлежат обработке, на основании полномочий оператора;
- обеспечение защиты прав и свобод работников, клиентов/контрагентов Общества, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- установление ответственности должностных лиц, имеющих доступ к персональным данным, лиц обрабатывающих персональные данные за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2.3. Настоящее Положение вступает в силу с момента его утверждения Генеральным директором Общества и действует бессрочно, до замены его новым Положением.

2.4. Все изменения в Положение вносятся приказом.

2.5. Работники Общества, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под роспись.

2.6. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Общества, если иное не определено законом.

3. Цели и задачи обработки персональных данных

3.1. Обработка персональных данных в Обществе осуществляется с целью содействия субъектам персональных данных в осуществлении их трудовой деятельности, обеспечения личной безопасности, исполнения договорных обязательств, а также наиболее полного исполнения Обществом

обязательств и компетенций в соответствии с Трудовым кодексом РФ и другими нормативно-правовыми актами в сфере трудовых отношений.

3.2. Обработка персональных данных сотрудников Общества осуществляется для решения следующих задач:

- учет информации о кадровом составе;
- формирования отчетов;
- назначение и начисление зарплаты и иных выплат;
- бухгалтерский учет и контроль финансово-хозяйственной деятельности Общества и исполнения финансовых обязательств по заключенным договорам;
- предоставление доступа к ресурсам сети Интернет;
- предоставление субъекту сведений о его трудовой деятельности в Обществе в период трудовых отношений и после увольнения;
- поддержание контактов с субъектом персональных данных по вопросам трудовой деятельности субъекта;
- поддержание контактов с законными представителями субъекта персональных данных;
- анализ персональных данных соискателей на должности в Обществе;
- решение социальных вопросов в интересах субъекта персональных данных;
- иные задачи, необходимые для повышения качества и эффективности деятельности Общества.

3.3. Обработка персональных данных контрагентов\клиентов в Обществе осуществляется для решения следующих задач:

- осуществления коммерческой деятельности;
- поддержание контактов с субъектом персональных данных по вопросам исполнения договорных обязательств;
- иные задачи, необходимые для повышения качества и эффективности деятельности Общества .

3.4. В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

4. Состав персональных данных, обрабатываемых в Обществе

4.1. Состав персональных данных, обрабатываемых в Обществе, определяется документом «Перечень персональных данных, подлежащих защите в информационных системах персональных данных ЗАО «ПармаТел» и соответствует целям и задачам обработки персональных данных в соответствии с разделом 3 настоящего Положения.

5. Права субъектов

5.1. Сотрудник Общества, либо лицо, поступающее на работу в Общество, в стадии заключения Трудового Договора, являясь субъектом персональных данных, своей волей и в своем интересе принимает решение о предоставлении своих персональных данных и дает письменное согласие на их обработку (приложение 1). Согласие не требуется в случаях, описанных в пункте 7.2.4. настоящего Положения.

5.2. Клиенты/контрагенты (физические лица), персональные данные которых обрабатывает организация без заключения с ними договора (например: доверенность, резюме), должны дать согласие на обработку их персональных данных. При условии дополнения текста фразой - «На обработку своих персональных данных в объеме и целях, указанных в доверенности/резюме согласен», дополнительного согласия не требуется.

5.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных по письменному заявлению на имя Генерального директора Общества с указанием причин отзыва. При подаче заявления необходимо предъявить основной документ удостоверяющий личность. После отзыва согласия все персональные данные, содержащиеся в ИСПДн с использованием средств автоматизации в течение трех дней уничтожаются без возможности восстановления, о чем субъект персональных данных уведомляется в письменной форме. Данные находящиеся на бумажных носителях передаются в архив и хранятся в течение сроков, установленных законодательством.

5.4. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту, а также на ознакомление с такими персональными данными. Копировать и делать выписки персональных данных работника, содержащихся в личном деле, разрешается исключительно в служебных целях с письменного разрешения руководителя организации.

5.5. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, требовать извещения Обществом всех лиц,

которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.6. Субъект персональных данных имеет право получать от оператора сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ, о сроках обработки персональных данных, в том числе о сроках их хранения, сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

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

5.8. Субъект персональных данных имеет право получать доступ к своим персональным данным и знакомиться с ними, включая право на безвозмездное получение копий любой записи, содержащей его персональные данные.

5.9. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при получении письменного запроса субъекта персональных данных или его законного представителя. Письменный запрос должен быть адресован на имя руководителя организации, содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. При подаче заявления субъект персональных данных должен предъявить основной документ удостоверяющий личность для проверки сведений указанных в заявлении.

5.10. Факты предоставления персональных данных по запросам регистрируются в журнале учета обращений субъектов ПДн о выполнении их законных прав.

5.11. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований федеральных законов или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

5.12. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6. Обязанности работодателя и сотрудников Общества, работающих с персональными данными

6.1. Сотрудники Общества, допущенные к персональным данным, несут ответственность за точное выполнение требований, предъявляемых к ним в целях обеспечения сохранности персональных данных. До получения доступа к работе, связанной с обработкой персональных данных, они обязаны изучить настоящее Положение и дать письменное обязательство о сохранении персональных данных (конфиденциальной информации).

6.2. Сотрудники Общества, допущенные к персональным данным должны:

6.2.1. Не разглашать персональные данные. О ставших им известной утечке персональных данных сообщать непосредственному руководителю и администратору по безопасности информации.

6.2.2. Знакомиться только с теми документами и выполнять только те работы, к которым они допущены.

6.2.3. Строго соблюдать правила пользования документами, содержащих персональные данные. Не допускать их необоснованного предоставления третьим лицам.

6.2.4. Выполнять требования настоящего положения, не допускать возможность ознакомления с персональными данными посторонних лиц, включая и других сотрудников Общества, не имеющих к указанным документам прямого отношения.

6.2.5. При ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения.

6.3. Обязанности работодателя:

6.3.1. Обеспечивает конфиденциальность персональных данных. Обеспечение конфиденциальности персональных данных не требуется в случае обезличенных персональных данных и в отношении общедоступных персональных данных.

6.3.2. До начала выполнения договорных обязанностей сотрудником довести до его сведения соответствующие положения документов по защите конфиденциальной информации, разглашение которой может нанести ущерб интересам Общества и нарушить требования действующего законодательства РФ в области «Персональных данных».

6.3.3. Предоставляет сотруднику необходимые условия для выполнения требований по охране конфиденциальных сведений, к которым допускается сотрудник.

6.3.4. Проводит разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

6.3.5. Производить контроль использования сотрудниками Общества информационных ресурсов, а также использования ими технических средств обработки, хранения и передачи информации, предоставленных Обществом для выполнения сотрудником договорных обязанностей, в соответствии с требованиями действующего законодательства РФ. Периодичность, сроки и методы контроля, определяются Генеральным директором Общества

7. Порядок сбора, хранения, использования и передачи персональных данных

7.1. Сбор персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений, в сфере оказания услуг связи, а также настоящим Положением и приказами Генерального директора Общества.

7.2. Порядок получения персональных данных

7.2.1. Все персональные данные следует получать непосредственно у субъекта ПДн. Если персональные данные возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее или от него должно быть получено письменное согласие. Должностное лицо Общества должно сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение.

7.2.2. Общество не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

7.2.3. Общество не имеет права получать и обрабатывать персональные данные субъекта ПДн о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами РФ.

7.2.4. Общество вправе обрабатывать персональные данные субъектов только с их письменного согласия, за исключением следующих случаев:

- обработка персональных данных осуществляется по требованию полномочных государственных органов и на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных, т. е. в качестве основания для обработки выступает договор, заключенный между субъектом персональных данных и оператором, который косвенно (но не прямо! – если такого положения не содержится в условиях заключенного договора) подтверждает согласие субъекта на обработку таких данных;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи;

- персональные данные являются общедоступными.

7.2.5. Субъект ПДн, принимаемый на работу, предоставляет Обществу достоверные сведения о себе. Специалист по кадрам проверяет достоверность сведений работника, сверяя данные, предоставленные им, с имеющимися документами.

7.2.6. В соответствии со ст. 86, гл. 14 ТК РФ в целях обеспечения прав и свобод человека и гражданина, Общество и его представители при обработке персональных данных работника должны соблюдать следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- объем и содержание, обрабатываемых персональных данных должны соответствовать Конституции Российской Федерации, Трудовому кодексу Российской Федерации и иным федеральным законами РФ;

- при принятии решений, затрагивающих интересы субъекта, Общество не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения;

- защита персональных данных субъекта от неправомерного их использования или утраты, обеспечивается Обществом за счет его средств, в порядке, установленном федеральными законами РФ;

- работники, и их представители должны быть ознакомлены под расписку с документами Общества, устанавливающими порядок обработки персональных данных, с перечнем собираемых и используемых сведений, с целями и задачами сбора, хранения, использования персональных данных, а также об их правах и обязанностях в этой области;

- субъект не должен отказываться от своих прав на сохранение и защиту персональных данных.

7.3. Ввод персональных данных в автоматизированные ИСПДн Общества осуществляется сотрудником в соответствии с его должностными обязанностями. Сотрудники, осуществляющие ввод и обработку данных с использованием автоматизированных ИСПДн Общества, несут ответственность за полноту и достоверность введенной информации и не должны вносить изменения, противоречащие информации, полученной непосредственно от субъекта персональных данных.

7.4. Хранение и обработка персональных данных в автоматизированных ИСПДн осуществляется на оборудовании Общества с использованием специализированного программного обеспечения, отвечающего требованиям информационной безопасности.

7.4.1. Трудовые договора, копии документов, карточки формы Т-2 в бумажном виде хранятся в отдельных делах, трудовые книжки – в запираемом шкафу в кабинете секретаря Общества.

7.4.2. Персональные данные могут храниться в бумажном и (или) электронном виде с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных. Право на обработку персональных данных предоставляется сотрудникам структурных подразделений и (или) должностным лицам Общества, определенным настоящим Положением, а также «Перечнем сотрудников, допущенных к обработке персональных данных ЗАО «ПармаТел», распорядительными документами или письменными указаниями Генерального директора Общества.

7.4.3. В случае если для научных, прикладных исследований, для решения задач статистики необходимо сохранить персональные данные, которые больше не используются в тех целях, ради которых они были собраны, эти данные могут сохраняться преимущественно в обезличенной форме в виде анонимных сведений.

7.4.4. На сайте Общества могут быть размещены общедоступные персональные данные лиц, перечень которых определяется перечнем сведений ПДн и согласием субъекта персональных данных на момент передачи в открытые источники.

7.5. При передаче персональных данных Общества соблюдает следующие требования:

- не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законодательством (ст. 49 п.5 Закон РФ "О средствах массовой информации");

- не сообщать персональные данные субъекта третьим лицам в коммерческих целях без его письменного согласия. Обработка персональных данных субъекта в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия;

- предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Данное положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные обрабатываемые в Обществе, которые необходимы для выполнения конкретных функций возложенных на этих лиц;

- передавать персональные данные субъекта, законным представителям субъектов в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

7.6. Порядок передачи информации, содержащей персональные данные, обрабатываемые Обществом, внутри Общества определяется должностными обязанностями сотрудников или внутренними распорядительными документами Общества.

7.7. В соответствии с законодательством Российской Федерации персональные данные, обрабатываемые Обществом, могут быть переданы правоохранительным, судебным органам и другим учреждениям, которые имеют на это право на основании федерального законодательства, а также в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороноспособности страны и безопасности государства без получения согласия субъекта ПДн.

7.8. Решение о передаче информации, содержащей персональные данные, обрабатываемые Обществом, третьим лицам, за исключением указанного в пункте 7.6. настоящего Положения, принимается Генеральным директором Общества только на основании мотивированного письменного запроса, если иное не предусмотрено договором или федеральным законодательством. Мотивированный запрос должен быть подписан уполномоченным должностным лицом, содержать указание цели и правовое основание предоставления персональных данных, срок предоставления этой информации, если иное не установлено федеральными законами РФ.

7.9. В соответствии с целями обработки ПДн указанных в разделе 3 настоящего Положения для представления интересов работника ПДн передаются в налоговые органы, в Пенсионный фонд РФ, ФОМС, центр занятости населения (по запросу в бумажном виде) и в банк.

8. Доступ к персональным данным субъектов

8.1. Доступ работников Общества к персональным данным осуществляется в соответствии со списками, которые утверждаются Генеральным директором Общества. Генеральный директор, разрешающий доступ работника своего подразделения к носителю персональных данных, несет персональную ответственность за данное разрешение.

8.2. Ознакомление лиц с персональными данными субъектов должно осуществляться только по необходимости и в тех объемах, которые необходимы для выполнения возложенных на них функций.

8.3. Доступ к персональным данным субъектов осуществляется на основании приказа, при этом исключен допуск посторонних лиц.

9. Порядок маркировки и учета электронных носителей ПДн

9.1. Электронные носители (магнитные ленты, съемные магнитные диски, дискеты, флеш-накопители, оптические диски), предназначенные для обработки или хранения на них ПДн, берутся на учет (приложение 2) до записи на них персональных данных. Журнал учета электронных носителей ведётся ответственным за обеспечение безопасности ПДн Общества. Журнал должен быть прошит, опечатан и учтен в секретариате Общества.

9.2. При постановке на учет носителя ПДн их маркировка производится на нерабочей поверхности, посредством нанесения записей механическим путем или красящим веществом, имеющим хорошую механическую стойкость.

9.3. Доступ к носителям ПДн разрешается лицам, допущенным к обработке ПДн, и только в те интервалы рабочего времени, которые отведены для решения указанной задачи в графике рабочего времени.

9.4. Работа с носителями ПДн производится на рабочих местах лиц, допущенных к обработке ПДн.

9.5. Персональные компьютеры, используемые для обработки ПДн, подлежат инвентарному учету. В этих случаях, для контроля доступа к

аппаратной части компьютера, крышки указанных компьютеров опечатываются ответственным за обеспечение безопасности ПДн с проставлением печати предприятия и образцами подписей ответственного за обеспечение безопасности ПДн и работника, допущенного к обработке ПДн на данном рабочем месте.

10.Обработка ПДн, осуществляемая без использования средств автоматизации

10.1. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

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

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

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

10.5. Необходимо обеспечивать раздельное хранение носителей ПДн, обработка которых осуществляется в различных целях.

10.6. При хранении носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

11.Обеспечение безопасности персональных данных

11.1. Лица, получившие доступ к персональным данным, обязаны не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

11.2. В случае, если Общество на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

11.3. Обществом и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

11.4. Меры по обеспечению конфиденциальности персональных данных, принимаемые в Обществе, должны включать, но не ограничиваясь этим, следующее:

- определение перечня персональных данных и мест обработки таких данных;
- ограничение доступа к персональным данным, их носителям, путем установления порядка обращения с этими данными и носителями, контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к персональным данным, и (или) лиц, которым такие данные были предоставлены или переданы;
- регулирование отношений по использованию персональным данным, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- учет носителей (документов), содержащих персональные данные.
- организационные меры безопасности:
    - инструктаж работников по правилам обеспечения безопасности обрабатываемых персональных данных;
    - учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;
    - мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок, разбирательств и составление заключений и принятие организационно-технических мер;
    - постоянный контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем внутренних аудитов);
- меры физической безопасности:
    - ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Приказом Генерального директора Общества устанавливается контролируемая зона предприятия, вводятся в действие Список помещений с ограниченным доступом и Список лиц, имеющих право посещать помещения предприятия с ограниченным доступом. Лица, не указанные в Списке, в том числе обеспечивающие техническое и бытовое обслуживание

(уборку, ремонт оборудования и технических средств), при наличии необходимости могут посещать помещения с ограниченным доступом в сопровождении ответственных лиц;

- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах контролируемой зоны;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

– технические меры безопасности:

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование защищенных каналов связи;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

12.Контроль выполнения работ по обеспечению безопасности персональных данных

12.1. Контроль выполнения работ по обеспечению безопасности персональных данных в Обществе (далее – Контроль) осуществляется путем проведения периодических контрольных мероприятий (в рамках внутренних аудитов) и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

12.2. В рамках проведения контрольных мероприятий выполняются:

- проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности персональных данных за истекший период;
- проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных;
- проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, фактическому состоянию;
- проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации;
- инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности персональных данных (при необходимости);
- проверка соответствия моделей угроз для информационных систем персональных данных условиям функционирования данных систем;
- проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональным данных действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

12.3. Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

12.4. Контрольные мероприятия проводятся как периодически в соответствии с планом и программой аудита, так и непланово по решению руководства Общества либо в случае возникновения инцидентов информационной безопасности.

12.5. Внутренние проверки в Обществе в обязательном порядке проводятся в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;
- халатность и несоблюдение требований к обеспечению безопасности персональных данных;

– несоблюдение условий хранения носителей персональных данных;
– использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

12.6. Задачами внутренней проверки являются:

– установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
– установление лиц, непосредственно виновных в данном нарушении;
– выявление причин и условий, способствовавших нарушению.
– Принятие мер по привлечению к ответственности виновных лиц, и устранению причин.

13.Совершенствование системы защиты персональных данных

13.1. Ежегодно ответственный по защите персональных данных направляет Генеральному директору Общества отчет о проделанной работе по обеспечению безопасности персональных данных, обрабатываемых в Обществе, вместе с перечнем предложений по совершенствованию системы защиты персональных данных.

13.2. Необходимость реализации мероприятий по совершенствованию системы защиты персональных данных может быть обусловлена:

– результатами проведенных аудитов и контрольных мероприятий;
– изменениями федерального законодательства в области персональных данных;
– изменениями структуры процессов обработки персональных данных в пенсионном фонде;
– результатами анализа инцидентов информационной безопасности;
– результатами мероприятий по контролю и надзору за обработкой персональных данных, проводимых уполномоченным органом;
– жалоб и запросов субъектов персональных данных.

13.3. На основании решения, принятого руководителем Общества по результатам рассмотрения ежегодного отчета и предложений по совершенствованию системы защиты персональных данных, ответственный по защите персональных данных составляет план работ по обеспечению безопасности персональных данных, обрабатываемых в Обществе, на следующий год.

14.Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

14.1. Работники Общества, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законами РФ.

Генеральный директор В.Н.Алекссевич