УТВЕРЖДАЮ

Директор

ООО «ВодоСнабжение»

_____В.Е. Карташов

«_01_» _____ 2018 г.

Положение о защите персональных данных работников, клиентов и контрагентов ООО «ВодоСнабжение»

1. Общие положения

1.1. Целью настоящего Положения является защита персональных данных работников, клиентов и контрагентов Общества с ограниченной ответственностью «ВодоСнабжение» ООО «ВодоСнабжение (далее «Общество») от несанкционированного доступа, неправомерного их использования или утраты.

1.2.Настоящее Положение разработано в соответствии с Конституцией РФ, Федеральным законом от 27.07.2006 № 152-ФЗ « О персональных данных», Федеральным законом № 149-ФЗ « Об информатизации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 15.09.2008 № 687 « Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными актами , действующими на территории Российской Федерации.

1.3. В настоящем Положении используются следующие термины и определения:

Оператор – Общество с ограниченной ответственностью «ВодоСнабжение (ООО ВодоСнабжение) –(далее Общество)., вступившее в договорные отношения с работником, с клиентом, контрагентом или оказывающее услуги физическому лицу, юридическому лицу или индивидуальному предпринимателю.

Клиент – физическое лицо, официальный представитель – физическое лицо юридического лица и индивидуального предпринимателя , вступившие в договорные отношения по оказанию услуг с Обществом.

Контрагент – физическое лицо, представитель – физическое лицо юридического лица и индивидуального предпринимателя , вступившие с обществом в договорные отношения.

Персональные данные Клиента – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Клиента, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, паспортные данные, социальное положение, имущественное положение, образование, профессия, специальность, занимаемая должность, доходы, ИНН, сведения ВУС, СНИЛС, сведения о трудовом и общем стаже, адрес электронной почты, телефон, место работы или учебы членов семьи и родственников, состав декларируемых сведений о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию, налоговый статус (резидент/нерезидент), иные сведения указанные заявителем.

Персональные данные Контрагента – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Контрагента, в том числе фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, паспортные данные, социальное положение, имущественное положение, образование, профессия, специальность, занимаемая должность, доходы, ИНН, сведения ВУС, СНИЛС, сведения о трудовом и общем стаже, адрес электронной почты, телефон, место работы или учебы членов семьи и родственников, состав декларируемых сведений о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию, иные сведения указанные заявителем.

Персональные данные Работника - информация, необходимая Обществу, как работодателю, в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о ра-

ботниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность, в том числе: фамилия, имя, отчество; образование; сведения о трудовом и общем стаже; сведения о составе семьи; паспортные данные; сведения о воинском учете; ИНН; налоговый статус (резидент/нерезидент); сведения о заработной платеработника; сведения о социальных льготах; специальность; занимаемая должность; адрес места жительства; телефон; место работы или учебы членов семьи и родственников; характер взаимоотношений в семье; содержание трудового договора; состав декларируемых сведений о наличии материальных ценностей; содержание декларации, подаваемой в налоговую инспекцию; иную, не указанную выше информацию, содержащуюся в личных делах и трудовых книжках сотрудников; информацию, являющуюся основанием к приказам по личному составу; информацию, содержащуюся в страховом свидетельстве обязательного пенсионного страхования, свидетельстве о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации, страховом медицинском полисе обязательного медицинского страхования граждан, медицинском заключении установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на работу в Общество; дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям.

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.

Субъект персональных данных – Работник, Клиент, Контрагент.

Защита персональных данных Работника, Клиента, Контрагента – деятельность Общества по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации.

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

Конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Подразделение – отдел информационной безопасности (ИБ) и режима «ООО»ВодоСнабжение»», либо сотрудник Общества, на которого возложены обязанности по обеспечению информационной безопасности и режима «ООО «ВодоСнабжение», в том числе обязанности по организации обработки персональных данных.

Подразделение по работе с персоналом – отдел по работе с персоналом «ООО»ВодоСнабжение» либо сотрудник Общества, на которого возложены обязанности по работе с персоналом.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.4. Персональные данные работников Общества относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законодательством Российской Федерации.

1.5. Действия настоящего Положения распространяется на всех Работников, Клиентов и Контрагентов Общества.

2. Обработка персональных данных

2.1. В целях обеспечения прав и свобод человека и гражданина Общество и (или) его представители при обработке персональных данных должны соблюдаться следующие общие требования:

2.1.1.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 РФ;

2.1.2.Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.1.3.Получение Обществом персональных данных может осуществляться как путем представления их самим работником, клиентом, контрагентом так и путем получения их из иных источников.

2.1.4.Персональные данные получаются Обществом непосредственно у самого работника, клиента, контрагента

2.1.5.Общество не имеет права получать и обрабатывать персональные данные работника, клиента, контрагента о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни работника, клиента, контрагента (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны Обществом только с его письменного согласия.

2.2. К обработке, передаче и хранению персональных данных могут иметь доступ:
Директор Общества; Руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения); при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения; сам работник, источник данных; другие сотрудники организации при выполнении ими своих служебных обязанностей.

2.3. Использование персональных данных возможно только в соответствии с целями, определившими их получение.
Персональные данные 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.

2.4. При идентификации клиента или контрагента Общества может затребовать предъявления документов, удостоверяющих личность и подтверждающих полномочия представителя.

2.5. При заключении договора, как и в ходе выполнения договора может возникнуть необходимость в предоставлении клиентом или контрагентом иных документов, содержащих информацию о нем.

2.6. После принятия решения о заключении договора или представления документов, подтверждающих полномочия представителя, а так же впоследствии, в процессе выполнения договора, содержащего персональные данные клиента или контрагента, так же будут относиться:
- договоры;
- приказы по основной деятельности;
- служебные записки;
- приказы о допуске представителей клиента, контрагента;
- другие документы, где включение персональных данных клиента или контрагента необходимо согласно действующему законодательству.

2.7. При передаче персональных данных Общество должно соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия работника, клиента, контрагента за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, клиента, контрагента а также в случаях, установленных законодательством Российской Федерации;
- не сообщать персональные данные в коммерческих целях без его письменного согласия; предупредить лиц, получающих персональные данные, о том, что эти данные могут быть

использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном законодательством Российской Федерации;

- разрешать доступ к персональным данным только специально уполномоченным лицам, определенным приказом директора Общества, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций; не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции; передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

2.7.1.Передача персональных данных от Общества и (или) его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

2.7.2.При передаче персональных данных внешним потребителям (в том числе и в коммерческих целях) Общество не должно сообщать эти данные третьей стороне без письменного согласия работника, клиента, контрагента за исключением случаев, установленных законодательством Российской Федерации.

2.7.3.Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

2.7.4. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

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

2.9.Период хранения и обработки персональных данных определяется в соответствии с Законом «О персональных данных». Обработка персональных данных начинается с момента поступления персональных данных в информационные системы персональных данных и прекращается:

- в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, Общество устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений, Общество в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных Общество уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;

- в случае достижения цели обработки персональных данных Общество незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, и уведомляет 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, Общество уведомляет также указанный орган;

- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Общество прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных Общество уведомляет субъекта персональных данных.

- в случае прекращения деятельности Общества.

2.10.Оператор 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 кон-

тректа, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом -ФЗ «О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона -ФЗ «О персональных данных».

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

2.12.В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

3. Создание, обработка и хранение персональных данных

3.1. Создание персональных данных работника.

Документы, содержащие персональные данные работника, создаются путем:

а) внесения сведений в учетные формы (на бумажных и электронных носителях);

б) получения оригиналов необходимых документов (трудовая книжка, личный листок по учету кадров, автобиография, медицинское заключение).

3.2. Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

3.2.1. При обработке персональных данных работника в целях их защиты и обеспечения прав и свобод человека и гражданина, а также при определении объема и содержания обрабатываемых персональных данных должны строго учитываться положения Конституции Российской Федерации, Трудового кодекса Российской Федерации и иных федеральных законов.

3.2.2. Обработка персональных данных работника осуществляется исключительно в целях:

а) обеспечения соблюдения законов и иных нормативных правовых актов;

б) содействия работникам в трудоустройстве;

в) обеспечения личной безопасности работников;

г) контроля количества и качества выполняемой работы;

д) обеспечения сохранности имущества работника и работодателя.

3.2.3. Все персональные данные работника следует получать у него самого, за исключением случаев, если их получение возможно только у третьей стороны.

3.2.4. Получение персональных данных работника у третьих лиц возможно только при уведомлении работника об этом заранее и с его письменного согласия.

В уведомлении работника о получении его персональных данных у третьих лиц должна содержаться следующая информация:

а) о целях получения персональных данных;

б) о предполагаемых источниках и способах получения персональных данных;

в) о характере подлежащих получению персональных данных;

г) о последствиях отказа работника дать письменное согласие на их получение.

3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, равно как и персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.2.6. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.2.7. Работники и их представители должны быть ознакомлены под расписку с докум ми работодателя, устанавливающими порядок обработки персональных данных работни также об их правах и обязанностях в этой области.

3.3. Сведения, содержащие персональные данные работника, включаются в его личн ло, карточку формы N Т-2, а также содержатся на электронных носителях информации, дос которым разрешен лицам, непосредственно использующим персональные данные работн служебных целях.

3.4. Хранение персональных данных в бухгалтерии:

а) персональные данные, содержащиеся на бумажных носителях, хранятся в запираемом ш установленном на рабочем месте бухгалтера;

б) персональные данные, содержащиеся на электронных носителях информации, хранятся бухгалтера.

3.4.1. Персональные данные, включенные в состав личных дел, хранятся в запира шкафу, установленном на рабочем месте инспектора по кадрам. Персональные данные, сод щиеся на электронных носителях информации, хранятся в ПК инспектора по кадрам.

3.4.2. Трудовая книжка, документы воинского учета, карточка формы N Т-2 хранятся пертом металлическом сейфе.

3.4.3. Доступ к ПК строго ограничен кругом лиц, определенных в п. 4.1 настоящего жения. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив пос течения установленного срока хранения.

3.5.Обработка персональных данных Клиента или Контрагента.

3.5.1.Персональные данные клиента или Контрагента относятся к категории конфид альной информации

3.5.2.В целях обеспечения прав и свобод человека и гражданина Оператор и его предс тели при обработке персональных данных Клиента или Контрагента обязаны соблюдать сле щие требования:

- обработка персональных данных должна осуществляться на законной и справедливо нове, исключительно в целях обеспечения соблюдения законов и иных нормативных вовых актов, содействия выполнения договорных обязательств в соответствии с зако тельством РФ
- обработка персональных данных осуществляется с согласия субъекта персональных да на обработку его персональных данных за исключением случаев, предусмотренных за дательством Российской Федерации, когда обработка персональных данных допуск без согласия субъекта персональных данных, при условии регламентации вопросов ботка персональных данных соответствующим законодательством Российской Федера
- обработка персональных данных должна ограничиваться достижением конкретных, за определенных и законных целей. Не допускается обработка персональных данных, вместимая с целями сбора персональных данных.
- Не допускается объединение баз данных, содержащих персональные данные, обработк торых осуществляется в целях, несовместимых между собой
- Обработке подлежат только персональные данные, которые отвечают целям их обрабо
- Содержание и объем обрабатываемых персональных данных должны соответствовать ленным целям обработке. Обрабатываемые персональные данные не должны быть точными по отношению к заявленным целям их обработки.
- При обработке персональных данных должны быть обеспечены точность персонал данных, их достаточность, а в необходимых случаях и актуальность по отношению к ц обработки персональных данных. Оператор должен принимать необходимые меры обеспечивать их принятие по удалению или уничтожению неполных или неточных дан
- Хранение персональных данных должно осуществляться в форме, позволяющей опр лить субъекта персональных данных, не дольше, чем этого требуют цели обработки пе нальных данных, если срок хранения персональных данных не установлен федераль законом, договором, стороной которого, выгодоприобретателем или поручителем по к рому является субъект персональных данных. Обрабатываемые персональные данные лежат уничтожению либо обезличиванию по достижении целей обработки или в случа

раты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

- Оператор не имеет права получать и обрабатывать персональные данные Клиента или Контрагента о его расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.
- Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда Клиента или Контрагента, затруднения реализации его прав и свобод.
- При принятии решений, затрагивающих интересы Клиента или Контрагента, Оператор не имеет права основываться на персональных данных Клиента или Контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.

3.5.3.При идентификации Клиента или Контрагента Общества может затребовать предъявления документов, удостоверяющих личность и подтверждающих полномочия представителя.

3.5.4.при заключении договора, как и в ходе выполнения договора может возникнуть необходимость в предоставлении Клиентом иных документов, подтверждающих информацию о нем.

3.5.5.После принятия решения о заключении договора или представления документов, подтверждающих полномочия представителя, а также впоследствии, в процессе выполнения договора, содержащего персональные данные Клиента или Контрагента, так же будут относиться:

- Договоры
- Приказы по основной деятельности
- Служебные записки
- Приказы о допуске представителей Контрагента
- Другие документы, где включены персональные данные Клиента или Контрагента необходимо согласно действующему законодательству

3.5.6.Оператор 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 контроля, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручении(оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ « О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗХ « О персональных данных»

3.5.7. Сведения о Клиентах и Контрагентах хранятся на бумажных и электронных носителях. Доступ к которым ограничен и регламентируется Обществом.

3.5.8.Период хранения и обработки персональных данных определяется в соответствии с Законом « О персональных данных». Обработка персональных данных начинается с момента поступления персональных данных в информационные системы персональных данных и прекращается:

- В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления. Общество устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений, Общество в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных Общество уведомляет субъекта персональных данных или его законного представителя, а в случае если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган.

- В случае достижения цели обработки персональных данных Общество незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий трех рабочихз дней с даты достижения цели обра-

ботки персональных данных, и уведомляет об этом субъекта персональных данных ил его ьзаконного представителя, а в случае, если обращение или запрос были направлен уполномоченным органом по защите прав субъектов персональных данных. Общество ув домляет также указанный орган

- В случае отзыва субъектом персональных данных согласия на обработку своих персонал ных данных Общество прекращает обработку персональных данных и уничтожает перс нальные данные в срок, не превышающий трез рабочих дней с даты поступления данно отзыва. Об уничтожении персональных данных Общество уведомляет субъекта перс нальных данных
- В случае прекращения деятельности Общества

4. Доступ к персональным данным

4.1. Список лиц, допущенных к обработке персональных данных (далее Список) и несущи ответственность в соответствии с законодательством Российской Федерации за нарушение прави обработки персональных данных, определяется и утверждается приказом директора Общества.

4.2. Подразделение по работе с персоналом при принятии на работу, увольнении или изме нении должностных обязанностей Работников не позднее чем в трехдневный срок вносит измене ния в список лиц, допущенных к обработке персональных данных, по согласованию с Подразд лением ИБ.

4.3. Подразделение ИБ, не реже одного раза в квартал, обязано проверять актуальност Списка. В случае выявления расхождений, Подразделение по работе с персоналом вносит измене ния в Список.

4.4. Работники Общества выполняют действия по обработке персональных данных в соот ветствии с возложенными на работников функциями.

4.5. Доступ к персональным данным предоставляется только лицам, замещающим должно сти из Списка.

4.6.Работники имеют доступ на ввод и коррекцию персональных данных в пределах, опре деленных должностными обязанностями.

4.7. Лица, получившие доступ к персональным данным, должны хранить в тайне известны им сведения конфиденциального характера и информировать Подразделение ИБ об утечке перс нальных данных, о фактах нарушения порядка обращения с ними, о попытках несанкционирован ного доступа к персональным данным.

4.8.Лица, получившие доступ к персональным данным, должны использовать эти данны лишь в целях, для которых они сообщены, обязаны соблюдать режим конфиденциальности и дат Обязательство о неразглашении персональных данных.

4.1. Другие организации.

4.1.1. Надзорно-контрольные органы имеют доступ к информации только в сфере свое компетенции.

4.1.2. Организации, в которые сотрудник может осуществлять перечисление денежны средств (страховые компании, негосударственные пенсионные фонды, благотворительные органи зации, кредитные учреждения), могут получить доступ к персональным данным работника тольк в случае его письменного разрешения.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением заявления ра ботника.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

5. Защита персональных данных

5.1.Все работники, имеющие доступ к персональным данным, обязаны подписать соглаше ние неразглашении персональных данных.

5.2.Защита персональных данных Клиентов или Контрагентов от неправомерного их ис пользования или утраты обеспечивается Оператором в порядке, установленном законодательством РФ.

5.3.Клиенты или Контрагенты до предоставления своих персональных данных должны иметь возможность ознакомится с настоящим Положением.

5.4.Защите подлежит:

- Информация о персональных данных субъектов
- Документы, содержащие персональные данные субъекта
- Персональные данные, содержащиеся на электронных носителях.

5.5.Оператор назначает ответственного за организацию обработки персональных данных.

5.6.Оператор издает документы, определяющие политику оператора в отношении обработки персональных данных, локальные акты, устанавливающие процедуры , направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

5.7.Оператора принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие 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 в соответствии со статьей 19 Федерального закона от 27.07.2006 года № 152-ФЗ « О персональных данных», в том числе

- Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных
- Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных
- Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации
- Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных
- Учет машинных носителей персональных данных
- Обнаружение фактов несанкционированного доступа к персональным данным и принятием мер
- Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним
- Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных
- Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных

5.8.Оператор осуществляет внутренний контроль и (или) аудит соответствия обработке персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ « О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

5.9.Оператор осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона , соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом.

5.10. Ознакамливает своих работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных , локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

5.11.Ответственные лица соответствующих подразделений, хранящих персональные да ные на бумажных носителях и машинных носителях информации, обеспечивают их защиту от н санкционированного доступа и копирования согласно «Положению об особенностях обработ персональных данных, осуществляемой без использования средств автоматизации», утвержде ному Постановлением правительства РФ от 15 сентября 2008 г. № 687.

6.Права и обязанности работника

6.1. Работники и их представители должны быть ознакомлены под расписку с документам Общества, устанавливающими порядок обработки персональных данных работников, а также с их правах и обязанностях в этой области.

6.2. В целях защиты персональных данных, хранящихся у работодателя, работник имее право:

- Требовать исключения или исправления неверных или неполных персональных данных
- На право получения копий любой записи, содержащей личные персональные данные

6.3. Работник обязан: передавать Обществу и(или) его представителю комплекс достовер ных, документированных персональных данных, состав которых установлен Трудовым кодексо Российской Федерации, своевременно сообщать Обществу об изменении своих персональны данных.

6.4. Работники ставят Общество в известность об изменении фамилии, имени, отчества, да ты рождения, что получает отражение в трудовой книжке на основании представленных докумен тов. При необходимости изменяются данные об образовании, профессии, специальности, при своении нового разряда и т.п.

7. Права и обязанности клиентов и контрагентов

7.1. В целях обеспечения защиты персональных данных, хранящихся у оператора, клиенты и контрагенты имеет право на:

7.1.1. Полную информацию о составе персональных данных и их обработке, в частности клиент или контрагент имеет право знать, кто и в каких целях использует или использовал инфор мацию о его персональных данных

7.1.2.. Свободный доступ к своим персональным данным, включая право на получение ко пий любой записи, содержащей персональные данные клиента или контрагента, за исключением случаев, предусмотренных законодательством РФ.

7.1.3. Требование об исключении или исправлении неверных или неполных, устревших, не достоверных, незаконно полученных или не являющихся необходимыми для Оператора персо нальных данных.

7.1.4. В целях обеспечения достоверности персональных данных, клиент и контрагент обя зан предоставить Оператору полные и достоверные данные о себе

7.1.5.В случае изменения сведений, составляющих персональные данные клиента или контрагента, незамедлительно, но не позднее пяти рабочих дней, предоставить данную информа цию Оператору.

8.Угроза безопасности персональных данных

8.1.Угрозами безопасности персональных данных, актуальными при их обработке в инфор мационных системах персональных данных, являются:

1. Угроза несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных данных, в том числе в ходе соз дания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных
2. Угроза воздействия вредоносного кода, внешнего по отношению к информационной систе ме персональных данных
3. Угроза использования методов социального инжиниринга к лицам, обладающим полномо чиями в информационной системе персональных данных
4. Угроза несанкционированного доступа к отчуждаемым носителям персональных данных

5. Угроза утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных
6. Угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных с использованием уязвимости в организации защиты персональных данных
7. Угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимости в программном обеспечении информационной системы персональных данных
8. Угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных
9. Угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных
10. Угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации

8.2.Определение типа угроз безопасности персональных данных, актуальных для информационной системы персональных данных, производится оператором информационной системы персональных данных в соответствии с пунктом 7 постановления Правительства РФ от 1 ноября 2012 года № 1119 « Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

9. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными работника

9.1. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

9.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное решение.

9.3.Каждый сотрудник Общества, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

9.5.За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера Общество вправе применить предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

9.6.Должностные лица, в обязанность которых входит обработка персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет за собой наказание согласно Кодекса об административных правонарушениях.

10.Заключительные положения.

10.1. Настоящее Положение вступает в силу с момента его утверждения приказом директора Общества.

10.2.Настоящее Положение доводится до сведения всех работников Общества под роспись.

Общество с ограниченной ответственностью «ВодоСнабжение»
(ООО «ВодоСнабжение)
ПРИКАЗ

01.06.2017 г № 77

О назначении ответственного
за организацию обработки персональных данных

В связи с требованиями статей 18.122.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ « О персональных данных»

ПРИКАЗЫВАЮ:

1.Утвердить перечень работников организации, имеющих доступ к сведениям, содержащим персональные данные работников. (Приложение 1)

2.Назначить ответственным за работу с персональными данными работников инспектора по кадрам Князеву Л.В.

3.Инженеру-программисту Шмаль С.В. обеспечить защиту персональных данных работников при автоматизированной обработке данных, при хранении данных на сервере организации и при их передаче по телекоммуникационным сетям.

Директор В.Е.Карташов

С приказом ознакомлены :

Князева Л.В._____01.06.2017

Шмаль С.В._____ 01.06.2017

Приложение № 1

ПЕРЕЧЕНЬ

РАБОТНИКОВ, ИМЕЮЩИХ ПРАВО ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ СОТРУДНИКОВ

№	Подразделение, наименование профессия, должность
1	2
1	Директор
2	Заместитель директора
3	Главный экономист
4	Главный бухгалтер
5	Заместитель главного бухгалтера
6	Инспектор по кадрам
7	Юрисконсульт
8	Инженер-программист
9	Руководители структурных подразделений (доступ к личным данным сотрудникам своего подразделения)
10	Сам работник, носитель данных

Все перечисленные в перечне сотрудники обязаны соблюдать конфиденциальность персональных данных и требования к защите обрабатываемых сведений, а также обеспечивать их безопасность.

Общество с ограниченной ответственностью «ВодоСнабжение»
(ООО «ВодоСнабжение)

ПРИКАЗ

01.08.2018 г Медногорск № 63

Об определении лиц, имеющих право доступа
к персональным данным работников, клиентов и контрагентов

В целях соблюдения порядка получения учета, хранения и эффективной защиты персональных данных работников, клиентов и контрагентов от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и иных неправомерных действий, обеспечению конфиденциальности персональных данных, а также в связи с требованиями статей 18.122.1 Федерального закона от 27 июля 2006 г № 152 ФЗ « О персональных данных»

ПРИКАЗЫВАЮ:

1.Утвердить в новой редакции « Положение о защите персональных данных работников, клиентов и контрагентов ООО «ВодоСнабжение» с 01.08.2018 г.

2.Утвердить перечень работников организации, имеющих доступ к сведениям, содержащим персональные данные работников, клиентов и контрагентов (Приложение 1)

3.Назначить ответственным за работу с персональными данными работников инспектора по кадрам Князеву Л.В.

4.Инженеру-программисту Кадыргулову Р.Ш. обеспечить защиту персональных данных работников при автоматизированной обработке данных, при хранении данных на сервере организации и при их передаче по телекоммуникационным сетям.

5. Все перечисленные в перечне сотрудники обязаны соблюдать конфиденциальность персональных данных и требования к защите обрабатываемых сведений, а также обеспечивать их безопасность.

Директор В.Е.Карташов

С приказом ознакомлены :

Заместитель директора	В.Г.Халявин	01.08.2018
Главный экономист	Е.В.Рябова	01.08.2018
Главный бухгалтер	М.А.Катанова	01.08.2018
Заместитель главного бухгалтера	А.А.Лопоносова	01.08.2018
Экономист	С.В.Кичаева	01.08.2018
Специалист по охране труда	Т.Д.Печайкина	01.08.2018
Бухгалтер	Ю.А.Крикотина	01.08.2018
Бухгалтер	Н.Н.Зотова	01.08.2018
Бухгалтер	Т.А.Горохова	01.08.2018
Бухгалтер	А.А.Катышева	01.08.2018
Инспектор по кадрам	Л.В.Князева	01.08.2018
Юрисконсульт	Л.А.Кобзева	01.08.2018
Начальник ПТО	В.Б.Глушков	01.08.2018
Инженер	А.Н.Наумов	01.08.2018
Инженер-лаборант	Л.И.Фоломейкина	01.08.2018

Начальник участка водоснабжения	В.А.Гордиенко	01.08.2018
Начальник участка отвода и переработки сточных вод	А.Ю.Ерпылев	01.08.2018
Заведующая лабораторией	Т.А.Федорова	01.08.2018
И.о.мастера участка водоснабжения насосной станции пос.Рамазан	М.Б.Забиров	01.08.2018
инженер-программист	Р.Ш.Кадыргулов	01.08.2018
Старший мастер	В.Л.Черных	01.08.2018
Техник	Т.В.Станчуляк	01.08.2018
Контролер водопроводного хозяйства	С.А.Агаркова	01.08.2018
Контролер водопроводного хозяйства	Т.В.Завалишина	01.08.2018
Контролер водопроводного хозйства	Н.В.Казначеева	01.08.2018
Контролер водопроводного хозяйства	О.С.Стебнева	01.08.2018
Контролер водопроводного хозяйства	О.А.Мазго	01.08.2018
Бухгалтер	О.А. Конькова	01.10.2018

Приложение № 1

ПЕРЕЧЕНЬ

РАБОТНИКОВ, ИМЕЮЩИХ ПРАВО ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ СОТРУДНИКОВ, КЛИЕНТОВ И КОНТРАГЕНТОВ

№	Подразделение, наименование профессия, должность
1	2
1	Директор
2	Заместитель директора
3	Главный экономист
4	Главный бухгалтер
5	Заместитель главного бухгалтера
6	Бухгалтер
7	Инспектор по кадрам
8	Юрисконсульт
9	Инженер-программист
10	Руководители структурных подразделений (доступ к личным данным сотрудникам своего подразделения)
11	Сам работник, носитель данных
12	Начальник ПТО
13	Старший мастер
14	Техник
15	Контролер водопроводного хозяйства
16	инженер
17	Специалист по охране труда
18	Экономист
19	Инженер-лаборант

Общество с ограниченной ответственностью «ВодоСнабжение» (ООО «ВодоСнабжение)

ПРИКАЗ

21.04.2015 г. № 3

Об утверждении Положения о защите персональных данных работника

Во исполнение требований главы 14 Трудового Кодекса Российской Федерации «Защита персональных данных работника» и Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение о защите персональных данных работников в ООО «ВодоСнабжение» с 21.04.2015 г.

2. Инспектору по кадрам Максименко Л.П., начальникам участков, руководителям структурных подразделений ознакомить всех сотрудников с Положением о защите персональных данных работников.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор В.Е.Карташов

УТВЕРЖДАЮ
Директор
ООО «ВодоСнабжение»
_____В.Е. Карташов
«__» _____04_____ 2015 г.

Положение о защите персональных данных работников ООО «ВодоСнабжение»

1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, а также Федерального закона "Об информации, информационных технологиях и о защите информации".

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие приказом генерального директора и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

2. Понятие и состав персональных данных

2.1. Под персональными данными работников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. Состав персональных данных работника:

- анкета;
- автобиография;
- образование;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;

- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- размер заработной платы;
- наличие судимостей;
- адрес места жительства;
- домашний, мобильный телефон;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным работника;
- рекомендации, характеристики и т.п.

2.3. Указанные в п. 2.2 сведения являются конфиденциальными и не подлежат разглашению иначе как по основаниям, предусмотренным законодательством РФ.

3. Создание, обработка и хранение персональных данных работника

3.1. Создание персональных данных работника.

Документы, содержащие персональные данные работника, создаются путем:

а) внесения сведений в учетные формы (на бумажных и электронных носителях);

б) получения оригиналов необходимых документов (трудовая книжка, личный листок по учету кадров, автобиография, медицинское заключение).

3.2. Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

3.2.1. При обработке персональных данных работника в целях их защиты и обеспечения прав и свобод человека и гражданина, а также при определении объема и содержания обрабатываемых персональных данных должны строго учитываться положения Конституции Российской Федерации, Трудового кодекса Российской Федерации и иных федеральных законов.

3.2.2. Обработка персональных данных работника осуществляется исключительно в целях:

а) обеспечения соблюдения законов и иных нормативных правовых актов;

б) содействия работникам в трудоустройстве;

в) обеспечения личной безопасности работников;

г) контроля количества и качества выполняемой работы;

д) обеспечения сохранности имущества работника и работодателя.

3.2.3. Все персональные данные работника следует получать у него самого, за исключением случаев, если их получение возможно только у третьей стороны.

3.2.4. Получение персональных данных работника у третьих лиц возможно только при уведомлении работника об этом заранее и с его письменного согласия.

В уведомлении работника о получении его персональных данных у третьих лиц должна содержаться следующая информация:

а) о целях получения персональных данных;

б) о предполагаемых источниках и способах получения персональных данных;

в) о характере подлежащих получению персональных данных;

г) о последствиях отказа работника дать письменное согласие на их получение.

3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, равно как и персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.2.6. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.2.7. Работники и их представители должны быть ознакомлены под расписку с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.3. Сведения, содержащие персональные данные работника, включаются в его личное дело, карточку формы N Т-2, а также содержатся на электронных носителях информации, доступ к которым разрешен лицам, непосредственно использующим персональные данные работника в служебных целях.

3.4. Хранение персональных данных в бухгалтерии:

а) персональные данные, содержащиеся на бумажных носителях, хранятся в запираемом шкафу, установленном на рабочем месте бухгалтера;

б) персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК бухгалтера.

3.4.1. Персональные данные, включенные в состав личных дел, хранятся в запираемом шкафу, установленном на рабочем месте инспектора по кадрам. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК инспектора по кадрам.

3.4.2. Трудовая книжка, документы воинского учета, карточка формы N Т-2 хранятся в запертом металлическом сейфе.

3.4.3. Доступ к ПК строго ограничен кругом лиц, определенных в п. 4.1 настоящего Положения. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).

4.1.1. Право доступа к персональным данным сотрудника имеют:

- директор организации;
- заместитель директора;
- главный бухгалтер;
- заместитель главного бухгалтера
- главный экономист
- инспектор по кадрам;
- юрисконсульт;
- сам работник, носитель данных;
- руководители структурных подразделений (доступ к личным данным сотрудников своего подразделения).

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Организации, в которые сотрудник может осуществлять перечисление денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.2.4. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением заявления работника.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеет право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (ТК РФ).

5. Защита персональных данных

5.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

5.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и не заинтересованные в возникновении угрозы лица.

5.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

5.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

5.5. Внутренняя защита.

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

5.5.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;

- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранению тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей.

5.5.3. Защита персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем.

5.6. Внешняя защита.

5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

5.6.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

5.7. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными работника

6.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Инспектор по кадрам
ООО «ВодоСнабжение» Л.П.Максименко

СОГЛАСОВАНО:
Юрисконсульт
ООО «ВодоСнабжение» О.Г.Лукина