

УТВЕРЖДАЮ

Директор ООО «АйТи Системы»
(наименование должности руководителя
организации)


А.Г. Юдина
01 июля 2022 г.


ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Термины, определения и сокращения

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

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

Информационные активы – информационные системы и информационные ресурсы, сформированные в их рамках.

Информационная безопасность – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах Организации.

Информационный ресурс – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, используемая в бизнес–процессах организации, формируемая в рамках существующих информационных систем.

Информационная система персональных данных (ИСПДн) – совокупность содержащейся в базах данных персональных данных и обеспечивающих ее обработку информационных технологий и технических средств.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Несанкционированный доступ – доступ к информации, нарушающий установленные правила разграничения доступа.

Неавтоматизированная обработка – персональных данных, содержащихся в ИСПДн либо извлеченных из такой системы, а также иных источников, осуществляемая при непосредственном участии человека, как с использованием, так и без использования средств вычислительной техники.

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 (предоставление, доступ), блокирование, удаление, уничтожение, распространение персональных данных.

Облачный сервис – предоставление Организации третьим лицом на основании договора виртуальных ресурсов информационно-телекоммуникационной инфраструктуры центров обработки данных (виртуальные серверы, резервное копирование данных), а также типового программного обеспечения и специального программного обеспечения, необходимого для обработки персональных данных.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое и 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.

Открытая (общедоступная) информация – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят или не был установлен. Информация, сформированная в результате деятельности Организации, которую запрещено относить к коммерческой тайне на основании законодательства Российской Федерации. Информация, представляемая в публичный доступ и с которой сняты грифы конфиденциальности в соответствии с требованиями Организации, используемая в хозяйственной деятельности Организации или имеющая значение для имиджа Организации.

Ответственный за обработку персональных данных – работник Организации, назначенный приказом директора Организации и подотчетный директору Организации, обеспечивающий организацию обработки персональных данных в Организации, осуществляющий внутренний контроль за соблюдением Организацией и ее работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных, осуществляющий информирование работников Организации о положениях законодательства РФ о персональных данных, локальных нормативных актов и иных внутренних документов по вопросам обработки персональных данных, требований к защите персональных данных, организующий прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляющий контроль за приемом и обработкой таких обращений и запросов.

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

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

Представитель – лицо, которое наделено правом представлять интересы субъекта персональных данных в силу специального указания закона или лицо, представляющее субъекта персональных данных, действующее на основании поручения (доверенности или иного документа) удостоверенного (удостоверенной) нотариально, или заверенного (заверенной) способами, приравненными к нотариальному заверению согласно ст. 185.1 ГК РФ.

Программное обеспечение – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

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

Средство криптографической защиты информации – средства шифрования, средства имитозащиты, средства электронной подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации)

Субъект персональных данных – физическое лицо, определенное или определяемое на основании информации, составляющей персональные данные.

Структурное подразделение – объединение нескольких должностных позиций и/или подразделений по признаку общности решаемых задач и регулярно выполняемых работ.

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

АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
ДМЗ	–	демилитаризованная зона
ИА	–	информационный актив
ИБ	–	информационная безопасность
ИС	–	информационная система
ИСПДн	–	информационная система персональных данных
ИР	–	информационный ресурс
НСД	–	несанкционированный доступ
ПДн	–	персональные данные
ПО	–	программное обеспечение
СЗИ	–	средства защиты информации
СКЗИ	–	средства криптографической защиты информации

2. Область применения

2.1. Настоящее положение устанавливает требования и совокупность правил в области организации обработки (как с использованием средств автоматизации, так и без использования таковых) и обеспечения защиты персональных данных, которыми ООО «АйТи Системы» (далее – Оператор, Организация, ООО «АЙТИС») руководствуется в своей деятельности.

2.2. Необходимые правовые, организационные и технические меры для защиты персональных данных при их автоматизированной обработке в корпоративной информационной системе Организации и при обработке без использования средств автоматизации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действия в отношении персональных данных, регламентируются настоящим Положением, Политикой информационной безопасности и другой организационно–распорядительной документацией.

2.3. Передача персональных данных Организацией третьему лицу должна осуществляться с согласия субъекта персональных данных (Приложение 3), если иное не предусмотрено действующим законодательством РФ.

2.4. Организация вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного

или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – Поручение).

2.5. Лицо, осуществляющее обработку персональных данных по Поручению обязано соблюдать принципы и правила обработки персональных данных, предусмотренных 152–ФЗ «О персональных данных».

2.6. В Поручении должны быть определены:

- перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;
- цели обработки персональных данных;
- обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;
- требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом от 27 июля 2006 года № 152–ФЗ «О персональных данных» (далее – Закон о персональных данных).

2.7. Лицо, осуществляющее обработку персональных данных по Поручению, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

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

2.9. Порядок обработки информации в системах контроля и управления физическим доступом на территорию (в здания и помещения) Организации, в системах видеонаблюдения, а также порядок обращения с носителями на которых эта информация размещается, устанавливается соответствующей организационно–распорядительной документацией Организации.

2.10. Положения настоящего документа не распространяются на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов, имеющих статус архивных документов в соответствии с действующим законодательством об архивном деле в РФ.

3. Ответственность за применение

3.1. Требования, изложенные в настоящем Положении, являются обязательными для выполнения всеми работниками Организации и иными лицами, имеющими договорные отношения с Организацией, при этом срочность и важность выполняемых ими работ не должны являться основанием для нарушения положения данного Положения и других документов, регламентирующих в Организации вопросы обработки и защиты персональных данных.

3.2. Ответственным за разработку, пересмотр и изменение настоящего Положения является работник, назначенный ответственным за организацию обработки персональных данных (далее – ответственный за ПДн).

3.3. Руководители структурных подразделений Организации несут персональную ответственность за соблюдение требований настоящего Положения, а также за действия подчиненных им работников в части соблюдения требований, установленных настоящим Положением. Руководители структурных подразделений Организации вправе назначить

ответственными за отдельные вопросы по организации обработки персональных данных и их защите иных должностных лиц.

3.4. Должностные лица, виновные в нарушении требований настоящего нормативного документа, могут быть привлечены к дисциплинарной, административной, гражданско–правовой или уголовной ответственности в порядке и по основаниям, предусмотренных законодательством РФ, Уставом Организации, организационно–распорядительной документацией и трудовыми договорами Организации.

4. Цели документа

4.1. Целью настоящего Положения является обеспечение выполнения Организацией требований, предусмотренных Законом о персональных данных, исключение неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий по отношению к персональным данным, обработку которых ведет Организация.

5. Основные положения

5.1. Организация, являясь оператором персональных данных, осуществляет обработку персональных данных, в том числе автоматизированную, субъектов персональных данных.

5.2. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, в других случаях, предусмотренных федеральными законами.

6. Цели обработки и состав персональных данных

6.1. Персональные данные обрабатываются Организацией в целях:

- ведение кадрового и бухгалтерского учета;
- обеспечение соблюдения трудового законодательства РФ;
- обеспечение соблюдения налогового законодательства РФ;
- обеспечение соблюдения пенсионного законодательства РФ;
- участие лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;
- подготовка, заключение и исполнение гражданско–правового договора;
- подбор персонала (соискателей) на вакантные должности оператора;

В состав персональных данных, обрабатываемых Организацией, входит любая информация, прямо или косвенно относящаяся к субъекту персональных данных относящаяся к субъекту персональных данных.

6.2. В целях реализации Положения в качестве субъектов персональных данных могут выступать:

- Работники;
- Уволенные работники;
- Родственники работников;
- Контрагенты;
- Представители контрагентов;

- Клиенты;
- Выгодоприобретатели по договорам;
- Соискатели;
- Иные категории субъектов персональных данных, персональные данные которых обрабатываются.

Все обрабатываемые в Организации персональные данные должны быть отнесены к одной из следующих категорий:

- специальные категории персональных данных;
- биометрические персональные данные;
- обезличенные и/или общедоступные персональные данные;
- персональные данные общей категории, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным.

6.5. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, в Организации не осуществляется.

6.6. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Организацией для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 11 Закона о персональных данных.

6.7. Типовые формы документов, в которых предполагается и допускается содержание персональных данные:

- личная карточка работника ОУ унифицированной формы;
- трудовой договор;
- дополнительное соглашение к трудовому договору;
- согласие на обработку персональных данных;
- согласие субъекта персональных данных на предоставление персональных данных третьим лицам;
- отзыв субъекта персональных данных согласия на обработку персональных данных;
- запрос субъекта персональных данных на предоставление информации о персональных данных;
- другие.

7. Основные принципы обработки персональных данных

7.1. Обработка персональных данных осуществляется в Организации на основе следующих законодательно определенных принципах:

- обработка персональных данных должна осуществляться на законной и справедливой основе;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

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

– обработке подлежат только персональные данные, которые отвечают целям их обработки;

– содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными к заявленным целям их обработки;

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

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

7.2. В трудовых договорах с работниками Организации и в договорах гражданско–правового характера с иными лицами, в случае, если эти лица имеют доступ к персональным данным, должны быть предусмотрены условия о неразглашении работниками и иными лицами, как охраняемой законом коммерческой или иной законодательно определенной тайны, имеющей в своем составе персональные данные, так и отдельных категорий персональных данных, не входящих в состав тайн.

7.3. С работниками, непосредственно осуществляющими обработку персональных данных, должны быть в установленном порядке оформлены обязательства о выполнении требований организационно–распорядительной документацией Организации по обработке, защите и неразглашении информации ограниченного доступа (в т.ч. персональных данных) (Приложение 8).

7.4. Работники Организации, допущенные к обработке персональных данных, обязаны:

7.4.1. Быть ознакомлены, знать и неукоснительно выполнять положения:

– законодательства Российской Федерации в области персональных данных;

– организационно–распорядительной документацией Организации по вопросам обработки и обеспечения безопасности персональных данных, в том числе требования к защите персональных данных.

7.4.2. Обрабатывать персональные данные только в рамках выполнения своих должностных обязанностей.

7.4.3. Не разглашать персональные данные, обрабатываемые в Организации.

7.4.4. Сообщать о действиях других лиц, которые могут привести к нарушению требований настоящего Положения;

7.4.5. Сообщать об известных фактах нарушения требований настоящего Положения ответственному за организацию обработки персональных данных в Организации.

7.5. Безопасность персональных данных в Организации обеспечивается выполнением согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности персональных данных, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и работы информационных систем персональных данных в случае реализации угроз.

7.6. В Организации должен быть установлен приказом директора Организации перечень работников, осуществляющих обработку персональных данных, в том числе в ИСПДн, либо имеющих доступ к персональным данным. Допускается указание работников в перечне (списке) на ролевой основе в соответствии с занимаемой должностью.

8. Сбор, обработка и хранение персональных данных

8.1. Организация осуществляет сбор, обработку и хранение персональных данных с использованием средств автоматизации и без использования средств автоматизации.

8.2. Все персональные данные следует получать у самого субъекта персональных данных или из общедоступных источников персональных данных. Работник Организации должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

8.3. Согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя (Приложение 1):

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных (Приложение 2).

8.4. Обработка персональных данных субъектов персональных данных работниками Организации осуществляется с согласия субъектов персональных данных, выраженного в письменной форме. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

8.5. Обработка персональных данных без согласия субъектов персональных данных работниками Организации осуществляется в следующих случаях:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом (в том числе ч. 16 ст. 155 Жилищного кодекса Российской Федерации), для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- 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 осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, уголовно-исполнительным законодательством Российской Федерации;

- обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

8.6. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В этом случае субъект персональных данных должен оформить отзыв согласия на обработку персональных данных (Приложения 12).

8.7. Передача персональных данных субъекта персональных данных третьим лицам производится в соответствии с условиями согласия на обработку персональных данных, за исключением случаев, установленных Законом о персональных данных.

8.8. Для обеспечения защиты персональных данных в информационных системах Организацией определяется их перечень, а также критерии отнесения автоматизированной системы к ИСПДн.

Для каждой ИСПДн определяется уровень защищенности в соответствии с требованиями Постановления Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Уровень защищенности ИСПДн указывается в акте определения уровня защищенности и утверждается Ответственным.

Требования к защите персональных данных при использовании «облачных» сервисов устанавливаются в соответствии с действующим законодательством РФ в области защиты персональных данных. В числе таких требований выступает подтверждение адекватности принятых организационных и технических мер по защите персональных данных лицом, предоставляющим «облачный» сервис.

8.9. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Законом о персональных данных, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

8.10. Документы и внешние электронные носители информации, содержащие персональные данные, хранятся в служебных помещениях в закрываемых шкафах, металлических ящиках, если возможно, отдельно от документов, не содержащих персональные данные. При этом должно обеспечиваться раздельное (на разных полках или в разных папках) хранение персональных данных, относящихся к разным целям обработки. Нахождение в помещении лиц, не являющихся работниками Организации, допущенными к обработке персональных данных, возможно только в присутствии работников, допущенных к обработке персональных данных.

8.11. Учет внешних (съемных) электронных носителей информации, содержащей персональные данные, осуществляется в структурных подразделениях, обрабатывающих указанные персональные данные, а также учет архивных носителей информации, содержащих персональные данные.

8.12. Работник, имеющий доступ к персональным данным субъектов персональных данных в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные, исключаящее доступ к ним третьих лиц;
- при уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте он обязан передать документы и иные носители, содержащие персональные данные, лицу, на которое приказом или распоряжением Организации будет возложено исполнение его трудовых обязанностей.

8.13. При обработке персональных данных в ИСПДн работник Организации, допущенный к обработке ПДн, должен соблюдать следующие правила:

- размещение на рабочем месте монитора компьютерной системы необходимо произвести таким образом, чтобы исключить несанкционированный просмотр данных на экране монитора лицами, не являющимися работниками Организации, допущенными к обработке ПДн. Необходимо исключить возможность размещения монитора экраном к входной двери;
- все пароли и ключи доступа к ИСПДн должны храниться в месте, недоступном третьим лицам;
- при работе с ИСПДн использовать только те персональные данные, которые необходимы для выполнения трудовых обязанностей. Просмотр ПДн, не связанных с выполнением трудовых обязанностей, не допускается;
- при печати документов, содержащих ПДн, обеспечить своевременное их получение с принтера, с целью исключения доступа к отпечатанным материалам лиц, не являющихся работниками Организации, допущенными к обработке ПДн;
- для сохранения на флеш-накопителях, смартфонах, планшетах и прочих мобильных носителях информации документов, содержащих ПДн в электронном виде, должны использоваться мобильные носители информации, выданные работнику Организации и разрешенных в системе контроля мобильных устройств. Использование личных мобильных носителей информации для целей обработки ПДн не допускается;
- при записи документов, содержащих ПДн, на носители информации необходимо следить за тем, чтобы ПДн, предназначенные для разных целей обработки, были записаны в разные каталоги (папки) носителя информации;
- при кратковременном уходе с рабочего места (на период не более одного часа) убедиться в том, что полученные для обработки и ввода в ИСПДн документы, содержащие ПДн, убраны со стола в сейф или запираемый шкаф, а компьютер заблокирован, чтобы в отсутствие работника, допущенного к обработке ПДн, у лиц, не являющихся работниками Организации, допущенными к обработке ПДн, не было возможности войти в ИСПДн под его учетными данными;
- при уходе с рабочего места на период более одного часа (окончание рабочего дня, выезд в командировку, отпуск и т.п.) убедиться, что сеанс доступа к ИСПДн завершен, а компьютер выключен. Все документы, носители информации, содержащие ИСПДн, должны быть убраны в сейф или запираемый шкаф;
- в случае возникновения нештатной ситуации при обработке ПДн в ИСПДн или на файловом ресурсе (сбой программы, обнаружение компьютерного вируса) необходимо немедленно прекратить обработку ПДн и сообщить Ответственному;
- в случае передачи в ремонт или на техническое обслуживание технических средств Организации, используемых для обработки ПДн, необходимо убедиться, что в них отсутствуют носители, содержащие ПДн (диски, флеш-карты, бумага в принтере и т.п.). При невозможности отделения материального носителя ПДн от передаваемого оборудования (жесткий диск компьютера и т.п.) и невозможности их уничтожения (стирания), технические средства могут передаваться третьему лицу с соблюдением требований законодательства;
- требования к рабочим местам, с которых осуществляется доступ к ИСПдн, к серверам ИСПДн и файловым ресурсам, содержащих ПДн, определяется соответствующим документом по информационной безопасности.

8.14. О фактах утраты ПДн либо их разглашения необходимо немедленно поставить в известность непосредственного руководителя и ответственного за обеспечение безопасности ПДн в Организации.

8.15. При увольнении работника, имеющего доступ к персональным данным субъекта персональных данных, документы и иные носители, содержащие указанные персональные данные, сдаются руководителю структурного подразделения.

8.16. Обрабатываемые персональные данные подлежат уничтожению в случае достижения целей обработки, отзыва согласия субъектом ПДн осуществляется в срок, не превышающий 30 календарных дней с момента возникновения события, если иной срок не вытекает из заключенных договоров либо не установлен законодательством РФ (в том числе установлено право обрабатывать ПДн без согласия субъекта ПДн).

8.17. Уничтожение персональных данных, не подлежащих передаче в архив Организации, осуществляется только комиссией в составе представителей структурного подразделения Организации, в чьем ведении находятся указанные персональные данные. Результаты уничтожения должны документироваться путем составления акта (Приложение 5).

8.18. В случае выявления недостоверных персональных данных субъекта персональных данных или неправомерных действий с ними работников Организации при обращении или по запросу субъекта персональных данных или его законного представителя осуществляется блокирование персональных данных, относящихся к соответствующему субъекту, с момента такого обращения или получения такого запроса на период проверки.

8.19. В случае подтверждения факта недостоверности персональных данных субъекта персональных данных на основании документов, представленных субъектом персональных данных или его законным представителем, или иных необходимых документов производится уточнение персональных данных, соответствующая блокировка снимается.

8.20. В случае выявления неправомерных действий с персональными данными в срок, не превышающий семи рабочих дней с момента выявления, необходимо устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий семи рабочих дней с момента выявления неправомерности действий с персональными данными, необходимо уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Организация обязана уведомить субъекта персональных данных или его законного представителя.

8.21. В случае отсутствия возможности уничтожения ПДн в течении сроков, указанных в предыдущих абзацах, Организация осуществляет блокирования таких ПДн и обеспечивает уничтожения этих ПДн в срок не более 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

8.22. Уничтожение ПДн, содержащихся в документах на бумажных носителях, осуществляется методом измельчения в шредере (уничтожителе бумаги). В случае привлечения к такому уничтожению третьих лиц с ними подписывается договор, включающий в себя положения о конфиденциальности передаваемых ПДн, запрет на копирование и гарантии их безвозвратного уничтожения.

8.23. Если иное не предусмотрено законодательством, доступ к ПДн, обрабатываемым в Организации, третьим лицам, не являющимися практикантами,

предоставляется только при наличии между организацией и третьим лицом соглашения о неразглашении конфиденциальной информации либо условий в договоре с третьим лицом о неразглашении конфиденциально информации, в том числе предусматривающих защиту полученных персональных данных.

8.24. Работники Организации, передающие в рамках исполнения должностных обязанностей персональные данные на материальных носителях третьим лицам, должны передавать их с обязательным составлением акта приема–передачи документов (иных материальных носителей), содержащих ПДн. Акт составляется по установленной форме (Приложение 6) и хранится в подразделении работника. В случае пересылки ПДн средствами электронной почты факты передачи фиксируются DLP– системой (при ее наличии), без участия лица, передающего ПДн. При отправки персональных данных средствами электронной почты необходимо разместить в тексте письма уведомление о конфиденциальности (Приложение 7).

8.25. Передача документов (иных материальных носителей), содержащих ПДн (при условии соблюдения требований о наличии согласия субъекта ПДн на передачу его ПДн третьей стороне или в случаях, когда такое согласие не требуется, в отсутствии такого согласия), осуществляется Организацией при наличии:

– соглашения о неразглашении конфиденциальной информации с лицом, которому передаются персональные данные, либо условий в договоре с третьим лицом о неразглашении конфиденциальной информации, в том числе предусматривающих защиту полученных персональных данных;

или

– письма–запроса от третьего лица (получающего персональные данные), которое должно включать в себя указание на правовое основание для получения ПДн, перечень, цель использования, ФИО и должность лица, которому поручается получить данную информацию.

8.26. Сведения об обрабатываемых ПДн должны быть предоставлены субъекту ПДн Организацией в доступной форме. В них не должны содержаться ПДн, относящиеся в другим субъектам ПДн.

8.26.1. Выбор формы обращения (запроса) для реализации своего права на получение сведений зависит от воли субъекта ПДн:

– устного обращения к работникам Организации, сопровождающегося обязательным предоставлением основного документа, удостоверяющего личность субъекта ПДн или его представителя, а также документа, подтверждающего полномочия этого представителя;

– предоставление запроса в организацию как на бумажном носителе, так и в форме электронного документа, подписанного электронной подписью в соответствии с законодательством РФ

8.26.2. Обращение (запрос) субъекта ПДн регистрируется в Журнале учета обращений. Ведение Журнала учета обращений осуществляется работником, назначенным приказом директора Организации.

8.26.3. Журнал учета обращений может вестись для каждого подразделения Организации отдельно. Журнал ведется в электронном виде, начинается в первый рабочий день года и распечатывается по окончании года в случае наличия зафиксированных обращений субъектов ПДн либо по запросу контролирующих органов, при этом Журнал

учета обращений нумеруется, брошюруется, скрепляется печатью и подписывается ответственным за организацию обработки ПДн в Организации.

8.26.4. Журнал учета проверок контролирующими органами ведется в электронном виде, начинается в первый рабочий день года и распечатывается по окончании года в случае наличия записей, при этом Журнал учета проверок контролирующими органами нумеруется, брошюруется, скрепляется печатью и подписывается ответственным за организацию обработки ПДн в Организации.

8.26.5. Хранение Журналов учета обращений и Журналов учета проверок контролирующими органами на бумажном носителе и оригиналы запросов хранятся у ответственного за организацию обработки ПДн в течение одного календарного года, а в последствии подлежат архивному хранению в соответствии с внутренними документами Организации.

8.26.6. Организация обязана сообщить субъекту ПДн или его представителю информацию об обрабатываемых ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с ними при обращении субъекта ПДн или его представителя в течение тридцати дней с даты обращения либо получения запроса субъекта ПДн или его представителя, если более короткий срок не предусмотрен законодательством (Приложение 9).

8.26.7. Организация вправе отказать в предоставлении субъекту ПДн или его представителю при получении запроса субъекта ПДн или его представителя информации о наличии ПДн о соответствующем субъекте ПДн. При этом Организация обязана дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок не превышающий тридцать дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя, если более короткий срок не предусмотрен федеральными законами.

8.26.8. Организация обязана безвозмездно предоставить субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к соответствующему субъекту ПДн, а также внести в них необходимые изменения (Приложение 10), уничтожить или заблокировать (Приложение 11) соответствующие ПДн по предоставлению субъектом ПДн или его представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Организация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О принятых мерах по отношению к ПДн обратившегося субъекта Организация обязана уведомить субъекта ПДн или его представителя и третьих лиц, которым ПДн этого субъекта были переданы (если применимо).

8.26.9. Все ответы субъектам ПДн либо их представителям регистрируются в Журнале учета обращений.

8.26.10. При поступлении от субъекта ПДн либо его представителя просьбы предоставить ответ путем вручения, факт его вручения субъекту ПДн либо его представителя регистрируется в Журнале учета обращений с пометкой «получено лично» и подписью субъекта ПДн или его представителя с указанием реквизитов доверенности представителя. В данном случае последующее направление ответа почтовым отправлением не требуется. В остальных случаях ответ на запрос субъекта ПДн подлежит направлению субъекту ПДн либо его представителю способом, указанным в запросе, при отсутствии

такого указания – по адресу места жительства субъекта ПДн почтовым отправлением с описью вложения и уведомлении о вручении.

8.27. Нештатными ситуациями являются:

- разглашение персональных данных работниками Организации, имеющими право доступа к ПДн, в том числе:
 - раскрытие ПДн лицам, не имеющим права доступа к ним;
 - передача незащищенных ПДн по открытым каналам связи (интернет, электронная почта, файлообменники, службы мгновенного обмена сообщениями, социальные сети и т.п.);
 - опубликование ПДн, не являющихся общедоступными, в Интернете, открытой печати и других средствах массовой информации;
- передача материального носителя ПДн лицу, не имеющему права доступа к ней;
- утрата материального носителя ПДн.
- несанкционированный доступ к персональным данным:
- использование устройств негласного съема информации;
- маскировка под зарегистрированного пользователя ИСПДн;
- использование дефектов программного обеспечения ИСПДн;
- применение программных вирусов;
- хищение материального носителя ПДн;
- умышленное нарушение функционирования технических средств обработки информации;
- блокирование доступа к ПДн путем перегрузки технических средств обработки информации (применение нерегламентированных внутренними документами Организации программного обеспечения, способного производить несанкционированные команды и действия);
- дефекты, сбои и отказы программного обеспечения ИСПДн.
- природные явления, стихийные бедствия, техногенные факторы, непосредственно угрожающие защите ПДн:
 - пожары, землетрясения, наводнения и другие климатические факторы;
 - электромагнитные факторы (грозовые разряды и т.д.).

Организационные и технические мероприятия по предотвращению нештатных ситуаций реализуются на основании внутренних документов по информационной безопасности поставщиком ИТ-услуг.

К мероприятиям, снижающим риск возникновения нештатных ситуаций, относится обучение работников, допущенных к обработке ПДн (в том числе и с использованием средств автоматизации), основным действиям в информационных системах, направленных на обеспечения информационной безопасности, в том числе тому, как распознать возникновение внештатной ситуации и порядок действия работника при ее возникновении.

9. Защита персональных данных

9.1. Организация самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами.

9.2. 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 незаинтересованные в возникновении угрозы лица.

9.3. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

9.4. В целях обеспечения безопасности персональных данных при их обработке, Организация принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных от неправомерного и случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, в частности соблюдается ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками Организации;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно–методических документов по защите информации и сохранению коммерческой тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами;
- 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 подразделений;
- воспитательная и разъяснительная работа с работниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- технические средства охраны, сигнализации;
- средства защиты информации;
- порядок охраны территории, зданий, помещений, транспортных средств.

9.5. Защита персональных данных в электронном виде реализуется с помощью средств защиты информации, средств криптографической защиты информации, внутренними возможностями информационной системы персональных данных.

9.6. В целях сохранности персональных данных субъектов персональных данных, хранящихся в автоматизированной системе Организации, Организация предпринимает меры по обеспечению безопасности этих данных, предусмотренные Законом о персональных данных и Федеральным законом от 27 июля 2006 года № 149–ФЗ «Об информации, информационных технологиях и о защите информации».

9.7. Безопасность указанных данных обеспечивается, в частности, путем предотвращения получения несанкционированного доступа к ним, неправомерного получения этих данных, а также предупреждения преднамеренного программно–

технического воздействия с целью уничтожения, копирования, переадресации или искажения данных в процессе их создания, использования, передачи и хранения.

9.8. Для хранения, кодирования и пересылки информации, относящейся к персональным данным субъектов персональных данных, могут использоваться только устройства и программное обеспечение в корпоративной сети передачи данных, отвечающим требованиям политик безопасности Организации.

10. Права и обязанности сторон

10.1. При определении объема и содержания обрабатываемых персональных данных Организация должна руководствоваться Конституцией Российской Федерации и иными федеральными законами.

10.2. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Организация вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 – 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Закона о персональных данных.

10.3. Защита персональных данных субъекта персональных данных от неправомерного их использования или утраты должна быть обеспечена Организацией за счет его средств в порядке, установленном Законом о персональных данных.

10.4. В целях защиты персональных данных, хранящихся в Организации, субъект персональных данных имеет право:

- требовать исключения, исправления, блокирования и уничтожения неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны;
- осуществление иных прав, предусмотренных законодательством Российской Федерации.

11. Нормативные ссылки

11.1. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

11.2. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

11.3. Постановление Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

11.4. Постановление Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

11.5. Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

11.6. Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА ООО «АЙТИ СИСТЕМЫ»

«__» _____ 20__ г.

г. Вологда

Я, _____,
проживающий по адресу: _____

паспорт: № _____,

выдан (кем и когда) _____.

(далее – «Работник»), своей волей и в своем интересе настоящим выражаю мое согласие (далее – «Согласие») на обработку моих персональных данных ООО «АйТи Системы» (далее, в зависимости от контекста – «Работодатель» или «Оператор»), юридический адрес: 160012, г. Вологда, ул. Козленская, 119–А, пом. 46 в следующих целях:

- ведение кадрового и бухгалтерского учета;
- реализация прав и обязанностей Работодателя по заключенному между Работником и Работодателем трудовому договору, в том числе для направления Работника на обучение и в командировки, организации участия Работника в выставках и закупках, заказа пропусков, оформления доверенностей, паспортов и виз, бронирования гостиниц, заказа авиабилетов, железнодорожных билетов и прочих проездных документов, перевода денег на зарплатную карту, банковские счета, счета депо для ценных бумаг и иное, а также предоставление обязательных и дополнительных льгот (обязательное и добровольное медицинское страхование, пенсионное страхование, организация совместного отдыха, оздоровление и иное), а также контроля качества выполняемой работы и обеспечения сохранности имущества Работодателя;
- обеспечение личной безопасности Работника;
- ведение договорной и финансово–хозяйственной деятельности Оператора.

1. Я согласен с тем, что перечень моих персональных данных, передаваемых Оператору для обработки, включают все или любую часть из указанных ниже персональных данных, необходимых для достижения целей, заявленных в настоящем Согласии, или иных целей обработки, предусмотренных законодательством:

- Фамилия, Имя, Отчество;
- Дата рождения;
- Месяц рождения;
- Год рождения;
- Место рождения;
- Семейное положение, сведения о детях, ближайших родственниках (фамилия, имя, отчество, дата рождения);
- Доходы;
- Адрес электронной почты;
- Адрес регистрации;
- СНИЛС;
- Гражданство;

- Адрес места жительства;
- Номер телефона;
- ИНН;
- Данные документа, удостоверяющего личность;
- Данные водительского удостоверения;
- Номер расчетного счета;
- Профессия;
- Сведения о трудовой деятельности;
- Реквизиты банковской карты;
- Номер лицевого счет;
- Должность;
- Отношение к воинской обязанности, сведения о воинском учете;
- Сведения об образовании.

3. Я ознакомлен с действующей организационно–распорядительной документацией Работодателя, устанавливающей порядок обработки персональных данных работников Оператора, включая порядок передачи моих персональных данных в пределах организации Оператора, а также со своими правами и обязанностями в этой области, что подтверждается моей подписью на последней странице настоящего Соглашения.

4. Я даю согласие на обработку Оператором моих персональных данных, в соответствии с положениями Федерального закона «О персональных данных» и Трудового кодекса РФ, включая согласие на совершение им следующих действий:

- сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение, (для обработки способами, предусмотренными настоящим Соглашением, в целях, предусмотренных настоящим Соглашением) ООО «АЙТИС» персональных данных, для достижения заявленных в настоящем Соглашении целей в отношении персональных данных, приведенных в п.1 настоящего соглашения.

5. Оператор вправе использовать следующие основные способы обработки моих персональных данных, в том числе:

- автоматизированная обработка;
- не автоматизированная обработка;
- смешанная обработка.

6. Я соглашаюсь с тем, что Работодатель может обрабатывать мои персональные данные в течение всего срока действия трудового договора между мной и Работодателем, при условии, что дальнейшая обработка не является правом и обязанностью Работодателя, которые возникают из требований законодательства РФ, коллективного договора Работодателя или трудового договора с Работником, и не требует согласия Работника.

7. Я соглашаюсь с тем, что Работодатель может хранить мои персональные данные в течении 50 (пятидесяти) лет после моего увольнения.

8. Я уведомлен о том, что по моему письменному запросу или письменному запросу моего представителя Работодатель должен предоставить мне или моему представителю информацию, касающуюся обработки моих персональных данных.

9. Настоящее Соглашение на обработку персональных данных дается мной добровольно, без принуждения, вступает в силу с даты его подписания мной и может быть в любой момент отозвано путем направления Работодателю письменного заявления.

Получив такое заявление, Работодатель будет обязан в срок, установленный законодательством, прекратить обработку указанных в сообщении Работника персональных данных либо обеспечить прекращение обработки, и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение, при условии что дальнейшая обработка не является правом или обязанностью Работодателя, которые установлены законодательством РФ, и не требуют согласия Работника.

Подпись работника:

(подпись)

(ФИО полностью, без сокращений)

**СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ,
РАЗРЕШЕННЫХ СУБЪЕКТОМ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ
РАСПРОСТРАНЕНИЯ, РАБОТНИКА ООО «АЙТИ СИСТЕМЫ»**

«__» _____ 20__ г.

г. Вологда

Я, _____,
проживающий по адресу: _____

паспорт: № _____,
выдан (кем и когда) _____.

(далее – «Работник») заявляю о согласии на общедоступность в течение всего срока действия настоящего Согласия моих следующих персональных данных у работодателя ООО «АйТи Системы» (далее, в зависимости от контекста – «Работодатель» или «Оператор»), юридический адрес: 160012, г. Вологда, ул. Козленская, 119–А, пом. 46:

- Фамилия, Имя, Отчество;
- Дата рождения;
- Месяц рождения;
- Год рождения;
- Адрес электронной почты;
- Номер телефона;
- Профессия;
- Должность.

Настоящее согласие дано мной добровольно и действует со дня его подписания до отзыва в установленном законом порядке.

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования работодатель обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

Подпись работника:

(подпись)

(ФИО полностью, без сокращений)

**СОГЛАСИЕ РАБОТНИКА ООО «АЙТИ СИСТЕМЫ» НА ПЕРЕДАЧУ
ПЕРСОНАЛЬНЫХ ДАННЫХ
ТРЕТЬЕЙ СТОРОНЕ**

Директору ООО «АйТи Системы»
Юдиной А.Г.

от _____

(ФИО субъекта персональных данных)

адрес места жительства: _____

телефон: _____

паспорт (иной основной документ,
удостоверяющий личность)

серии _____ № _____

выданный (кем, когда) _____

Согласие на передачу персональных данных третьей стороне

Настоящим выражаю мое согласие (далее – «Согласие») на передачу моих персональных данных третьей стороне _____, в целях оказания ООО «АйТи Системы» услуг по _____.

Я согласен с тем, что перечень моих персональных данных, передаваемых третьей стороне для обработки, включают все или любую часть из указанных ниже персональных данных, необходимых для достижения целей, заявленных в настоящем Согласии, или иных целей обработки, предусмотренных законодательством:

- Фамилия, Имя, Отчество;
- Дата рождения;
- Месяц рождения;
- Год рождения;
- Место рождения;
- Семейное положение, сведения о детях, ближайших родственниках (фамилия, имя, отчество, дата рождения);
- Доходы;
- Адрес электронной почты;
- Адрес регистрации;
- СНИЛС;
- Гражданство;
- Адрес места жительства;
- Номер телефона;
- ИНН;

- Данные документа, удостоверяющего личность;
- Данные водительского удостоверения;
- Номер расчетного счета;
- Профессия;
- Сведения о трудовой деятельности;
- Реквизиты банковской карты;
- Номер лицевого счет;
- Должность;
- Отношение к воинской обязанности, сведения о воинском учете;
- Сведения об образовании.

Настоящее Соглашение на передачу персональных данных третьей стороне дается мной добровольно, без принуждения, вступает в силу с даты его подписания мной и может быть в любой момент отозвано путем направления Работодателю письменного заявления.

Получив такое заявление, Работодатель будет обязан в срок, установленный законодательством, прекратить обработку указанных в сообщении Работника персональных данных либо обеспечить прекращение обработки, и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение, при условии что дальнейшая обработка не является правом или обязанностью Работодателя, которые установлены законодательством РФ, и не требуют согласия Работника.

Подпись работника:

(подпись)

(ФИО полностью, без сокращений)

**СОГЛАСИЕ СУБЪЕКТА ПДН, НЕ ЯВЛЯЮЩЕГОСЯ РАБОТНИКОМ ООО
«АЙТИ СИСТЕМЫ», НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Я, _____,
проживающий по адресу: _____,

паспорт: № _____,
выдан (кем и когда) _____.

своей волей и в своем интересе настоящим выражаю мое согласие на обработку моих персональных данных ООО «АйТи Системы», юридический адрес: 160012, г. Вологда, ул. Козленская, 119–А, пом. 46 в составе:

– Фамилия, Имя, Отчество;

–

–

Для следующих целей обработки:

–

–

Настоящим согласием разрешаю производить с моими персональными данными следующие действия: 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 (для обработки способами, предусмотренными настоящим Согласием, в целях, предусмотренных настоящим Согласием) ООО «АйТи Системы», обезличивание, удаление, блокирование, уничтожение персональных данных, передача третьему лицу на основании заключаемого с этим лицом договора, для оказания Оператору услуг по организации и ведению бухгалтерского, кадрового и налогового учета.

Настоящее Согласие на обработку персональных данных дается мной добровольно, без принуждения, вступает в силу с даты его подписания и может быть в любой момент отозвано путем направления письменного требования на адрес Оператора: 160012, г. Вологда, ул. Козленская, 119–А, пом. 46.

Мои права в области персональных данных мне разъяснены.

(подпись)

(ФИО полностью, без сокращений)

«__» _____ 20__ г

АКТ УНИЧТОЖЕНИЯ ДОКУМЕНТОВ (ИНЫХ МАТЕРИАЛЬНЫХ НОСИТЕЛЕЙ),
СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

« ___ » _____ 20__ г.

г. Вологда

Комиссия в составе:

ФИО — Должность
 ФИО — Должность
 ФИО — Должность

Провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации бумажные носители персональных данных подлежат уничтожению.

Уничтожены следующие бумажные носители персональных данных:

№ п/п	Название документа/массива документов	Количество листов	Основание для уничтожения

Бумажные носители уничтожены путем shredding.

Члены Комиссии:

_____ (ФИО)

_____ (ФИО)

_____ (ФИО)

**АКТ ПРИЕМА–ПЕРЕДАЧИ ДОКУМЕНТОВ
(ИНЫХ МАТЕРИАЛЬНЫХ НОСИТЕЛЕЙ), СОДЕРЖАЩИХ
ПЕРСОНАЛЬНЫЕ ДАННЫЕ**

«__» _____ 20__ г.

г. Вологда

ООО «АйТи Системы», в лице

(ФИО, должность работника, осуществляющего передачу персональных данных)

передает, а _____
(ФИО лица, осуществляющего прием персональных данных/наименование организации, принимающей документы)
получает документы (иные материальные носители, уточнить какие), содержащие персональные
данные, для целей обработки в соответствии с _____,
(указать основание передачи (договор, нормативный акт и т.п.)

приведенные в следующем перечне:

№ п/п	Вид документа (материального носителя)	Кол-во	Единица измерения	Цель обработки
Всего:				

Полученные персональные данные могут быть использованы только в целях, указанных в перечне, для достижения которых они переданы. Использование предоставленных персональных данных в иных целях является незаконным и может повлечь соответствующую гражданско–правовую, материальную, дисциплинарную, административно–правовую и/или уголовную ответственность. Лица, принявших документы (иные материальные носители) содержащие персональные данные обязуются соблюдать в отношении них требования конфиденциальности.

Передал (подпись, ФИО, должность работника ООО «АйТи Системы», осуществляющего передачу персональных данных)

Принял (подпись, ФИО лица, осуществляющего прием персональных данных/наименование организации, принимающей документы)

УВЕДОМЛЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ

УВЕДОМЛЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ: это электронное сообщение и любые документы, приложенные к нему, содержат конфиденциальную информацию. Содержащиеся в настоящем сообщении персональные данные могут быть использованы только работниками компании, физическим или юридическим лицом, которому они адресованы. Указанная информация не может быть использована, скопирована или разглашена Вами, если согласие на выполнение таких действий ранее не было предоставлено Вам обладателем такой информации. Настоящим уведомляем Вас о том, что, если это сообщение не предназначено Вам, использование, копирование, распространение информации, содержащейся в настоящем сообщении, а также осуществление любых действий на основе этой информации, строго запрещено. Если Вы получили это сообщение по ошибке, пожалуйста, сообщите об этом отправителю по электронной почте и удалите это сообщение.

СОГЛАШЕНИЕ О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПДн

Я, _____,
проживающий по адресу: _____,

паспорт: № _____,
выдан (кем и когда) _____.

предупрежден(а) о том, что на период исполнения мною должностных обязанностей по трудовому договору, заключенному между мною и ООО «АйТи Системы», и предусматривающих работы с персональными данными субъектов персональных данных мне будет предоставлен доступ к указанной информации.

Настоящим добровольно принимаю на себя обязательства:

- не передавать (в любом виде) и не разглашать третьим лицам и работникам организации, не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением руководителя организации, информацию, содержащую персональные данные Субъектов, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;
- в случае попытки третьих лиц или работников организации, не имеющих на это право, получить от меня информацию, содержащую персональные данные Субъектов, немедленно сообщать об этом факте своему непосредственному или (в случае отсутствия непосредственного) вышестоящему руководителю;
- не использовать информацию, содержащую персональные данные Субъектов организации, с целью получения выгоды;
- выполнять требования закона и иных нормативных правовых актов Российской Федерации, а также внутренних документов организации, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;
- в течение 3 (трех) лет после прекращения моих прав на доступ к информации, содержащей персональные данные, переход на должность, не предусматривающую доступ к персональным данным Субъектов и прекращения трудового договора, не разглашать и не передавать третьим лицам и неуполномоченным на это работникам организации, известную мне информацию, содержащую персональные данные Субъектов.

Я ознакомлен(а) с положениями законодательства Российской Федерации, а также локальными нормативными актами (регламенты, положения, инструкции, приказы, распоряжения), в части защиты персональных данных.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с действующим законодательством Российской Федерации.

_____ «__» _____ 20__ г.
(фамилия, инициалы) (подпись)

ЗАЯВЛЕНИЕ О ПОЛУЧЕНИИ ИНФОРМАЦИИ О ПЕРСОНАЛЬНЫХ ДАННЫХ

Директору ООО «АйТи Системы»
Юдиной А.Г.

от _____
(ФИО субъекта персональных данных)

адрес места жительства: _____

телефон: _____

паспорт (иной основной документ,
удостоверяющий личность)

серии _____ № _____

выданный (кем, когда) _____

Заявление о получении информации о персональных данных

Прошу Вас предоставить мне сведения об имеющихся в ООО «АйТи Системы» моих персональных данных, целях и способах их обработки, источниках их получения, лица, имеющих к ним доступ, сроках их обработки (в том числе хранения), ознакомить меня с указанными персональными данными.

1. Фамилия, имя, отчество;
- 2.
- 3.

Предпочтительный способ предоставления информации: _____

_____ «__» _____ 20__ г.
(фамилия, инициалы субъекта персональных данных) (подпись)

_____ «__» _____ 20__ г.
(фамилия, инициалы работника) (подпись)

Входящий номер: _____

Исходящий номер: _____

ЗАЯВЛЕНИЕ ОБ ИЗМЕНЕНИИ/ДОПОЛНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Директору ООО «АйТи Системы»

Юдиной А.Г.

от _____

(ФИО субъекта персональных данных)

адрес места жительства: _____

телефон: _____

паспорт (иной основной документ,

удостоверяющий личность)

серии _____ № _____

выданный (кем, когда) _____

Заявление об изменении/дополнении персональных данных

ООО «АйТи Системы» осуществляет обработку следующих персональных данных:

1. Фамилия, имя, отчество;
- 2.
- 3.

Вышеуказанные персональные данные являются неполными (или: устаревшими, неточными), что подтверждается _____.

На основании изложенного, руководствуясь ч. 1 ст. 14 Федерального закона О персональных данных, прошу Вас в срок, установленный законодательством, внести изменения/дополнения в персональные данные, а именно:

Перечень вносимых изменений:

Персональные данные, обрабатываемые Оператором	Корректное значение персональных данных

Приложения:

1. Документы, подтверждающие неполноту (или: неактуальность, неточность) персональных данных.
2. Иные документы, подтверждающие обстоятельства, на которых заявитель основывает свои требования.

(фамилия, инициалы субъекта персональных данных)

(подпись)

«__» _____ 20__ г.

(фамилия, инициалы работника)

(подпись)

«__» _____ 20__ г.

Входящий номер: _____

Исходящий номер: _____

ЗАЯВЛЕНИЕ ОБ УНИЧТОЖЕНИИ (БЛОКИРОВАНИИ) ПЕРСОНАЛЬНЫХ ДАННЫХ

Директору ООО «АйТи Системы»
Юдиной А.Г.

от _____
(ФИО субъекта персональных данных)

адрес места жительства: _____

телефон: _____

паспорт (иной основной документ,
удостоверяющий личность)

серии _____ № _____

выданный (кем, когда) _____

Заявление об уничтожении (блокировании) персональных данных

ООО «АйТи Системы» осуществляет обработку следующих персональных данных:

1. Фамилия, имя, отчество;
- 2.
- 3.

Прошу Вас в сроки, установленные законодательством, уничтожить (блокировать) как неполные/ устаревшие/ неточные/ незаконно полученные/ не являющиеся необходимыми для заявленной цели обработки персональные данные, указанные в таблице:

Перечень подлежащих уничтожению персональных данных:

№ п/п	Персональные данные

Приложения:

_____ «__» _____ 20__ г.
(фамилия, инициалы субъекта персональных данных) (подпись)

_____ «__» _____ 20__ г.
(фамилия, инициалы работника) (подпись)

Входящий номер: _____

Исходящий номер: _____

ЗАЯВЛЕНИЕ ОБ ОТЗЫВЕ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Директору ООО «АйТи Системы»
Юдиной А.Г.

от _____
(ФИО субъекта персональных данных)

адрес места жительства: _____

телефон: _____

паспорт (иной основной документ,
удостоверяющий личность)

серии _____ № _____

выданный (кем, когда) _____

Заявление об отзыве согласия на обработку персональных данных

ООО «АйТи Системы» осуществляет обработку следующих персональных данных:

1. Фамилия, имя, отчество;
- 2.
- 3.

Заявляю об отзыве моих персональных данных и прошу прекратить их обработку.

_____ «__» _____ 20__ г.
(фамилия, инициалы субъекта персональных данных) (подпись)

_____ «__» _____ 20__ г.
(фамилия, инициалы работника) (подпись)

Входящий номер: _____

Исходящий номер: _____