ИНЖИНИРИНГ
группа компаний

Общество с ограниченной ответственностью «Инжиниринг»
300012, г. Тула, ул. Тимирязева, д.99в

ПРИКАЗ

«01» марта 2021 г. № 66-к

г. Тула

Об обеспечении соблюдения требований законодательства о защите персональных данных в ООО «Инжиниринг»

В целях защиты персональных данных в ООО «Инжиниринг» на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27.07.206 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить положение о персональных данных в ООО «Инжиниринг» (Приложение 1).
2. Утвердить перечень должностных лиц, имеющих допуск к персональным данным (Приложение 2).
3. Определить места хранения персональных данных (Приложение 3).
4. Утвердить инструкцию для работы с персональными данными сотрудников ООО «Инжиниринг», имеющих допуск к персональным данным (Приложение 4).
5. Назначить ответственных за обработку и безопасность персональных данных в ООО «Инжиниринг» начальника отдела правового обеспечения, начальника отдела кадров, начальника отдела управления персоналом, главного бухгалтера, начальника отдела охраны труда и промышленной безопасности, начальника управления безопасности, ответственным за обработку и безопасность персональных данных в информационных системах назначить заместителя начальника отдела корпоративных и технологических АСУ.

6. Организовать получение согласие работников ООО «Инжиниринг» на обработку персональных данных в ООО «Инжиниринг» и их передачу в ФНС, ПФР и т.п.
7. Работникам отдела кадров ознакомить сотрудников ООО «Инжиниринг» под роспись с законом «О персональных данных», положением «О персональных данных в ООО «Инжиниринг» и осуществлять ознакомление с настоящим приказом под роспись всех вновь принимаемых работников ООО «Инжиниринг».
8. Работникам отдела кадров получить обязательство о неразглашении персональных данных с сотрудников, имеющих допуск к персональным данным, и осуществлять получение указанных обязательств с принимаемых на работу лиц, имеющих допуск к персональным данным.
9. Работникам отдела кадров вести список лиц, имеющих допуск к персональным данным.
10. Работникам отдела кадров ознакомить лиц, имеющих допуск к персональным данным, с инструкцией о защите персональных данных.
11. Ответственным за защиту персональных данных осуществлять внутренний контроль процесса обработки персональных данных и производить оценку вреда, который может быть причинен субъектам персональных данных, соотношение указанного вреда и принимаемых мер по обеспечению безопасности персональных данных.
12. Разместить копии локальных актов по защите персональных данных в ООО «Инжиниринг» в отделе кадров и на сервере, для возможности ознакомления с ними сотрудников ООО «Инжиниринг».
13. Контроль за исполнением настоящего приказа оставляю за собой.

Заместитель генерального директора по безопасности **Р.С. Шведов**

Приложение 1
к приказу от 01.03.2021 № 66-к

ПОЛОЖЕНИЕ
О ПЕРСОНАЛЬНЫХ ДАННЫХ
В ОБЩЕСТВЕ С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«ИНЖИНИРИНГ»

Содержание

1. Назначение и область применения

2. Ответственность

3. Термины

4. Общие положения. Состав персональных данных

5. Обработка и обеспечение безопасности персональных данных

5.1. Порядок получения и обработки персональных данных

5.2. Защита персональных данных

5.3. Хранение персональных данных

5.4. Доступ к персональным данным

5.5. Передача персональных данных

5.6. Уничтожение персональных данных

5.7. Внутренние проверки состояния защищенности персональных данных

6. Права и обязанности субъекта персональных данных и Общества

7. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения

8. Нормативные ссылки

Приложение 1 – Согласие на обработку персональных данных

Приложение 2 – Согласие на передачу персональных данных третьей стороне

Приложение 3 – Обязательство о неразглашении персональных данных

1. Назначение и область применения

1.1. Положение разработано в соответствии с законодательством Российской федерации (Конституция РФ, Трудовой кодекс РФ, Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (далее – Федеральный закон от 27.07.2006 № 152-ФЗ), Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ и др.), направлено на обеспечение прав и свобод человека и гражданина при обработке его персональных данных и определяет порядок обращения с персональными данными в Обществе с ограниченной ответственностью «Инжиниринг» (далее – Компания).

1.2. Положение определяет политику Общества в отношении обработки персональных данных и устанавливает процедуры, направленные на предотвращение, а также выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

1.3. Положение является обязательным для исполнения всеми работниками Общества, вступает в силу с момента его утверждения и действует бессрочно.

2. Ответственность

2.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области обработки персональных данных субъектов персональных данных, привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном действующим Федеральными законами.

2.2. Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, установленных Федеральным законом от 27.07.2006 № 152-ФЗ, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

2.3. Работник, представивший работодателю подложные документы или заведомо ложные сведения о себе, несет дисциплинарную ответственность вплоть до увольнения.

3. Термины

Для целей настоящего Положения используются следующие понятия и термины:

- ***персональные данные*** - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) (п. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- ***оператор*** – Общество с ограниченной ответственностью «Инжиниринг» как юридическое лицо, самостоятельно организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- ***конфиденциальность информации*** – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (п. 7 ст. 2

Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»);

- ***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 (п. 3 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- ***обработка персональных данных без использования средств автоматизации*** – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченные из такой системы, считается осуществленной без использования средств автоматизации, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение ПД в отношении каждого субъекта ПД, осуществляется при непосредственном участии человека (п. 1,2 ч.1 Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»);
- ***автоматизированная обработка персональных данных*** - обработка персональных данных с помощью средств вычислительной техники (п. 4 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- ***биометрические персональные данные*** – сведения, которые характеризуют физиологические и биометрические особенности человека, на основании которых можно установить его личность и которые используются Обществом для установления личности субъекта персональных данных (п. 1 ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ);
- ***распространение персональных данных*** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (п. 5 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- ***предоставление персональных данных*** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц (п. 6 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- ***блокирование персональных данных*** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (п. 7 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- ***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 (п. 8 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- ***обезличивание персональных данных*** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (п. 9 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- ***информационная система персональных данных*** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (п. 10 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);

- ***трансграничная передача персональных данных*** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу (п. 11 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ).

4. Общие положения. Состав персональных данных

4.1. Персональные данные относятся к конфиденциальной информации, порядок работы с которыми регламентирован Федеральным законом от 27.07.2006 № 152-ФЗ и осуществляется с соблюдением строго определенных правил и условий.

4.2. Компания осуществляет обработку персональных данных физических лиц в рамках требований законодательства в следующих целях:

- выполнения трудового законодательства Российской Федерации;
- заключения договоров, сторонами которых являются субъекты персональных данных, при этом персональные данные субъектов не распространяются, а также не предоставляются третьим лицам без согласия субъектов персональных данных и используются Компанией исключительно для исполнения указанных договоров и заключения договоров с субъектами персональных данных;
- обеспечения выполнения договоров, заключенных Компанией с юридическими лицами по ведению учета и составлению отчетности;
- в иных целях, предусмотренных законодательством Российской Федерации и локальными нормативными актами Компании.

4.3. Компания обрабатывает персональные данные следующих категорий субъектов персональных данных:

- физические лица, являющиеся кандидатами на замещение вакантных должностей;
- физические лица, являющиеся работниками Компании;
- физические лица, осуществляющих выполнение работ, оказание услуг и заключивших с Компанией договор гражданско-правового характера;
- физические лица, являющиеся клиентами, а также руководителями, участниками (акционерами) или работниками юридического лица, являющегося клиентом (потенциальным клиентом, контрагентом) Компании;
- физические лица, персональные данные которых сделаны ими общедоступными, а их обработка не нарушает их прав и соответствует требованиям, установленным законодательством Российской Федерации;
- другие субъекты персональных данных (для обеспечения реализации целей обработки, указанных в п. 4.2. Положения).

4.4. Общество не осуществляет обработку специальных категорий персональных данных, касающихся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

4.5. В Компании могут обрабатываться следующие персональные данные в связи с реализацией трудовых отношений:

- фамилия, имя, отчество, дата и место рождения, гражданство, пол;
- прежние фамилия, имя, отчество, дата и причина изменения (в случае изменения);
- владение иностранными языками;
- сведения об образовании (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификации по диплому);

- сведения о послевузовском профессиональном образовании (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
- сведения о стаже (выполняемая работа с начала трудовой деятельности, включая военную службу и т.п.);
- занимаемая должность;
- государственные награды, иные награды и знаки отличия (кем награжден и когда);
- семейное положение (состояние в браке, фамилии, имена, отчества, даты рождения близких родственников (муж (жена), дети, отец, мать, близкие сестры и братья));
- адрес места жительства (по паспорту и фактический), дата регистрации по месту жительства;
- паспорт (серия, номер, кем и когда выдан, код подразделения), водительское удостоверение, иной документ удостоверяющий личность;
- паспорт, удостоверяющий гражданина РФ за пределами РФ (загранпаспорт РФ, серия, номер, кем и когда выдан);
- номер телефона;
- отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- идентификационный номер налогоплательщика;
- номер страхового свидетельства обязательного пенсионного страхования;
- наличие (отсутствие) заболевания, препятствующего приему на определенную должность, подтвержденное заключением медицинского учреждения;
- результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования;
- сведения о заработной плате работника и социальных льготах;
- сведения об аттестации, повышение квалификации, профессиональной переподготовке;
- фотографии и фотографические изображения, позволяющие идентифицировать личность;
- иные данные, которые с учетом специфики работы и в соответствии с законодательством РФ должны быть представлены субъектом персональных данных при заключении договора или в период его действия.

4.6. В Компании могут обрабатываться следующие персональные данные в связи с заключением гражданско-правовых договоров:

- фамилия, имя, отчество;
- дата и место рождения;
- паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ, код подразделения);
- гражданство;
- адрес места жительства (адрес регистрации и фактическое место проживания), дата регистрации по месту жительства или по месту пребывания;
- номера контактных телефонов;

- содержание и реквизиты гражданско-правового договора с физическим лицом;
- номер страхового свидетельства государственного пенсионного страхования;
- сведения об идентификационном номере налогоплательщика;
- сведения об образовании (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);
- сведения о стаже (выполняемая работа с начала трудовой деятельности, включая военную службу и т.п.);
- занимаемая должность;
- государственные награды, иные награды и знаки отличия (кем награжден и когда);
- семейное положение (состояние в браке, фамилии, имена, отчества, даты рождения близких родственников (муж (жена), дети, отец, мать, близкие сестры и братья));
- сведения о заработной плате работника и социальных льготах.

4.7. В отделе кадров Компании могут создаваться, храниться следующие группы документов, содержащие данные о работниках в единичном или сводном виде;

- документы, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении (копии следующих документов: паспорт или иной документ, удостоверяющий личность, документы воинского учета, свидетельство обязательного пенсионного страхования, документы об образовании, о составе семьи, справка о доходах с предыдущего места работы, медицинские заключения, свидетельства о заключении брака и рождении детей);
- документы по анкетированию, тестированию, проведению собеседований с кандидатом на должность;
- подлинники и копии приказов (распоряжений) по кадрам;
- личные дела, личная карточка работника по форме № Т-2 и трудовые книжки;
- дела, содержащие основания к приказу по личному составу;
- должностные инструкции работников;
- дела, содержащие материалы аттестаций работников;
- дела, содержащие материалы внутренних расследований;
- справочно-информационный банк данных по персоналу (картотеки, журналы);
- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Общества, руководителям структурных подразделений;
- копии отчетов, направляемые в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;
- приказы, распоряжения, указания руководства Общества;
- документы планирования, учета, анализа и отчетности по вопросам кадровой работы.

4.8. В отделе бухгалтерии могут храниться:

- документы, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;
- оригиналы и копии приказов (распоряжений) по кадрам;
- справочно-информационный банк данных по персоналу (картотеки, журналы);

- оригиналы и копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

4.9. Персональные данные могут храниться и в иных подразделениях Компании, если это необходимо для осуществления Компанией административно-хозяйственной и предпринимательской деятельности в соответствии с локальным нормативным актом, определяющим перечень таких данных и лиц, ответственных за их сохранность.

5. Обработка и обеспечение безопасности персональных данных

5.1. Порядок получения и обработки персональных данных

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

5.1.2. Все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (*Приложение 2*). Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

5.1.3. Работодатель не имеет права получать и обрабатывать персональные данные работника о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

5.1.4. Работодатель не имеет права получать и обрабатывать данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

5.1.5. Обработка персональных данных работников работодателем возможна только с их согласия либо без их согласия в следующих случаях:

- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья работника, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;
- по требованию полномочных государственных органов - в случаях, предусмотренных федеральным законом.

5.1.6. Работодатель вправе обрабатывать персональные данные работников только с их письменного согласия. Письменное согласие работника 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;
- наименование (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;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

5.1.7. Согласие работника не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия работодателя;
- обработка персональных данных в целях исполнения трудового договора;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

5.1.8. Работник Компании представляет в отдел кадров достоверные сведения о себе. Отдел кадров проверяет достоверность сведений.

5.1.9. В соответствии со ст. 86 Трудового кодекса РФ в целях обеспечения прав и свобод человека и гражданина руководитель Компании и его законные, полномочные представители при обработке персональных данных работника должны выполнять следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов или иных правовых актов, содействия работникам в трудоустройстве, обучении и профессиональном продвижении, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- при определении объема и содержания обрабатываемых персональных данных работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами;
- при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных, полученных о нем исключительно в результате их автоматизированной обработки или электронного получения;
- защита персональных данных работника от неправомерного их использования, утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральным законом;
- работники и их представители должны быть ознакомлены под расписку с документами Компании, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области;
- во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен;
- при принятии решений, затрагивающих интересы субъекта ПД, Компания не имеет права основываться на персональных данных субъекта ПД, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5.1.10. Обработка ПД прекращается при достижении целей такой обработки, а также по истечении срока, предусмотренного законом, договором или согласием субъекта ПД на обработку его ПД. При отзыве субъектом ПД согласия на обработку

его ПД обработка осуществляется в пределах, необходимых для исполнения, заключенного с ним договора и в целях, предусмотренных законодательством РФ.

5.2. Защита персональных данных

5.2.1. Обеспечение безопасности обрабатываемых ПД осуществляется Компанией в рамках единой комплексной системы организационно-технических и правовых мероприятий по защите информации, составляющей коммерческую тайну, с учетом требований законодательства о персональных данных, принятых в соответствии с ним нормативных правовых актов. Система информационной безопасности Компании непрерывно развивается и совершенствуется на базе требований международных и национальных стандартов информационной безопасности.

5.2.2. Защита персональных данных субъекта ПД от неправомерного их использования или утраты обеспечивается за счет средств Компании в порядке, установленном федеральными законами РФ в области защиты персональных данных.

5.2.3. Компания принимает следующие меры по организации обработки и обеспечения безопасности ПД, обрабатываемых без средств автоматизации, в том числе:

- для каждой категории ПД определены места хранения ПД (материальных носителей), установлен перечень лиц, осуществляющих обработку ПД и имеющих к ним доступ;
- обеспечено раздельное хранение ПД (материальных носителей), обработка которых осуществляется в различных целях;
- соблюдаются условия, обеспечивающие сохранность ПД, исключающие несанкционированный или случайный к ним доступ при хранении материальных носителей, а также иные неправомерные действия;
- применяются технические средства охраны;
- с работниками, которые в силу своих должностных обязанностей связаны с получением, обработкой и защитой персональных данных субъектов ПД, оформлены обязательства о неразглашении персональных данных (*Приложение 3*).

5.2.4. Обеспечение безопасности персональных данных, содержащихся в информационных системах, достигается, в частности, путем:

- определения уровней защищенности ПД при их обработке информационных системах;
- выполнения требований по защите ПД в информационных системах в соответствии с определенными уровнями защищенности ПД;
- применения необходимых средств защиты информации, использования сертифицированных программных и программно-аппаратных средств защиты информации, предотвращающих несанкционированный доступ третьих лиц к персональным данным субъектов ПД;
- осуществления оценки эффективности принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию информационных систем, содержащих персональные данные;
- осуществления учета машинных носителей ПД;
- обнаружения фактов несанкционированного доступа к персональным данным и принятия необходимых мер;
- осуществления восстановления ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установления правил доступа к ПД, обрабатываемых в информационных системах, а также регистрации и учета действий, совершаемых с ПД в

информационных системах, там, где это необходимо;

- контролирования принимаемых мер по обеспечению безопасности ПД и уровня защищенности информационных систем.

5.2.5. В целях обеспечения сохранности и конфиденциальности персональных данных работников Компании все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только работниками отдела кадров, бухгалтерии осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

5.2.6. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке предприятия и в том объеме, который позволяет не разглашать излишний объем персональных сведений о работниках предприятия.

5.2.7. Передача информации, содержащей сведения о персональных данных работников организации, по телефону, факсу, электронной почте без письменного согласия работника запрещается.

5.2.8. Личные дела и документы, содержащие персональные данные работников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

5.2.9. Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

5.2.10. «Внешняя защита» персональных данных:

5.2.10.1. Для защиты конфиденциальной информации (персональных данных работников) 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.

5.2.10.2. 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 в структурных подразделениях Компании.

5.2.10.3. Для обеспечения внешней защиты персональных данных работников необходимо соблюдать ряд мер:

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

5.2.10.4. Функция внешней защиты персональных данных работников в отношении мер, указанных в п. 5.2.10.3., возлагается на Управление безопасности.

5.2.11. По возможности персональные данные обезличиваются.

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

5.3. Хранение персональных данных

5.3.1. Компания обеспечивает раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5.3.2. Сведения о субъектах ПД на бумажных носителях должны храниться в металлических шкафах либо в сейфах в помещениях, оборудованных надежными замками (ключи от данных помещений должны находится у лиц, имеющих доступ в ПД в соответствии с локальным нормативным актом). Все помещения в рабочее время при отсутствии в них ответственных работников должны быть закрыты. Проведение уборки в данных помещениях осуществляется в присутствии ответственного лица.

5.3.3. Обязанности по хранению сведений о субъектах ПД, заполнению, хранению и выдаче документов, содержащих персональные данные, возлагается на лицо, ответственное за организацию обработки персональных данных.

5.3.4. Съемные электронные носители, на которых хранятся резервные копии персональных данных субъектов ПД, должны быть промаркированы и учтены в журнале регистрации, учета и выдачи внешних носителей для хранения резервных копий ПД.

5.3.5. В процессе хранения персональных данных субъектов ПД обеспечивается контроль за достоверностью и полнотой персональных данных, их регулярным обновлением и внесение по мере необходимости соответствующих изменений.

5.4. Доступ к персональным данным

5.4.1. Право доступа к персональным данным работников определены должности работников (Приложение 4), имеющих доступ к персональным данным, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения и решения поставленных задач.

5.4.2. Работник Компании имеет право:

- получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копии любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом;
- требовать от работодателя уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для работодателя персональных данных, а также данных обработанных с нарушением требований Трудового кодекса РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- получать от работодателя о наименовании и месте нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- требовать извещения работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия работодателя при обработке и защите его персональных данных.

5.5. Передача персональных данных

5.5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

5.5.1.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом.

5.5.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия. Обработка персональных данных работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

5.5.1.3. Предупредить лиц, получивших персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

5.5.1.4. Осуществлять передачу персональных данных работников в пределах Компании в соответствии с настоящим Положением.

5.5.1.5. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

5.5.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

5.5.1.7. Передавать персональные данные работника его законным, полномочным представителям в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции.

5.5.2. Персональные данные работников обрабатываются и хранятся на бумажных носителях в отделе кадров, в электронной версии (программа 1С Предприятие) – в бухгалтерии Компании.

5.5.3. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

Персональные данные на бумажных носителях (личные дела и личные карточки работников) хранятся в отделе кадров в специальном шкафу, закрывающимся на ключ и обеспечивающим защиту от несанкционированного доступа. Трудовые книжки хранятся в несгораемом металлическом сейфе.

Персональные данные на электронных носителях хранятся в программе «1С: Зарплата и кадры». Доступ к данной программе имеют Руководитель Компании и сотрудники бухгалтерии Компании. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечивается системой паролей.

5.5.4. Автоматизированная обработка и хранение персональных данных работников допускаются только после выполнения всех основных мероприятий по защите информации.

5.5.5. При получении персональных данных не от работника (за исключением случаев, если персональные данные являются общедоступными) работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные федеральными законами права субъекта персональных данных.

5.5.6. Внешний доступ к персональным данным работников имеют контрольно-ревизионные органы при наличии документов, на основании которых они проводят проверку. Дистанционно персональные данные работников могут быть представлены контрольно-надзорным органам (органы прокуратуры, судебные органы, налоговые органы и государственные пенсионные фонды) только по письменному запросу. Страховые фонды, негосударственные пенсионные фонды, другие организации, а также родственники и члены семьи работника не имеют доступа к персональным данным работника, за исключением наличия письменного согласия самого работника.

5.5.7. После увольнения работника в личное дело вносятся соответствующие документы (заявление работника о расторжении трудового договора, копия приказа об увольнении), дело передается на хранение.

5.5.8. Компания не осуществляет трансграничную передачу персональных данных.

5.6. Уничтожение персональных данных

5.6.1. Оператор обязан уничтожить персональные данные субъекта (или обеспечить их уничтожение):

- при представлении субъектом персональных данных (или его представителем) сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки - в течение семи рабочих дней со дня представления таких сведений (ч. 1 ст. 14, ч. 3 ст. 20 Закона N 152-ФЗ);
- при выявлении неправомерной обработки персональных данных, если невозможно обеспечить ее правомерность, - в течение десяти рабочих дней с даты выявления неправомерной обработки персональных данных (ч. 3 ст. 21 Закона N 152-ФЗ);
- при достижении цели обработки персональных данных - в течение 30 дней с даты достижения цели обработки персональных данных (ч. 4 ст. 21 Закона N 152-ФЗ);
- при отзыве субъектом персональных данных согласия на обработку его персональных данных, если их сохранение более не требуется для целей обработки персональных данных, - в течение 30 дней с даты поступления указанного отзыва (ч. 5 ст. 21 Закона N 152-ФЗ).

5.6.2. Однако при достижении цели обработки персональных данных и при отзыве субъектом персональных данных согласия на обработку его персональных данных

может применяться другой срок для уничтожения персональных данных субъекта, если:

- он предусмотрен договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных;
- он предусмотрен иным соглашением между оператором и субъектом персональных данных;
- если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Законом N 152-ФЗ или другими федеральными законами (ч. 7 ст. 5, ч. 4, 5 ст. 21 Закона N 152-ФЗ).

5.6.3. Таким образом, общий срок уничтожения персональных данных оператором при достижении цели обработки персональных данных, а также при отзыве субъектом персональных данных согласия на обработку его персональных данных составляет 30 дней с даты достижения цели обработки персональных данных или с даты поступления указанного отзыва.

5.6.4. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в ч.3 – 5 ст. 21 Закона № 152-ФЗ, оператор осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами (ч. 6 ст. 21 Закона № 152-ФЗ).

5.6.5. Порядок документального оформления факта уничтожения персональных данных субъекта персональных данных законодательно не установлен, поэтому он определяется оператором персональных данных самостоятельно.

5.6.6. Уничтожение персональных данных осуществляется комиссией (либо иным должностным лицом), созданной (уполномоченным) на основании оператора. Как правило, факт уничтожения персональных данных оформляется актом о прекращении обработки персональных данных либо регистрируется в специальном журнале. Формы акта и журнала утверждаются оператором самостоятельно.

5.7. Внутренние проверки состояния защищенности персональных данных

5.7.1. Лицо, ответственное за безопасность персональных данных в информационной системе, совместно с лицом, ответственным за организацию обработки персональных данных, проводит внутренние проверки состояния их защищенности и аудит соответствия обработки персональных данных в Компании требованиям действующего законодательства российской Федерации. Внутренние проверки и аудит проводятся ежегодно или в любое время по инициативе руководства Компании.

5.7.2. Внутренняя проверка состояния защищенности ПД осуществляется с целью определения соответствия нормативных, организационных, практических и технических мероприятий, реализуемых Компанией, требованиям законов и иных нормативных правовых актов российской Федерации в области информационной безопасности и защиты персональных данных.

5.7.3. Внутренняя проверка состояния защищенности включает в себя:

- определение характера обрабатываемых персональных данных и установленных режимов их обработки;

- определение актуальности организационно-распорядительной документации, учитывающей конкретные условия функционирования средств вычислительной техники различного уровня и назначения (рабочие станции пользователей, серверное и периферийное оборудование, технические средства защиты информации, в том числе средства криптографической защиты информации), порядок работы сотрудников организации при эксплуатации средств вычислительной техники;
- анализ принятых мер (программных, технических, организационных, правовых), обеспечивающих защиту средств вычислительной техники, информационной системы и баз данных от несанкционированного доступа, оценка продуктивности организационного процесса защиты информации. Достаточность технических средств обработки и защиты информации, наличие подтверждений соответствия по требованиям информационной безопасности (сертификатов соответствия);
- проведение анализа конфигураций активного сетевого оборудования, маршрутизаторов, коммутаторов, серверов с целью выявления уязвимых мест в системе защиты информации;
- проведение инструментального анализа сетевого и серверного оборудования локально-вычислительных сетей, информационных систем и баз данных с применением программно-аппаратных средств;
- внутренняя проверка работоспособности используемых программных и программно-аппаратных средств обнаружения и предотвращения компьютерных атак;
- внутренняя проверка наличия лицензионных средств защиты от вредоносных программ и вирусов или сертифицированных свободно распространяемых антивирусных средств защиты;
- внутренняя проверка оснащения серверных и кроссовых помещений средствами контроля доступа и пожаротушения, обеспечения температурного режима, регламент доступа к серверным и кроссовым помещениям;
- внутренняя проверка состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва);
- внутренняя проверка состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов);
- проверка мест хранения персональных данных на бумажных носителях;
- проверка соблюдения режима доступа к персональным данным на бумажных носителях;
- иные мероприятия, необходимые для обеспечения конфиденциальности ПД.

5.7.4. Внутренняя проверка мероприятий по защите персональных данных завершается составлением акта о результатах проверки состояния защищенности ПД. Акт должен содержать: дата, время и место составления акта и проведения проверки; сведения о результатах проверки, в том числе о выявленных нарушениях в их характере; достоверное и обоснованное изложение состояния защищенности информационной системы и ресурсов, выявленных недостатков и нарушений со ссылками на соответствующие документы и факты, выводы и предложения по их устранению с указанием конкретных сроков.

6. Права и обязанности субъекта персональных данных и Компании

6.1. Субъект персональных данных имеет право:

6.1.1. Требовать от Компании уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.1.2. Получать полную информацию, касающуюся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Компание1;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Компанией способы обработки персональных данных;
- сведения о лицах (за исключением работников Компании), которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных, относящихся к соответствующему субъекту ПД, и источник их получения, если иной представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- иные сведения, предусмотренные действующим законодательством Российской Федерации.

6.1.3. Получать свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта ПД, за исключением случаев, предусмотренных законодательством.

6.1.4. Определять представителей для защиты своих персональных данных.

6.1.5. Требовать исключить или исправить неверные, или неполные персональные данные, а также данные, обрабатываемые с нарушением требований законодательства о персональных данных.

6.1.6. Требовать об извещении Компанией всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта ПД, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.1.7. Обжаловать в судебном порядке любые неправомерные действия или бездействия Компании при обработке и защите его персональных данных.

6.2. В целях обеспечения достоверности персональных данные субъект ПД обязан предоставлять полные и достоверные данные о себе и своевременно уведомлять в случае изменения своих ПД.

6.3. Компания имеет право:

- обрабатывать персональные данные субъекта ПД в соответствии с заявленной целью;
- поручить обработку персональных данных третьему лицу с согласия субъекта персональных данных;
- требовать от субъекта ПД предоставления достоверных персональных данных, необходимых для исполнения договора, оказания услуги, идентификации субъекта персональных данных, а также в иных случаях, предусмотренных законодательством о персональных данных;
- обрабатывать общедоступные персональные данные.

6.4. Компания обязана:

- предоставить по просьбе субъекта персональных данных информацию, касающуюся обработки его персональных данных, указанную в пункте 6.1.2. настоящего Положения;
- разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с федеральным законом;
- обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ;
- осуществлять защиту персональных данных субъекта ПД;
- вести журнал учета обращений субъектов персональных данных по вопросам обработки их ПД;
- обеспечивать хранение документации, содержащей персональные данные субъектов ПД, при этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

7. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения

7.1. Согласие на обработку персональных данных, разрешенных субъектом ПД для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

7.2. В случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия, предусмотренного настоящей статьей, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

7.3. В случае, если персональные данные оказались раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

7.4. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без права распространения.

7.5. В случае, если из предоставленного субъектом ПД согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных не установил запреты

и условия на обработку персональных данных, предусмотренные пунктом 7.9. настоящего Положения, или если в предоставленном субъектом персональных данных таком согласии не указаны категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты в соответствии с пунктом 7.9. настоящего Положения, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц.

7.6. Согласие на обработку персональных данных, разрешенных субъектом ПД для распространения, может быть предоставлено оператору:

- непосредственно;
- с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных (в ред. ФЗ от 30.12.2020 N 519-ФЗ) вступает в силу с 01.07.2021).

7.7. Правила использования информационной системы уполномоченного органа по защите прав субъектов персональных данных, в том числе порядок взаимодействия субъекта персональных данных с оператором, определяются уполномоченным органом по защите прав субъектов персональных данных.

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

7.9. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом персональных данных запретов и условий, предусмотренных настоящей статьей, не допускается.

7.10. Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.

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

7.12. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании

персональные данные могут обрабатываться только оператором, которому оно направлено.

7.13. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления оператору требования, указанного в пункте 7.12. настоящего Положения.

7.14. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений настоящей статьи или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

7.15. Требования пункта 7 настоящего Положения не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления функций, полномочий и обязанностей.

8. Нормативные ссылки

8.1. Конституция Российской Федерации.

8.2. Трудовой кодекс Российской Федерации.

8.3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

8.4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

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

8.6. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

8.7. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

8.8. Федеральный закон от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»».

Приложение 1
к положению о персональных данных

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(фамилия, имя, отчество полностью)

паспорт серии _____ № _____, выдан _____
(дата выдачи, наименование

_____
выдавшего органа)

_____

зарегистрированный(ая) по адресу: _____

даю согласие ООО «Инжиниринг», расположенному по адресу: 300012, г. Тула, ул. Тимирязева, д 99В, на обработку (любое действие (операцию) 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) следующих персональных данных:

фамилия, имя, отчество, дата и место рождения, гражданство, пол; прежние фамилия, имя, отчество, дата и причина изменения (в случае изменения); паспорт (серия, номер, кем и когда выдан), водительское удостоверение, иной документ удостоверяющий личность; паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан); номер телефона; владение иностранными языками; сведения об образовании (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому); сведения о послевузовском профессиональном образовании (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов); сведения о стаже: выполняемая работа с начала трудовой деятельности, включая военную службу и т.п.; занимаемая должность; государственные награды, иные награды и знаки отличия (кем награжден и когда); семейное положение: состояние в браке, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер, детей, мужа (жены)); адрес места жительства (по паспорту и фактический), дата регистрации по месту жительства; отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу); идентификационный номер налогоплательщика; номер страхового свидетельства обязательного пенсионного страхования; наличие (отсутствие) заболевания, препятствующего приему на определенную должность, подтвержденное заключением медицинского учреждения; результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования; сведения о заработной плате работника и социальных льготах; сведения об аттестации, повышении квалификации, профессиональной переподготовке; фотографии и фотографические изображения (в том числе и в электронном виде), позволяющие идентифицировать личность; иные данные, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть представлены субъектом персональных данных при заключении договора или в период его действия.

Вышеуказанные персональные данные предоставляю в ООО «Инжиниринг» в целях обеспечения соблюдения законодательства Российской Федерации, содействия в трудоустройстве, получении образования и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Настоящим даю свое согласие на передачу моих персональных данных и их обработку (сбор, запись, систематизацию, накопление, хранение, передачу, уточнение, извлечение, использование, обезличивание, блокирование, удаление, уничтожение) в ООО «Инжиниринг» (адрес: г. Тула, ул. Тимирязева, д 99 В) в целях расчета и начисления заработной платы, исчисления и уплаты налогов, сборов и взносов на обязательное социальное и пенсионного страхование, представления установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС РФ, сведений в ФСС РФ, предоставлять сведения в банк для оформления банковской карты и перечисления заработной платы на карты, и третьим лицам для оформления полиса ДМС, получения образования, а также предоставлять сведения в случаях, предусмотренных федеральными законами и иными нормативно-правовыми актами.

Также в целях информационного обеспечения деятельности ООО «Инжиниринг» даю согласие на включение моих персональных данных (фамилия, имя, отчество; номер телефона и адрес рабочей электронной почты; должность, место работы; анкетные данные; сведения о профессии и образовании; служебная фотография) в общедоступные источники персональных данных (телефонный справочник, адресная книга электронной корпоративной почты, корпоративный сайт и Интернет).

Я ознакомлен(а), что:

Приложение 2
к положению о персональных данных

СОГЛАСИЕ
на передачу персональных данных третьей стороне

Я, _____
(фамилия, имя, отчество полностью)

паспорт серии _____ № _____, выдан _____
(дата выдачи, наименование

_____
выдавшего органа)

_____

зарегистрированный(ая) по адресу: _____
даю согласие ООО «Инжиниринг», расположенному по адресу: 300012, г. Тула, ул. Тимирязева, д 99В, на передачу следующих персональных данных:

_____
(указать перечень передаваемых персональных данных)

_____

_____

_____

другому лицу: _____
(наименование или ФИО и адрес лица, осуществляющего обработку персональных данных по поручению работодателя)

_____

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

«_____» _____202__г. _____ _____
(подпись) (расшифровка подписи)

Приложение 3
к положению о персональных данных

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных

Я, _____
(фамилия, имя, отчество полностью)

паспорт серии _____ № _____, выдан _____
(дата выдачи, наименование

_____
выдавшего органа)

_____

Предупрежден(а), что в период исполнения должностных обязанностей мне будет предоставлен доступ к персональным данным, обрабатываемым в ООО «Инжиниринг», в т.ч. передаваемым третьими лицами.
Объем обрабатываемых персональных данных включает в себя: фамилия, имя, отчество, дата и место рождения, гражданство, пол; прежние фамилия, имя, отчество, дата и причина изменения (в случае изменения); паспорт (серия, номер, кем и когда выдан), водительское удостоверение, иной документ удостоверяющий личность; паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан); номер телефона; владение иностранными языками; сведения об образовании (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому); сведения о послевузовском профессиональном образовании (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов); сведения о стаже: выполняемая работа с начала трудовой деятельности, включая военную службу и т.п.; занимаемая должность; государственные награды, иные награды и знаки отличия (кем награжден и когда); семейное положение: состояние в браке, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер, детей, мужа (жены)); адрес места жительства (по паспорту и фактический), дата регистрации по месту жительства; отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу); идентификационный номер налогоплательщика; номер страхового свидетельства обязательного пенсионного страхования; наличие (отсутствие) заболевания, препятствующего приему на определенную должность, подтвержденное заключением медицинского учреждения; результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования; сведения о заработной плате работника и социальных льготах; сведения об аттестации, повышении квалификации, профессиональной переподготовке; фотографии и фотографические изображения (в том числе и в электронном виде), позволяющие идентифицировать личность; иные данные, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть представлены субъектом персональных данных при заключении договора или в период его действия.

Я добровольно принимаю на себя обязательства:

1) Не разглашать (не передавать) третьим лицам конфиденциальные сведения о персональных данных субъектов персональных данных, которые мне доверены (будут доверены), известны (станут известны) в связи с выполнением моих должностных обязанностей.

2) Не использовать конфиденциальные сведения о субъектах персональных данных с целью получения выгоды.

3) В случае попытки третьих лиц получить от меня конфиденциальные сведения сообщать непосредственному руководителю.

4) Прекратить обработку персональных данных, ставших мне известных в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных субъектов персональных данных, или их утраты я несу ответственность в соответствии со ст. 90 ТК РФ.

«_____» _____202__г. _____ _____
(подпись) (расшифровка подписи)

Приложение 2
к приказу от 01.03.2021 года № 66-к

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ

работников ООО «Инжиниринг», допущенных к работе с персональными данными

1. Генеральный директор
2. Советник генерального директора
3. Исполнительный директор
4. Главный инженер
5. Заместитель главного инженера по строительству
6. Заместитель главного инженера по производству
7. Заместитель исполнительного директора
8. Заместитель генерального директора по безопасности
9. Коммерческий директор
10. Советник исполнительного директора по закупкам и снабжению
11. Советник исполнительного директора по управлению проектами
12. Помощник исполнительного директора по экономическим вопросам
13. Начальник службы управления проектами
14. Заместитель начальника службы управления проектами
15. Руководитель проектов службы управления проектами
16. Помощник руководителя проектов службы управления проектами
17. Начальник тендерного отдела
18. Заместитель начальника тендерного отдела
19. Ведущий специалист тендерного отдела
20. Начальник отдела развития
21. Ведущий специалист отдела развития
22. Начальник отдела материально-технического снабжения
23. Заместитель начальника отдела материально-технического снабжения
24. Начальник сметного отдела
25. Заместитель начальника сметного отдела
26. Главный бухгалтер
27. Заместитель главного бухгалтера
28. Ведущий бухгалтер
29. Начальник финансово-экономического отдела
30. Главный специалист финансово-экономического отдела
31. Начальник отдела правового обеспечения
32. Главный юрисконсульт отдела правового обеспечения
33. Специалист 1 категории отдела правового обеспечения
34. Руководитель секретариата
35. Помощник руководителя
36. Начальник отдела управления персоналом
37. Главный специалист управления персоналом
38. Начальник отдела кадров
39. Главный специалист отдела кадров
40. Начальник управления безопасности
41. Начальник отдела внутреннего контроля
42. Главный специалист отдела внутреннего контроля
43. Ведущий специалист отдела внутреннего контроля
44. Начальник отдела экономической безопасности

45. Главный специалист отдела экономической безопасности
46. Начальник административно-хозяйственного отдела
47. Заместитель начальника административно-хозяйственного отдела
48. Заведующий хозяйством административно-хозяйственного отдела
49. Начальник складского хозяйства
50. Начальник отдела корпоративных и технологических АСУ
51. Заместитель начальника отдела корпоративных и технологических АСУ
52. Главный специалист по сопровождению 1С отдела корпоративных и технологических АСУ
53. Ведущий специалист отдела корпоративных и технологических АСУ
54. Начальник департамента проектирования
55. Заместитель начальника департамента проектирования
56. Помощник начальника департамента проектирования
57. Начальник отдела проектирования первичных систем департамента проектирования
58. Руководитель строительной группы департамента проектирования
59. Начальник отдела проектирования систем департамента проектирования
60. Начальник производственно-технического отдела
61. Заместитель начальника производственно-технического отдела
62. Начальник отдела по сопровождению производственной деятельности
63. Заместитель начальника отдела по сопровождению производственной деятельности
64. Главный механик отдела механизации строительства
65. Механик отдела механизации строительства
66. Диспетчер отдела механизации строительства
67. Начальник отдела охраны труда и промышленной безопасности
68. Заместитель начальника отдела охраны труда и промышленной безопасности
69. Начальник производственной базы обособленного производственного подразделения «Производственная база в г. Ефремове Тульской области
70. Заместитель начальника производственной базы обособленного производственного подразделения «Производственная база в г. Ефремове Тульской области
71. Начальник службы линий электропередач и подстанций
72. Заместитель начальника службы линий электропередач и подстанций
73. Начальник службы релейной защиты и автоматики
74. Заместитель начальника службы релейной защиты и автоматики

Приложение 3
к приказу от 01.03.2021 года № 66-к

МЕСТА ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Персональные данные, необходимые для осуществления кадрового учета, хранятся в кабинете отдела кадров и управления персоналом, в сейфах и шкафах, запираемые на ключ.

2. Персональные данные, необходимые для начисления заработной платы, хранятся в кабинете бухгалтерии, в сейфах и шкафах, запираемые на ключ.

3. Персональные данные, обрабатываемые в информационной системе, хранятся на жестком диске (сервере) в серверной комнате, запираемой на ключ.

Приложение 4
к приказу от 01.03.2021 года № 66-к

Инструкция
для работы с персональными данными для сотрудников ООО «Инжиниринг», имеющих доступ к персональным данным

В документе использованы следующие термины и определения:

1. ***База данных*** (далее – БД) – централизованное хранилище информации, оптимизированное для многопользовательского доступа и работающее под управлением системы управления базами данных (далее – СУБД).

2. ***Комплекс программных средств*** (далее – КПС) – система или приложение, использующее непосредственный доступ к БД.

3. ***Идентификатор*** (учетное имя или login) – присвоенная пользователю индивидуально буквенно-числовая последовательность, используемая для идентификации пользователя при установлении доступа к Б, и позволяющая однозначно определять работу конкретного пользователя в БД.

4. ***Пароль*** – секретная персональная последовательность символов, известная только пользователю, которая используется совместно с идентификатором для доступа в БД и позволяет подтвердить, что доступ к Б, осуществляет именно конкретный пользователь.

5. ***Пользователи*** – должностные лица ООО «Инжиниринг», имеющие доступ к персональным данным.

6. ***Администратор БД***. должностное лицо ООО «Инжиниринг», уполномоченное для выполнения административных функций и обеспечивающие функционирование БД и ее безопасность соответственно.

7. ***Локально-вычислительная сеть*** (далее –ЛВС) – группа компьютеров, а также периферийное оборудование, объединенные одним или несколькими автономными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

8. ***Политика информационной безопасности*** – комплекс организационно-технических мероприятий, правил и условий использования информационных систем ООО «Инжиниринг», определяющих нормальное функционирование систем и обеспечение безопасности информации, обрабатываемой в ООО «Инжиниринг».

Общие положения по организации доступа к персональным данным

1. Инструкция пользователя определяет комплекс организационных и технических мероприятий по обеспечению безопасности персональных данных конфиденциальной информации, хранящейся в ООО «Инжиниринг», в том числе в информационной системе.

2. Инструкция является частью политики информационной безопасности ООО «Инжиниринг» и предназначена для обеспечения эффективной организации и управления доступом пользователей к персональным данным, хранящимся в Обществе.

3. Для обеспечения безопасности БД, используемых ООО «Инжиниринг», администратор осуществляет следующие мероприятия:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее – машинные носители персональных данных);
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее – инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

4. Требования Инструкции пользователя обязательны для выполнения всеми работниками ООО «Инжиниринг», имеющим доступ к персональным данным.

5. Доступ к персональным данным предоставляется исключительно лицам, входящим в перечень должностей, утвержденный приказом.

6. При возникновении ситуаций, не указанных в настоящей Инструкции, пользователь обращается к системному администратору.

7. Для доступа к информационной системе ООО «Инжиниринг» у каждого пользователя БД должен быть свой уникальный идентификатор и пароль доступа к БД, который выдает системный администратор.

8. Доступ к информационной системе ООО «Инжиниринг» может быть предоставлен с любого компьютера локальной сети.

9. Доступ к БД предоставляются пользователем на срок действия их трудовых отношений и исполнения служебных обязанностей.

10. В случае расторжения трудового договора лицом, имеющим доступ к персональным данным, работники отдела кадров в течение одного рабочего дня уведомляет системного администратора, который блокирует доступ увольняемого лица к БД.

Обязанности и ответственность пользователей

1. Перед началом работы с конфиденциальной информацией пользователь обязан изучить законодательство о персональных данных, а также локальные акты ООО

«Инжиниринг» о защите персональных данных, а также подписать «Обязательство о неразглашении персональных данных».

2. Пользователь несет ответственность за выполнение требований законодательства и локальных актов в области защиты персональных данных.

3. Пользователю запрещается передавать и сообщать кому-либо персональные данные лиц, ставшие ему известными в силу выполнения должностных обязанностей.

4. Пользователю запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа к конфиденциальной информации другим лицам. Запрещается хранение пароля в общедоступных местах, позволяющих другим лицам получить информацию о пароле.

5. Пользователь конфиденциальной информации обязан обеспечивать правильность ввода и коррекции персональных данных в БД, за которые отвечает.

6. Пользователь обязан закрывать соединение с БД на время своего отсутствия у компьютера.

7. В случае выявления инцидентов с доступом к БД (фактов несанкционированного доступа посторонними людьми, людьми без допуска к конфиденциальным данным, фактов несанкционированного доступа к БД, блокировки доступа, утери или компрометации пароля и т.п.) пользователь обязан незамедлительно сообщить об этом системному администратору.

8. Установку и конфигурирование программного обеспечения на компьютерах с доступом к персональным данным выполняет системный администратор. Пользователям данных рабочих мест запрещается самостоятельно устанавливать какое-либо программное обеспечение.

9. Пользователю запрещается использовать информацию, полученную в результате доступа к персональным данным, в целях, не предусмотренных его функциональными обязанностями и технологическими схемами.

10. Пользователь несет ответственность за все действия, совершенные от имени его идентификатора, учетной записи или логина, если не доказан факт несанкционированного использования таковых.

11. При работе с персональными данными на бумажных носителях пользователь обеспечивает их хранение в местах, исключающих доступ к ним третьих лиц на весь период хранения, в соответствии с перечнем мест хранения информации.

12. Все документы, содержащие персональные данные, не используемые в работе, хранятся в местах, исключающих доступ к ним третьих лиц, куда они помещаются после окончания работы и/или при уходе пользователя с рабочего места, в т.ч. во время перерыва на отдых и питание.