



АСТ

Территориальная
Электросетевая
Компания
Территориаль
Электр сеттерзаре
Компанияны

Общество с ограниченной ответственностью «Автоматизация Системы Технологии»
(ООО «АСТ»)

ПРИКАЗ

20 05 2021 г.

№ ПД-336

г. Стерлитамак

О введение в действие Положение
об обработке и защите персональных
данных работников ООО «АСТ»

В целях исполнения требований Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, требований к обработке персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687, Приказа Роскомнадзора от 30.05.2017 № 94 «Об утверждении Методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения», а также иными нормативными документами по защите персональных данных,

ПРИКАЗЫВАЮ:

1. Ввести в действие Положение об обработке и защите персональных данных работников ООО «АСТ» (далее по тексту - Положение) с даты подписания настоящего приказа (Приложение 1 к настоящему приказу).

2. Назначить ответственным лицом:

2.1. За организацию обработки персональных данных работников ООО «АСТ» (далее по тексту - Предприятие) - начальника отдела по управлению персоналом (далее по тексту - ОУП) Макарову М. В.;

2.2. За организацию мероприятий по защите информационных систем персональных данных – начальника отдела информационных технологий (далее по тексту-ОИТ) Маринич А.А.

2.3. За организацию общих мероприятий по обеспечению безопасности персональных данных и контролю за их выполнением - заместителя генерального директора по безопасности Гайсина И.А.

3. Создать комиссию по проведению служебных проверок по фактам нарушения требований Положения и определению уровня защищенности персональных данных в Организации в следующем составе:

председатель комиссии: заместитель генерального директора по безопасности Гайсин И.А.;

члены комиссии:

- начальник ОУП Макарова М.В.,

- начальник отдела правового обеспечения и управления собственностью Утина О.А.,

- ведущий инженера-программист ОИТ Юлтимирова Ф.К.,

- начальник канцелярии Малиновская И.В.

4. Начальнику ОИТ Маринич А.А.:

4.1. Организовать мероприятия по недопущению несанкционированного доступа сторонних лиц к персональным данным работников через информационные системы Организации.

Срок: постоянно

4.2. Осуществлять постоянный контроль за порядком использования лицами, допущенными к работе с персональными данными (операторами), информационных систем персональных данных, в соответствии требованиями Положения.

Срок: постоянно

4.3. Направить в Управление Роскомнадзора по Республике Башкортостан Уведомление об обработке персональных данных для включения ООО «АСТ» в Реестр операторов, осуществляющих обработку персональных данных.

Срок: в течение 10 рабочих дней со дня утверждения приказа.

4.4. Утвердить Политику защиты и обработки персональных данных и разместить её на официальном сайте ООО «АСТ».

Срок: в течение 10 рабочих дней со дня утверждения приказа.

Ответственный: начальник ОИТ Маринич А.А.

5. По каждому факту нарушения требований Положения организовывать проведение служебных проверок с предоставлением заключения на имя генерального директора.

Ответственный: Гайсин И.А.

Срок: постоянно

7. Секретарю руководителя Федоровой Е.В. ознакомить руководителей структурных подразделений в системе ЭДО с настоящим приказом в течение одного рабочего дня с даты утверждения приказа.

8. Руководителям структурных подразделений ознакомить персонал с Положением под подпись, с предоставлением подписных листов в канцелярию.

Ответственный: руководители структурных подразделений.

Срок: в течение 10 рабочих дней с даты утверждения приказа.

9. Контроль за исполнением приказа возложить на заместителя генерального директора по безопасности Гайсина И.А.

Генеральный директор

Ю.В. Кузнецов

Исп. ЗГД по безопасности

И.А. Гайсин 89872468610

Разослать: все структурные подразделения ООО «АСТ»

 АСТ Территориальные Автоматизированные Системы Технологии Систем Технологии	Общество с ограниченной ответственностью «Автоматизация Систем Технологии» (ООО «АСТ»)	
---	--	--

Приложение 1

УТВЕРЖДЕНО

Приказом

генерального директора

№ 336

от 20 05 2021 г.

ПОЛОЖЕНИЕ
 об обработке и защите персональных данных
 работников Общества с ограниченной ответственностью
 «Автоматизация Систем Технологии»

1. Общие положения

1.1. Настоящим Положением определяются порядок осуществления операций с персональными данными работников Общества с ограниченной ответственностью «Автоматизация Системы Технологии», (далее по тексту – Организация), и порядок их защиты от несанкционированного доступа.

1.2. Настоящее Положение разработано на основе и во исполнение следующих нормативно-правовых актов: части 1 статьи 23, статьи 24 Конституции Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», положений главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников», «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных Постановлением Правительства РФ от 01.11.2012 N 1119. Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

1.3. Положение определяет права и обязанности работников Организации при проведении операций с персональными данными, а также порядок взаимодействия в процессе их сбора, документирования, систематизации, хранения, передачи персональных данных и уничтожения их носителей.

1.4. Приказом Генерального директора назначается лицо, ответственное за организацию процесса обработки персональных данных в Организации (приложение 1).

1.5. Сведения о персональных данных работников относятся к категории конфиденциальных (охраняемых законом в Организации). Режим конфиденциальности в отношении персональных данных снимается в случае их обезличивания, а именно:

Документы по работникам, законченные делопроизводством до 1 января 2003 года, хранятся 75 лет.

Документы по работникам, законченные делопроизводством после 1 января 2003 года, хранятся 50 лет, в других случаях, предусмотренных федеральными законами.

1.6. Настоящее Положение вступает в силу с момента его утверждения Генеральным директором Организации и действует бессрочно, до замены его новым Положением. Все изменения в Положение вносятся соответствующими приказами.

2. Основные понятия персональных данных работников

2.1. Для реализации целей настоящего Положения используются следующие основные понятия:

персональные данные работника - любая информация, относящаяся к данному работнику (субъекту персональных данных) и необходимая Организации (оператору персональных данных) в соответствии с трудовым законодательством, в том числе:

- фамилия, имя, отчество работника;
- дата и место рождения работника;
- адрес места жительства работника;
- домашний телефон;
- семейное, социальное, имущественное положение работника;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате работника;
- сведения о социальных льготах;
- образование, профессия сотрудника, занимаемая должность;
- наличие судимостей;
- содержание трудового договора;

- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки работника;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, результатам служебных расследований;
- копии отчетов, направляемые в органы статистики;
- другая аналогичная информация, на основании которой возможна безошибочная идентификация субъекта персональных данных.

Перечень персональных данных, подлежащих обработке, зависит от субъекта обработки персональных данных (приложение 2).

обработка персональных данных работника - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение носителей персональных данных;

конфиденциальность персональных данных - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;

распространение персональных данных - действия, направленные на передачу персональных данных работников определенному кругу лиц (передача персональных данных) или ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или представление доступа к персональным данным работников каким-либо иным способом;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

использование персональных данных - действия (операции) с персональными данными, совершаемые уполномоченным должностным лицом Организации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

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

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

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

персональные данные, разрешенные субъектом персональных данных для распространения - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

информация - сведения (сообщения, данные) независимо от формы их представления;

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

носитель - материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

3. Создание, обработка и хранение персональных данных работника

3.1. Информация, представляемая работником при поступлении на работу в Организации, должна быть в виде соответствующих документов. При заключении трудового договора, в соответствии со ст. 65 Трудового кодекса РФ, лицо, поступающее на работу, предъявляет следующие документы:

3.1.1. Паспорт или иной документ, удостоверяющий личность.

3.1.2. Трудовую книжку, за исключением следующих случаев:

- Если трудовой договор заключается впервые.

- Если работник поступает на работу по совместительству.

3.1.3. Документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, форма АДИ-РЕГ, в том числе в форме электронного документа, либо страховое свидетельство государственного пенсионного страхования (СНИЛС), за исключением случая, когда претендент поступает на работу впервые и не имеет открытого индивидуального лицевого счета.

3.1.4. Документы воинского учета, если на работу поступает военнообязанный или лицо, подлежащее призыву на военную службу.

3.1.5. Документ об образовании и (или) о квалификации или наличии специальных знаний, если работник поступает на работу, которая требует соответствующих специальных знаний или специальной подготовки.

3.1.6. Свидетельство о присвоении ИНН (при его наличии у работника).

3.1.7. Справку о характере и условиях труда по основному месту работы - при приеме на работу по совместительству с вредными и (или) опасными условиями труда (приложение 3).

3.2. Работник Организации обязан предоставлять в отдел управления персоналом, далее ОУП исключительно только достоверные сведения о себе. ОУП проводит проверку достоверности предоставленных сведений.

3.3. При оформлении работника специалистами ОУП заполняется унифицированная форма Т-2 "Личная карточка работника", в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

- сведения о воинском учете;

- данные о приеме на работу;

- сведения об аттестации;

- сведения о повышенной квалификации;

- сведения о профессиональной переподготовке;

- сведения о наградах (поощрениях), почетных званиях;

- сведения об отпусках;

- сведения о социальных гарантиях;

- сведения о месте жительства и о контактных телефонах.

3.4. Создание носителей персональных данных работника.

Документы, содержащие персональные данные работника, создаются путём:

а) копирования оригиналов (документ об образовании, свидетельство ИНН, страховое пенсионное свидетельство);

б) внесения сведений в учётные формы (на бумажных и электронных носителях);

в) получения оригиналов необходимых документов (трудовая книжка, личный листок по учёту кадров, автобиография, медицинское заключение и т.д.).

3.5. В ОУП Организации создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

3.5.1. Документы, содержащие персональные данные работников:

- комплекты документов, сопровождающих процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

- комплекты материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;

- подлинники и копии приказов (распоряжений) по кадрам;

- личные дела и трудовые книжки;

- дела, содержащие основания к приказу по персоналу;

- дела, содержащие материалы аттестаций работников;

- дела, содержащие материалы внутренних служебных расследований;

- справочно-информационный банк данных по персоналу (картотеки, журналы);

- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Организации, руководителям структурных подразделений;

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

3.5.2. Документация по организации работы структурных подразделений:

- положения о структурных подразделениях;

- должностные инструкции работников;

- приказы, распоряжения, указания руководства Организации;

- документы по планированию, учету, анализу и отчетности в сфере кадровой работы.

3.6. При определении объема и содержания обрабатываемых персональных данных, работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.

3.7. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения федеральных и региональных законов или иных правовых актов, содействия работникам в трудоустройстве, обучении и профессиональном продвижении, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.8. Все персональные данные работника передаются непосредственно самим работником. Если персональные данные возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее (в письменной форме) и от него должно быть получено письменное согласие. Ответственное должностное лицо работодателя обязано сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа работника дать письменное согласие на их получение.

3.9. Работодатель не имеет права получать и обрабатывать персональные данные работника, содержащие информацию 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.

3.10. Письменное согласие сотрудника на обработку своих персональных данных должно включать в себя следующие сведения:

- 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 (приложение 4), (приложение 5).

3.11. Согласие на обработку персональных данных, разрешенных субъектом персональных данных 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 (приложение 28), (приложение 29), (приложение 30), (приложение 31).

3.12. Согласие сотрудника не требуется в следующих случаях:

- осуществление обработки персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- осуществление обработки персональных данных необходимо для защиты жизни, здоровья или иных жизненно важных интересов сотрудника, если получение его согласия невозможно;
- передаче соответствующим правоохранительными и надзорным органам, ФНС, Судам.

3.13. Работники и их представители должны быть ознакомлены под подпись с документами Организации, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области (приложение 6).

3.14. Во всех случаях отказ работника от своих прав на сохранение и защиту тайны не имеет правовой силы.

3.15. Персональные данные, включённые в состав личных дел, хранятся в отделе управления персоналом. Трудовые книжки, документы воинского учёта, хранятся в закрытом металлическом ящике.

3.16. Персональные данные, содержащие сведения о заработной плате работника хранятся в Отделе бухгалтерского, налогового учета и отчетности, заместителя генерального директора по экономике, заместителя генерального директора по финансам, отделе бюджетирования и корпоративного финансирования, отделе планирования и тарифного ценообразования и ОУП Организации.

3.17. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных и электронных автономных носителях, так и в электронном виде (посредством локальной компьютерной сети) (приложение 7).

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

3.19. В случае достижения цели обработки персональных данных, Оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

3.20. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.21. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

3.22. В случае отсутствия возможности уничтожения персональных данных в течение указанных выше сроков, Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

3.3. Порядок обработки персональных данных в информационной системе:

3.3.1. В информационной системе персональных данных должна соблюдаться парольная защита (приложение 8).

3.3.2. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.3.3. Все машинные носители информации, на которых записана информация, содержащая персональные данные субъектов, должны быть зарегистрированы в «Журнале учета машинных носителей информации», и иметь этикетку, на которой указывается учетный (регистрационный) номер (приложение 9).

3.3.4. При эксплуатации информационной системы, предназначенной для обработки персональных данных, пользователям запрещается:

- вносить изменения в состав, конструкцию, конфигурацию и размещение технических средств информационной системы;
- вносить изменения в состав программного обеспечения, структуру файловой системы;
- осуществлять попытки несанкционированного доступа к ресурсам информационной системы и к информации других пользователей;
- подключать информационную систему персональных данных к информационным сетям общего пользования без использования дополнительных средств защиты (сертифицированные межсетевые экраны и средства криптографической защиты данных);
- использовать неучтенные машинные накопители информации.

3.3.5. При проведении технического обслуживания и ремонта компонентов информационной системы персональных данных, запрещается передавать указанные компоненты третьим лицам в отсутствие пункта о соблюдении конфиденциальности в соглашении, заключенном с этими лицами.

3.3.6. Обязанности сотрудника по обработке ПДн в информационной системе персональных данных:

- при работе с АРМ использовать только установленное программное обеспечение, необходимое для выполнения должностных обязанностей сотрудника;
- при обработке персональных данных на АРМ исключить возможность ознакомления посторонних лиц с электронными документами;
- при отлучении с рабочего места закрывать все электронные документы, базы данных, содержащие персональные данные, блокировать АРМ;
- использовать только учтенные машинные носители информации;
- обеспечивать сохранность машинных носителей информации;
- при повреждении и выходе из строя внешних машинных носителей сдавать их для уничтожения;
- докладывать непосредственному руководителю о выявленных или допущенных нарушениях правил.

3.4. Порядок обработки персональных данных без использования средств автоматизации:

3.4.1. Персональные данные при их обработке без использования средств автоматизации, фиксируются на отдельных носителях персональных данных, в специальных разделах или на полях форм (бланков).

3.4.2. При фиксации персональных данных на носителях не допускается фиксация на одном носителе персональных данных, цели обработки которых заведомо не совместимы.

3.4.3. При использовании типовых форм документов, характер информации в которых, предполагает включение персональных данных, должно соблюдаться следующее условие: типовая форма или связанные с ней документы (административный регламент, инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных.

3.4.4. В отношении каждой категории персональных данных должны быть определены места хранения персональных данных (носителей персональных данных) и установлен перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

3.4.5. Обязанности сотрудника по обработке ПДн без использования средств автоматизации:

- выполнять требования, установленные Правилами обработки, хранения и уничтожения персональных данных и Политикой обработки и защиты персональных данных;
- обеспечить сохранность бумажных документов в процессе обработки и хранения;
- исключать просмотр документов, содержащих персональные данные, третьими лицами, в том числе сотрудниками Оператора, которым не предоставлен доступ к данным документам;
- хранить документы на рабочем месте исключительно с целью обработки ПДн. При достижении целей обработки сдавать документы в архив, либо осуществлять в установленном порядке уничтожение документов;
- в нерабочее время бумажные документы хранить в запираемых секциях рабочих столов или в шкафах, либо в запираемом помещении.

4. Передача и распространение персональных данных

4.1. Передача и распространение персональных данных работника возможна только с письменного согласия работника или в случаях, прямо предусмотренных законодательством (приложение 4).

4.2. При передаче и распространении персональных данных сотрудника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения возникновения угрозы жизни и здоровью сотрудника, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные сотрудника в коммерческих целях, без его письменного согласия. Обработка персональных данных сотрудников 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;

- предупреждать лиц, получивших доступ к персональным данным сотрудника, о том, что эти данные могут быть использованы лишь в целях, для которых они были им сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие доступ к персональным данным сотрудника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на порядок обмена персональными данными сотрудников в порядке, установленном федеральными законами;

- осуществлять передачу персональных данных сотрудников в пределах Предприятия в соответствии с настоящим Положением;

- разрешать доступ к персональным данным сотрудников, только специально уполномоченным лицам, при этом указанные лица должны иметь право доступа только к тем персональным данным, которые необходимы для выполнения конкретных действий;

- передавать персональные данные сотрудника 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 действий;

4.3. Не допускается передача конфиденциальной информации по телефону или факсу!

4.4. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом о персональных данных. В поручении должны быть определены: перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом о персональных данных.

4.5. Трансграничная передача персональных данных, обрабатываемых в Операторе, допускается в случаях, предусмотренных Федеральным Законодательством и международными договорами Российской Федерации.

4.6. Оператор передает персональные данные субъекта персональных данных третьим лицам на основании письменного запроса о предоставлении персональных данных (далее - запрос). Запрос должен содержать сведения о положениях федерального закона, устанавливающего право обратившегося на получение запрашиваемых персональных данных или о заключенном договоре (соглашении) об информационном взаимодействии с Оператором; о целях получения персональных данных; о составе персональных данных. В случае если запрос

направляется по информационно-телекоммуникационным сетям, он должен быть подписан усиленной квалифицированной электронной подписью (приложение 10).

5. Доступ к персональным данным работников

5.1. Внутренний доступ (доступ внутри Организации).

5.1.1. Право доступа к персональным данным работника имеют:

- Генеральный директор Организации;
- сам работник, носитель данных;
- другие работники Организации, при выполнении ими своих служебных обязанностей, в т.ч. устанавливается перечень должностей и список работников, имеющих доступ к персональным данным в информационной системе "1С" (приложение 11).

Субъект персональных данных, чьи персональные данные обрабатываются Оператором, имеет право на доступ к своим персональным данным в соответствии со статьей 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

5.1.2. Перечень должностей и список лиц, имеющих право доступа к персональным данным работников, определяется приказом по Предприятию.

5.1.3. Уполномоченные лица наделены правом доступа только к тем персональным данным работника, которые необходимы им для выполнения конкретных действий, в соответствии с должностными инструкциями указанных лиц. Все остальные работники предприятия имеют право на получение всей информации только о своих собственных персональных данных и последующую их обработку (приложение 12).

5.1.4. Работник, допущенный к обработке персональных данных, принимает на себя обязательства в случае прекращения с ним трудовых отношений, перевода на другую работу, освобождения от работ, связанных с обработкой персональных данных, прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей. Обязательство в письменной форме приобщается к личному делу работника (приложение 13).

5.2. Внешний доступ (другие организации и граждане).

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

- Федеральная налоговая служба;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военные комиссариаты;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

5.2.2. Контрольно-надзорные органы имеют право доступа к конфиденциальной информации только в рамках своей компетенции.

5.2.3. Организации, в которые работник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получать доступ к персональным данным работника только в случае его письменного согласия.

5.2.4. Другие организации.

Сообщение сведений о персональных данных работников другим организациям и гражданам разрешается при наличии письменного согласия работника и заявления подписанного руководителем организации либо гражданином, запросившим такие сведения.

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

5.2.5. Предоставление сведений о персональных данных работников без соответствующего их согласия возможно в следующих случаях:

- в целях предупреждения возникновения угрозы жизни и здоровью работника;
- при поступлении официальных запросов, в соответствии с положениями Федерального закона «Об оперативно-розыскной деятельности»;
- при поступлении официальных запросов из органов ФНС, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов.

5.2.6. Работник, о котором запрашиваются сведения, должен быть уведомлён о передаче его персональных данных третьим лицам, за исключением случаев, когда такое уведомление невозможно в силу форс-мажорных обстоятельств, а именно: стихийных бедствий, аварий, катастроф.

5.2.7. Запрещается передача персональных данных работника третьим лицам в коммерческих целях без его согласия.

6. Защита персональных данных

6.1. Под угрозой или опасностью подразумевается ситуация, которая может привести к утрате персональных данных работников, несанкционированный доступ для последующего использования на защищаемую информацию.

6.2. 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 (приложение 14), (приложение 15).

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

Для составления плана мероприятий по защите персональных данных определяется уровень защищенности персональных данных, при их обработке в информационной системе на Предприятии, с составлением соответствующего акта (приложение 16), (приложение 17), (приложение 18).

6.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем в порядке, установленном федеральным законом.

6.5. «Внутренняя защита».

6.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных.

Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами Организации.

6.5.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдение ряда мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации (приложение 19);
- определение мест хранения материальных носителей персональных данных, исключающих несанкционированный доступ к ним сторонних лиц (приложение 20);

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

Личные дела могут выдаваться на рабочие места только Генеральному директору, заместителю Генерального директора по безопасности и начальнику отдела корпоративной защиты и, в исключительных случаях, по письменному разрешению генерального директора, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

6.5.3. Защита персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается руководителю службы управления персоналом, и руководителю отдела информационных технологий.

6.6. «Внешняя защита».

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

6.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Организации, 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 отделе управления персоналом.

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

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

6.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

6.8. По возможности персональные данные обезличиваются.

6.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников (приложение 21).

7. Порядок уничтожения персональных данных

7.1. Обрабатываемые персональные данные подлежат уничтожению (удалению), либо обезличиванию по окончании срока хранения бумажных носителей персональных данных,

достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством.

7.2. Уничтожение (удаление) персональных данных осуществляется комиссией с составлением акта, по истечению сроков хранения и обработки персональных данных (приложение 22).

7.3. Уничтожение бумажных носителей персональных данных должно осуществляться путем сожжения, либо измельчения в уничтожителе бумаг (шредере).

7.4. При необходимости уничтожения (удаления) части персональных данных, уничтожается материальный носитель с предварительным копированием сведений, не подлежащих уничтожению (удалению), способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению (удалению) (приложение 23).

7.5. Уничтожение машинных носителей информации должно производиться следующими способами:

- оптические диски и дискеты – путем физического повреждения;
- флеш-накопители – путем ударно-механического повреждения основной платы, на которой располагается флеш-память;
- накопитель на жестком магнитном диске – путем измельчения магнитных дисков.

7.6. Для удаления персональных данных с машинных носителей информации могут использоваться программные методы гарантированного удаления информации, в которых используются алгоритмы гарантированного удаления данных.

7.7. Для удаления персональных данных из электронных баз данных применяются методы обезличивания персональных данных с целью невозможности определить принадлежность персональных данных конкретному субъекту в соответствии с Правилами работы с обезличенными данными (приложение 24).

8. Права и обязанности работника

8.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

8.2. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных.
- на свободный, безвозмездный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные (в соответствии с Трудовым кодексом РФ);
- на определение определять своих представителей для обеспечения защиты своих персональных данных;
- на обеспечение сохранности и защиты своей личной и семейной тайны.

8.3. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
- своевременно сообщать работодателю об изменении своих персональных данных.

8.4. Работники ставят работодателя в известность в течение трех рабочих дней об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

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

9.1. Персональная ответственность — одно из главных требований к Организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

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

9.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

9.4. Каждый работник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами. По каждому факту выявленных нарушений в сфере защиты персональных данных составляется комиссионный акт и, при необходимости, проводится служебная проверка (приложение 25).

9.6. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

9.7. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

9.8. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

10. Контроль и надзор за обработкой персональных данных

10.1. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи (Роскомнадзор). В вышеуказанный орган направляются сведения об операторе, осуществляющем обработку персональных данных (приложение 26).

10.2. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

10.3. Управление Роскомнадзора по Республике Башкортостан
450005, г. Уфа, ул. 50 лет Октября, 20/1,
Телефон для справок: (347) 222-20-98
Факс: (347) 222-20-97
E-mail: rsockanc02@rkn.gov.ru
Сайт: <http://02.rkn.gov.ru/>