У Т В Е Р Ж Д Е Н О

Приказом
Генерального директора
ОАО "ПК "Ахтуба"
№ 423 от 27.06. 2014 года

П О Л О Ж Е Н И Е
о защите персональных данных работников ОАО «ПК «Ахтуба»

Содержание:

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом РФ, Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ, Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119, Постановлением Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687, Приказом ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 №21.

1.2. В настоящем Положении не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также вопросы применения криптографических методов и способов защиты информации.

1.3. Настоящее положение принято в целях сохранения личной тайны и защиты персональных данных работников ОАО «ПК «Ахтуба» от несанкционированного доступа, неправомерного использования и утраты.

1.4. Положение определяет права и обязанности руководителей и работников, порядок защиты персональных данных, обрабатываемых в служебных целях.

1.5. Внутренний доступ (доступ внутри организации) к персональным данным имеют.

- генеральный директор организации;
- заместители генерального директора (к персональным данным работников возглавляемых ими подразделений);
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
- сам работник, носитель данных;
- сотрудники организации, в должностные обязанности которых входит работа с документами, содержащими персональные данные.

1.5.1. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом генерального директора организации.

1.5.2. Сотрудники, указанные в пункте 1.5. настоящего Положения, имеют право получать только те персональные данные работников, которые необходимы им для выполнения своих должностных обязанностей.

1.6. Внешний доступ к персональным данным (массовое потребление персональных данных вне организации) могут иметь:

1.6.1. Государственные и негосударственные функциональные структуры:

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

1.6.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции, в соответствии с законодательством РФ.

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

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

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

2. Основные понятия

Работник - физическое лицо, вступившее в трудовые отношения с работодателем.

Работодатель - Открытое акционерное общество «Производственный комплекс «Ахтуба».

Персональные данные работника - любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

В состав персональных данных работника входят:

- анкетные и биографические данные;

- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний, мобильный телефон;
- семейное положение;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- биометрические данные.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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;

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

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

Блокирование персональных данных - временное прекращение обработки

персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

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

Защита персональных данных - принятие ряда необходимых правовых, организационных и технических мер для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3. Защита персональных данных

3.1. «Внутренняя защита».

3.1.1. Основным источником угрозы 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.

3.1.2. Для обеспечении внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с персональными данными и базами данных ПДн;

- определение и регламентация состава работников, имеющих право доступа (входа) в помещения, предназначенные для работы с персональными данными;

- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

- разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с документами, содержащими персональные данные;

- запрет выдачи личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только генеральному директору, работникам отдела комплектования и подготовки кадров и, в исключительных случаях, по письменному разрешению генерального директора, - руководителю структурного подразделения. (например, при подготовке материалов для аттестации работника).

3.1.3. Защита персональных данных сотрудника при автоматизированной обработке осуществляется посредством:

- управления доступом (идентификация и проверка подлинности пользователя при входе в операционную систему и ИСПДн по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов);

- регистрации и учета (регистрация входа (выхода) пользователя в ИСПДн (из ИСПДн) и регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из ИСПДн и операционной системы или останова не проводится в моменты аппаратного отключения. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа. Ведётся учёт всех защищаемых носителей информации с помощью их маркировки и занесение учётных данных в журнал учёта с отметкой об их выдаче (приёме));

- обеспечения целостности (целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации. Наличие средств восстановления системы защиты ПДн, предусматривающих их периодическое обновление и контроль работоспособности);

- обеспечение сохранности носителей ИСПДн с помощью организации специализированной серверной, защищающей сервера от пожара, перегрева и несанкционированного доступа. Резервное копирование баз данных ИСПДн;

- для защиты от несанкционированного доступа используется сертифицированное программное средство антивирусный комплекс “Касперский”;

- с целью определения уровня доступа допущенных к обработке ПДн в ИСПДн сотрудников ведутся матрицы доступа, согласовываемые с руководителями подразделений, чьи сотрудники пользуются ИСПДн.

3.1.4. Защита ПДн сотрудников при неавтоматизированной обработке осуществляется в соответствии с требованиями Постановления Правительства РФ от 15.09.2008 №687, а также раздела 3 Положения об обработке ПДн работников ОАО «ПК «Ахтуба».

3.2. «Внешняя защита».

3.2.1. 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.

3.2.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности предприятия, 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 комплектования и подготовки кадров.

3.2.3. 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 магнитных пропусков;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях;
- разработать модели угроз информационных систем персональных данных;
- определить уровень защищённости ПДн при их обработке в ИСПДн.

3.2.4. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении информации, содержащей персональные данные, форма которого утверждена «Положением об обработке персональных данных работников ОАО «ПК «Ахтуба»».

3.2.5. По возможности персональные данные обезличиваются.

3.3. Физическая охрана технических средств и носителей информации, содержащих ПДн, предусматривающая контроль доступа в помещения, предназначенные для работы с ПДн, посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения.

3.3.1. Для физической защиты помещений от проникновения посторонних используются возможности отдела безопасности.

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

3.5. В целях обеспечения надлежащей защиты персональных данных назначается ответственное лицо — администратор ИСПДн.

3.6. При работе в ИСПДн в качестве мер технической защиты ПДн применяются все положения «Инструкции по защите информации на объектах ЭВТ», «Инструкции по антивирусной защите информации на объектах ЭВТ», а также меры, предусмотренные приказом ФСТЭК России от 18.02.2013 №21, в соответствии с определённым уровнем защищённости ПДн при их обработке в ИСПДн. В соответствии с этими документами осуществляется многоуровневая защита данных, начиная с отделов ПО, ПдиТР,ОЗИиПДн и заканчивая начальником отдела, эксплуатирующего ИСПДн и, непосредственно, сотрудником, работающим в ней.

4. Права и обязанности работника

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

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

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

- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

4.4. 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

4.5. Работники ставят работодателя в известность 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.

4.6. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

4.7. Администратор ИСПДн обязан обеспечивать строгое выполнение требований по защите персональных данных в соответствии с действующими нормативными и руководящими документами, инструкциями, положениями и распоряжениями.

5. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

5.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

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

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

5.4. На администратора ИСПДн возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты персональных данных.

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

5.6. 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.

5.6.1. 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.

5.6.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

5.6.3. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

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

Начальник отдела ПО И.В. Николенко

Начальник ОКиПК В.И. Синегин

Согласовано:

Первый ЗГД В.И. Кубраков
"26" 05 2014г.

Начальник ОПдИТР,ОЗИиПДн В.И. Митрофанов
"26" мая 2014 г.