

* сведения о заработной плате сотрудника;
* сведения о социальных льготах;
* специальность,
* занимаемая должность;
* адрес места жительства;
* домашний телефон;
* 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, пенсионного фонда.

# Обработка персональных данных

3.1. Под обработкой персональных данных работника, учащегося понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника, учащегося.

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника, учащегося обязаны соблюдать следующие общие требования:

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

3.2.2. При определении объема и содержания обрабатываемых персональных данных работника, учащегося работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

3.2.3. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.

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

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

3.2.6. Работодатель не имеет право получать и обрабатывать персональные данные работника, учащегося о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. К обработке, передаче и хранению персональных данных работника, учащегося могут иметь доступ сотрудники:

* бухгалтерии;
* администрация учреждения, классные руководители по своему классу, учителя – предметники к данным по своему предмету;
* системный администратор учреждения.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.5. Передача персональных данных работника, учащегося возможна только с согласия работника, учащегося или в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных работника, учащегося работодатель должен соблюдать следующие требования:

* не сообщать персональные данные работника, учащегося третьей стороне без письменного согласия работника, учащегося, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, учащегося, а также в случаях, установленных федеральным законом;
* не сообщать персональные данные работника, учащегося в коммерческих целях без его письменного согласия;
* предупредить лиц, получающих персональные данные работника, учащегося, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, учащегося, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;
* разрешать доступ к персональным данным работников, учащихся только специально уполномоченным лицам, определенным приказом по учреждению, управлению образования при этом указанные лица должны иметь право получать только те персональные данные работника, учащегося, которые необходимы для выполнения конкретных функций;
* не запрашивать информацию о состоянии здоровья работника, учащегося, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником, учащимся трудовой функции и обучения;
* передавать персональные данные работника, учащихся представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, учащихся, которые необходимы для выполнения указанными представителями их функций.
  + 1. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
    2. При передаче персональных данных работника, учащихся потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, учащихся, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, учащихся или в случаях, установленных федеральным законом.
  1. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника, учащихся распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
  2. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.
  3. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.
  4. При принятии решений, затрагивающих интересы работника, учащихся, работодатель не имеет права основываться на персональных данных работника, учащихся, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, учащихся, его добросовестный и эффективный труд.

# Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).

4.1.1. Право доступа к персональным данным сотрудника, учащихся имеют:

* директор учреждения;
* руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников, учащихся своего подразделения, класса, предмета);
* при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника, учащегося может иметь руководитель нового подразделения;
* сам работник, носитель данных;
* другие сотрудники организации при выполнении ими своих служебных обязанностей.

4.2. Внешний доступ.

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

* налоговые инспекции;
* правоохранительные органы;
* органы статистики;
* военкоматы;
* пенсионные фонды;
* муниципальный орган управления образования,
* муниципальное учреждение «Центр развития образования».
  + 1. Надзорно – контрольные органы имеют доступ к информации только в сфере своей компетенции.
    2. Организации, в которые сотрудник, учащийся может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника, учащегося только в случае его письменного разрешения.
    3. Другие организации.

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

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

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

# Защита персональных данных

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

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

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

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

5.5. Внутренняя защита.

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

5.5.2. Для обеспечения внутренней защиты персональных данных работников, учащихся 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 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 учреждения;
* воспитательная и разъяснительная работа с сотрудниками учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
* не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору, работникам отдела персонала и в исключительных случаях, по письменному разрешению директора, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

5.5.3. Защита персональных данных сотрудника, учащегося на электронных носителях.

Все папки, содержащие персональные данные сотрудников, учащихся класса должны быть защищены паролем, который сообщается директору службы управления персоналом и руководителю службы информационных технологий

5.6. Внешняя защита.

* + 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.
    2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, 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 персонала.
    3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:
* порядок приема, учета и контроля деятельности посетителей;
* пропускной режим организации;
* учет и порядок выдачи удостоверений;
* технические средства охраны, сигнализации;
* порядок охраны территории, зданий, помещений, транспортных средств;
* требования к защите информации при интервьюировании и собеседованиях.
  1. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников, учащихся.
  2. По возможности персональные данные обезличиваются.
  3. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

# Права и обязанности работника

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

6.2. 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.

6.3. 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.

6.4. Работник, учащийся 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
  1. Работники, учащиеся 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.
  2. 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.

# Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

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

7.2. 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.

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

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

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

7.5.1. 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.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, учащегося, 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.

7.5.3. 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.

7.5.4. 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.

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