Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Агабекян Раиса Левоновна
Должность: ректор
Дата подписания: 24.11.2021 11:59:52
Уникальный программный ключ:
4237c7ccb9b9e111bbaf1f4fcda9201d015c4dbaa123ff774747307b9b9fbcbe

НАН ЧОУ ВО «Академия маркетинга и социально-информационных технологий – ИМСИТ» (г.Краснодар)
Зиповская ул., д.5, Краснодар г., 350010

Тел/факс (861)252-25-81, 278-22-83

УТВЕРЖДАЮ
президент _____ В.А.Косяков
«____» _____20_17_г.

ПОЛОЖЕНИЕ
о персональных данных работников

1. Общие положения.

1.1. Целью положения об обработке персональных данных работников (далее – Положение) является защита персональных данных работников негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования «Академия маркетинга и социально-информационных технологий – ИМСИТ» (г.Краснодар) (далее – Общество) от несанкционированного доступа, неправомерного их использования или утраты, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Положение разработано в соответствии со статьями 85-90 Трудового Кодекса Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Правилами внутреннего трудового распорядка Организации.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Положение вступает в силу с момента утверждения его Генеральным директором Общества и действует бессрочно, до замены его новым положением.

1.3.2. Все изменения в Положения вносятся соответствующим приказом.

1.4. Все работники Общества должны быть ознакомлены с настоящим Положением под подпись.

1.5. Режим конфиденциальности персональных данных снимается в случае их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Общества, если иное не определено законом.

2. Основные понятия.

2.1. Для целей настоящего Положения используются следующие основные понятия

- 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;
- обработка персональных данных – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников Общества;
- 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 на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным работников каким-либо иным способом;
- использование персональных данных – действия (операции) с персональными данными, совершаемые должностным лицом Общества 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 работников, в том числе их передачи;
- уничтожение 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;
- общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
- 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.

3. Состав персональных данных работников.

3.1. В состав персональных данных работников Общества 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;
- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- 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 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.

3.2. Данные документы являются конфиденциальными, при этом, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

4. Обработка персональных данных.

4.1. В целях обеспечения прав и свобод работника Общество и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

4.1.1. 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.

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

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

4.1.4. 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. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

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

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

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

- Бухгалтерии;
- Отдела персонала;
- Отдела информационных технологий.

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

4.3.1. 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.

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

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

- 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;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, 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, 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 только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми

персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.4.2. 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.

4.4.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

4.5. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

4.6. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

4.7. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4.8. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

5. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в Организации при его приеме, переводе и увольнении.

5.1. Информация, представляемая работником при поступлении на работу в Организацию, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт гражданина Российской Федерации;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН.

5.2. При оформлении работника в Организацию работником отдела кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
- сведения о воинском учете;
- данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- сведения о месте жительства и контактных телефонах.

5.3. В отделе персонала Общества создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

5.3.1. Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; 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, налоговые инспекции, вышестоящие органы управления и другие учреждения).,

5.3.2. 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 части работы с персоналом Организации.

6. Доступ к персональным данным.

6.1. Внутренний доступ (доступ внутри Общества).

6.1.1. Право доступа к персональным данным сотрудника имеют:

- Генеральный директор Общества;
- Сотрудники отдела персонала Общества;
- руководители 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.
- другие сотрудники организации при выполнении ими своих служебных обязанностей.

6.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом Генерального директора Общества.

6.2. Внешний доступ.

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

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

6.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

6.2.3. 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.

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

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

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

7. Защита персональных данных

7.1. 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.

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

7.3. Внутренняя защита.

7.3.1. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к персональным данным сотрудников.
- 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 подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения 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 генеральному директору, работникам отдела персонала и в исключительных случаях, по письменному разрешению генерального директора, - руководителю структурного подразделения. (например, при подготовке материалов для аттестации работника).

7.3.2. Защита персональных данных сотрудников на электронных носителях.
Все папки, содержащие персональные данные сотрудника, должны иметь ограниченный доступ (только для сотрудников отдела персонала и директора по информационным технологиям).

7.4. Внешняя защита.

7.4.1. 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 (электронный ключ, сигнализации);
- порядок охраны территории, зданий, помещений, транспортных средств;

7.5. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны не разглашать персональные данные работников.

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

8. Права и обязанности работника.

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

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

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

8.3. Работник обязан передавать Обществу комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым Кодексом РФ, а также своевременно сообщать об изменениях своих персональных данных.

8.4. Работники ставят Общество 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.

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

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

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

9.3. 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.

Приложение №1: заявление о согласии на обработку персональных данных
Приложение №2: Ответственность работника, имеющего доступ к персональным данным других работников

Приложение № 1 к положению
о персональных данных работника

Руководителю Академии ИМСИТ
_____

ЗАЯВЛЕНИЕ
о согласии на обработку персональных данных

Я, _____, в соответствии со статьей 9 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" даю согласие НАН ЧОУ ВПО "Академия маркетинга и социально-информационных технологий – ИМСИТ г.Краснодар»", находящейся по адресу: 350010, г.Краснодар, ул. Зиповская, 5, а также её структурным подразделениям на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, совершение действий, предусмотренных пунктом 3 части 1 статьи 3 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", в целях обеспечения соблюдения законов и иных нормативных правовых актов, обеспечения безопасности, дальнейшего повышения квалификации и продвижении по службе, содействия в трудоустройстве, заключения трудового договора, оформления работника в кадровой службе Академии, осуществления им трудовой деятельности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, а именно:
использовать все нижеперечисленные данные для формирования кадровых документов и для выполнения ООО «Академия» всех требований трудового законодательства, использовать мои персональные данные в информационной системе для осуществления расчетов работодателя со мной как работником и для составления и передачи установленных форм отчетов.

Даю согласие на обработку следующих моих персональных данных:

1. Фамилия, имя, отчество;
2. Пол;
3. Личная фотография;
4. Дату рождения; место рождения, гражданство, возраст;
5. Серия, номер паспорта гражданина РФ, кем и когда выдан, страховой номер индивидуального лицевого счета (СНИЛС), ИНН;
6. Семейное положение (близкие родственники, дети, их ФИО, даты рождения);
7. Отношение к воинской обязанности;
8. Адрес регистрации по месту жительства;
9. Адрес фактического проживания, контактный телефон;
10. Образование, специальность, профессия, квалификация, профессиональная подготовка, переподготовка и сведения о повышении квалификации и аттестации, реквизиты документов об образовании, проф. подготовке и переподготовке, о повышении квалификации и аттестации;
11. Предыдущее(ие) место(а) работы, сведения о трудовом, специальном и общем стаже;
12. Сведения об отпусках;
13. Сведения о социальных гарантиях;
14. Размер заработной платы;
15. Должность, структурное подразделение;
16. Состояние здоровья, результаты мед. обследования на предмет годности к осуществлению трудовых обязанностей;
17. Иные сведения, с которыми работник считает нужным ознакомить работодателя.

Об ответственности за достоверность представленных сведений предупрежден (предупреждена).

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме, и в течение срока, установленного архивным законодательством.

РАБОТНИК

Фамилия, Имя, Отчество_____

Паспорт: серия _____№ _____
выдан _____
(кем и когда)
«____» _____ _____ г.
Дата рождения _____
Телефон _____
Место и дата регистрации:
_____
_____ (_____)
(расшифровка подписи)
«____»_____ 20____ г.

Приложение № 2 к положению
о персональных данных работника

Ответственность работника, имеющего доступ к персональным данным других работников

Исходя из смысла ст. 90 ТК РФ лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами. И ФЗ от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) "О персональных данных" ч.1 ст. 24. Ответственность за нарушение требований настоящего Федерального закона лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность; ч. 2 ст. 24 моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Административная ответственность: на основании Кодекса РФ об административных правонарушениях ст. 5.39. неправомерный отказ в предоставлении гражданину, в том числе адвокату в связи с поступившим от него адвокатским запросом, и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации -влечет наложение административного штрафа на должностных лиц в размере от 5000 до 10000 рублей;

ст. 13.11 КоАП «Нарушение законодательства Российской Федерации в области персональных данных» защищает любые сведения, нераспространение которых гарантировано законодательством, состоит из 7 частей и достаточно подробно описывает все возможные виды наказания:

- Часть первая. Рассматривает запрос и обработку персональных данных в тех случаях, когда она не требуется по закону. Грозит предупреждением, наложением штрафа от 1000 до 3000 рублей для граждан, от 5000 до 10000 для должностных лиц и от 30000 до 50000 для юридических лиц;
- Часть вторая. Рассматривает сбор и обработку персональных данных без письменного согласия их владельца в тех случаях, когда оно необходимо. Наказанием послужит штраф от 3000 до 5000 рублей для граждан, от 10000 до 20000 для должностных лиц и от 15000 до 70000 для организаций;
- Часть третья. Невыполнение оператором, выполняющим обработку персональных данных, правил и норм по их опубликованию или обеспечению доступа. Наказывается штрафом от 700 до 1700 рублей для физических лиц, от 3000 до 6000 для должностных и от 15000 до 30000 для организаций;
- Часть четвертая. Рассматривает нарушения в работе оператора, касающиеся его обязанностей по предоставлению персональных данных или информации об их обработке субъекту. Наказывается штрафом от 1000 до 2000 рублей для физических лиц, от 4000 до 6000 для должностных лиц и от 20000 до 40000 для юридических лиц;
- Часть пятая. Рассматривает любое нарушение сроков в обработке, хранении, передаче, уничтожении персональных данных. Наказанием за такой проступок послужат штрафы от 1000 до 2000 рублей для физических лиц, от 4000 до 6000 для должностных лиц и от 25000 до 40000 для юридических лиц;
- Часть шестая. Рассматривает нарушения, которые привели к распространению персональных данных случайно или умышленно, а так же ошибки при обеспечении безопасности персональных сведений и закрытой информации. Наказываются подобные деяния штрафом до 2000 рублей для физических лиц, до 10000 для должностных лиц и до 50000 рублей – для организаций.
- Часть седьмая. Рассматривает нарушения законов о персональных данных, которые были замечены за сотрудниками муниципальных или государственных органов власти. Наказываются подобные нарушения штрафами до 6000 рублей

ст. 13.14. КоАП Разглашение информации с ограниченным доступом разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, влечет наложение административного штрафа на граждан в размере от 500 до 1000 рублей; на должностных лиц - от 4000 до 5000 рублей.

Уголовная ответственность: уголовная ответственность наступает в том случае, если были разглашены личные данные человека, которые создали угрозу его частной жизни, затронули его безопасность или предоставили для общего доступа сведения, которые не подлежат огласке и охраняются законами РФ. За подобные деяния отвечает статья 137 Уголовного Кодекса, именуемая «нарушение неприкосновенности частной жизни», которая состоит из трех частей:

ч. 1 ст. 137 УК РФ**:**

- Штрафом до 200 000 рублей;
- Штрафом в размере дохода виновного за полтора года;
- Обязательными работами до 360 часов;
- Исправительными работами сроком до года;
- Принудительными работами на 2 года;
- Четырьмя месяцами ареста;
- Двумя годами лишения свободы.

ч. 2 ст. 137 УК РФ**:**

- 100 000 – 300 000 рублей штрафа;
- 4 года принудительных работ;
- 6 месяцев ареста;
- До 4 лет лишения свободы;
- Лишение права заниматься определенным видом деятельности, дающим полномочия, на срок до 5 лет.

ч. 3 ст. 137 УК РФ:

- Штраф от 150 000 до 300 000 рублей;
- Штраф в размере заработка виновного за период до 3х лет;
- До 5 лет принудительных работ;
- До 6 месяцев ареста;
- До 5 лет лишения свободы;
- Запрет на ведение деятельности, дающей определенные полномочия, на срок до 6 лет.

ч. 1 ст. 272. УК РФ Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, - наказывается штрафом в размере до 2000 рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

ч. 2 ст. 272. УК РФ то же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, - наказывается штрафом в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

ч. 3 ст. 272. УК РФ деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказываются штрафом в размере до 500 000 рублей

или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

ч. 4 ст. 272. УК РФ Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Дисциплинарная ответственность: персональные данные относятся к сведениям, которые охраняются федеральным законом. Неправомерное разглашение персональных данных лицом, в чьи обязанности входит соблюдение правил хранения, обработки и использования такой информации, также является основанием для привлечения этого лица к дисциплинарной ответственности (ст. 90 ТКРФ). Согласно пп. «в» 6 ч. 1 ст. 81 ТК РФ трудовой договор с работником может быть расторгнут по причине разглашения охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе по причине разглашения персональных данных другого работника. Поскольку такое увольнение относится к увольнению за нарушение трудовой дисциплины, то работника, разгласившего персональные данные, необходимо уволить с соблюдением процедуры, предусмотренной ст. 193 ТК РФ.

Материальная ответственность: ст. 90 ТК РФ предусмотрена материальная ответственность за виновное нарушение норм, регулирующих получение, обработку и защиту персональных данных работников. Так, в результате незаконно распространения информации о персональных данных работника последнему может быть причинен моральный вред, подлежащий возмещению работодателем. В соответствии со ст. 238 ТК РФ работник обязан возместить работодателю причиненный последнему прямой действительный ущерб. Согласно ч. 2 указанной статьи по прямым действительным ущербом также понимается необходимость возмещения ущерба третьим лицам. Следовательно, если вред работнику был допущен по вине лица, которое было ответственно за неразглашение персональных данных, то работодатель может привлечь последнее к материальной ответственности за ущерб, который был нанесен работнику такими действиями. В соответствии с п. ст. 243 ТК РФ материальная ответственность в полном размере причиненного ущерба возлагается на работника в случае разглашения сведений, составляющих охраняемую законом тайну.

Гражданско-правовая ответственность: в соответствии со ст. 151 ГК РФ, если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в иных случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда. Согласно ч. 2 ст. 1099 ГК РФ моральный вред, причиненный действиями (бездействиями), нарушающими имущественные права гражданина, подлежит компенсации в случаях, предусмотренных законом. На основании ст. 152 ГК РФ гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности.