

Утверждено приказом
генерального директора
Ассоциации СРО «Центризыскания»
от 07.05.2019 № 08

Положение
о защите персональных данных работников
членов Ассоциации СРО «Центризыскания»

2019 год

1. Общие положения

1.1. Положение о защите персональных данных работников членов Ассоциации СРО «Центризыскания» (далее Положение) разработано в соответствии с Конституцией Российской Федерации, Трудовым, Гражданским, Уголовным кодексами Российской Федерации, Кодексом об административных правонарушениях Российской Федерации, Градостроительным Кодексом Российской Федерации, Федеральными законами: «Об информации, информационных технологиях и защите информации» и «О персональных данных», Уставом Ассоциации СРО «Центризыскания».

1.2. Настоящее Положение определяет комплекс мер, направленных на обеспечение защиты персональных данных работников членов Ассоциации СРО «Центризыскания» (далее – Ассоциации) от несанкционированного доступа к ним, неправомерного их использования или утраты.

1.3. Настоящее Положение утверждается генеральным директором Ассоциации и является обязательным для исполнения всеми работниками Ассоциации.

1.4. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

2. Понятие и состав персональных данных

2.1. Персональные данные о работниках члена Ассоциации (далее – работниках) - информация, необходимая Ассоциации для обеспечения соблюдения членом Ассоциации требований, установленных в Ассоциации в соответствии с действующим законодательством.

2.2. В состав персональных данных работника входят:

- анкетные и биографические данные;
- сведения о полученном образовании;
- сведения о трудовом и общем стаже;
- паспортные данные;
- сведения о заработной плате;
- содержание трудового договора;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний, мобильный и иные телефоны работника;
- иные сведения.

2.3. Основными документами, в которых содержатся персональные данные работников, являются:

- трудовой договор;
- отчеты, направляемые в органы пенсионного фонда, и их копии;
- трудовые книжки работников;
- документы работников о полученном образовании;
- документы о повышении квалификации и переподготовке работников, их аттестации, служебного расследования, и др.;
- разрешения на работу (для иностранных граждан);
- иные документы.

2.4. Документы с персональными данными являются конфиденциальными.

3. Обработка персональных данных

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

3.2. В целях обеспечения прав и свобод человека и гражданина, Ассоциация и ее представители при обработке персональных данных работников обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, контроля за соблюдением обязательных требований членом Ассоциации;

3.2.2. Персональные данные работника представляются его работодателем и (или) самим работником. Если персональные данные работника представляются работодателем, то работник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие, за исключением случаев, предусмотренных федеральным законом. Ассоциация и (или) член Ассоциации должны сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение, за исключением случаев, предусмотренных федеральным законом;

3.3. К обработке персональных данных работника члена Ассоциации имеют доступ лица, установленные п.4 настоящего Положения.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение. Персональные данные не могут быть использованы Ассоциацией 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.

3.5. Передача (распространение, передача, доступ) персональных данных работника возможна только с согласия работника и его волеизъявлением, или в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных работника Ассоциация обязана 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 конфиденциальности;

- 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.

3.5.2. 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.

3.6. Действие настоящего положения при сборе, обработке и хранении персональных данных работника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону, факсу или электронной почтой (в отсутствие электронного ключа).

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

3.9. Юридическое лицо, являющееся членом Ассоциации, обязано принять следующие меры в целях правомерной передачи данных о своих работниках Ассоциации:

- получить от каждого работника, данные которого планируются к передаче Ассоциации, письменное согласие работника или его законного представителя, действующего на основании нотариально заверенной доверенности, на обработку Ассоциацией его персональных данных;

- принять все необходимые меры по защите персональных данных своих работников при передаче таких данных Ассоциации.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри Ассоциации). Право доступа к персональным данным работников членов Ассоциации имеют:

- члены Контрольного комитета Ассоциации;
- члены Дисциплинарной комиссии Ассоциации;
- работники Исполнительного органа Ассоциации по письменному разрешению Председателя контрольного комитета Ассоциации;
- сам работник, носитель данных.

4.2. Внешний доступ.

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

- органы налоговой инспекции;
- правоохранительные органы;
- национальное объединение саморегулируемых организаций, членом которого является Ассоциация.

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

5. Защита персональных данных от угрозы утраты и несанкционированного доступа

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, доступ к информации в нарушение должностных полномочий сотрудников, доступ закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

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 динамический 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 Ассоциации.

5.4. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается Ассоциацией за счет собственных средств и в порядке, установленном федеральным законом.

5.5. «Внутренняя защита».

5.5.1. Для обеспечения внутренней защиты персональных данных работников Ассоциация обязуется соблюдать следующие меры:

- ограничить и регламентировать состав работников, функциональные обязанности которых требуют конфиденциальных знаний;

- избирательно и обоснованно распределить доступ к документам и информации между членами Контрольного комитета Ассоциации и работниками исполнительного органа, и членами иных органов Ассоциации;

- контролировать знание работниками требований нормативно – методических документов по защите информации и сохранению тайны;

- организовать порядок уничтожения информации.

5.5.2. Защита персональных данных сотрудников на электронных носителях. Информационные базы и иные вычислительные комплексы, используемые Ассоциацией и содержащие персональные данные сотрудников, должны быть защищены паролем.

5.6. «Внешняя защита».

5.6.1. Для обеспечения внешней защиты конфиденциальной информации применяются меры, препятствующие несанкционированному доступу к информации. Результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним понимается лицо, не имеющее непосредственного отношения к деятельности Ассоциации, 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 Ассоциации.

5.6.3. Для обеспечения внешней защиты персональных данных сотрудников Ассоциация устанавливает:

- ограничение на доступ в помещение архива Контрольного комитета;

- систему видеонаблюдения в помещении архива Контрольного комитета;

- запорные механизмы, исключающие свободный доступ к делам членов Ассоциации.

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

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

6.1. Работники Ассоциации несут персональную ответственность за разглашение конфиденциальной информации, связанной с персональными данными.

6.2. Председатель Контрольного комитета, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

6.3. Каждый работник Ассоциации, получающий конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность хранящейся на нем информации.

6.4. 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.

8. Заключительные положения

8.1. Неотъемлемой частью настоящего Положения являются:

Приложение 1 - форма обязательства по исполнению настоящего Положения;

8.2. Настоящее Положение вступает в силу с момента утверждения генеральным директором Ассоциации.

ПРИЛОЖЕНИЕ №1
к Положению о защите персональных
данных работников членов Ассоциации СРО «Центризыскания»

ОБЯЗАТЕЛЬСТВО
сотрудника Ассоциации СРО «Центризыскания»

Я, _____
(ФИО)

(наименование должности, подразделения или выборной должности, место работы)

обязуюсь не разглашать персональные данные работников членов Ассоциации, ставшие мне известными в связи с исполнением своих должностных обязанностей или в процессе деятельности Ассоциации. Об ответственности за разглашение персональных данных работников предупрежден(а).

Должность: _____

_____ (подпись)

" ____ " _____ 20__ г.