



**Автономная некоммерческая организация
Общеобразовательная организация
«ШКОЛА «ПРЕЗИДЕНТ»**

Российская Федерация, 143082, Московская область, Одинцовский район,
д. Жуковка, Ильинский подъезд, дом 2, стр. 1., тел.: +7 (495) 225-81-00
web: <http://school-president.ru>, e-mail: info@school-president.ru
ОКПО 87645441, ОГРН 1087799029834, ИНН/КПП 7713386783/503201001

«УТВЕРЖДАЮ»

Директор



/Л.А. Машина/

приказ № 39 от 21.02.2018 г.

ПОЛОЖЕНИЕ

о защите персональных данных работников

1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников Автономной некоммерческой организации Общеобразовательной организации «ШКОЛА «ПРЕЗИДЕНТ» (далее – АНО «ШКОЛА «ПРЕЗИДЕНТ» или школа) от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, а также Федерального закона "Об информации, информатизации и защите информации".

1.3. 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.

1.4. Настоящее Положение утверждается и вводится в действие приказом директора школы и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

2. Понятие и состав персональных данных

2.1. Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. В состав персональных данных работника входят:

- 2.2.1. анкетные и биографические данные;
- 2.2.2. образование;
- 2.2.3. сведения о трудовом и общем стаже;
- 2.2.4. сведения о составе семьи;
- 2.2.5. паспортные данные;
- 2.2.6. сведения о воинском учете;
- 2.2.7. сведения о заработной плате сотрудника;
- 2.2.8. сведения о социальных льготах;
- 2.2.9. специальность;
- 2.2.10. занимаемая должность;

- 2.2.11. наличие судимостей;
 - 2.2.12. адрес места жительства;
 - 2.2.13. домашний телефон;
 - 2.2.14. место работы или учебы членов семьи и родственников;
 - 2.2.15. характер взаимоотношений в семье;
 - 2.2.16. содержание трудового договора;
 - 2.2.17. состав декларируемых сведений о наличии материальных ценностей;
 - 2.2.18. содержание декларации, подаваемой в налоговую инспекцию;
 - 2.2.19. подлинники и копии приказов по личному составу;
 - 2.2.20. личные дела и трудовые книжки сотрудников;
 - 2.2.21. основания к приказам по личному составу;
 - 2.2.22. дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
 - 2.2.23. копии отчетов, направляемые в органы статистики.
- 2.3. Документы, указанные в п. 2.2. настоящего Положения, являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3. Обработка персональных данных

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

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника 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, содействия работникам 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 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 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 также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.2.5. 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.

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

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

3.3.1. сотрудники финансовой службы;

3.3.2. сотрудники кадровой службы;

3.3.3. сотрудники IT-службы;

3.3.4. иные сотрудники школы, в чьи функции входит работ с источниками, содержащими персональные данные.

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

3.5. 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.

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

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

3.7.1. 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;

3.7.2. не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

3.7.3. 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;

3.7.4. разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по школе, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

3.7.5. не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

3.7.6. 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.

3.8. 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.

3.9. При передаче персональных данных работника 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.

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

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

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

3.13. 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.

4. Доступ к персональным данным

Внутренний доступ (доступ внутри организации).

4.1. Право доступа к персональным данным сотрудника имеют:

4.1.1. директор школы;

4.1.2. сам работник, носитель данных;

4.1.3. другие сотрудники школы в рамках выполнения ими своих должностных обязанностей.

4.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом директора школы.

Внешний доступ.

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

4.3.1. налоговые инспекции;

- 4.3.2. правоохранительные органы;
- 4.3.3. органы статистики;
- 4.3.4. страховые агентства;
- 4.3.5. военкоматы;
- 4.3.6. органы социального страхования;
- 4.3.7. пенсионные фонды;
- 4.3.8. подразделения муниципальных органов управления;

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

4.5. 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.

Другие организации.

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

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

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

5. 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 и субъективные факторы

и обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

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

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

Внутренняя защита

5.5. Регламентация доступа работников к конфиденциальным сведениям, документам и базам данных является основным направлением организационной защиты информации и предназначена для разграничения полномочий между работниками.

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

5.6.1. регламентация состава работников, функциональные обязанности которых требуют работы с источниками, содержащими конфиденциальные данные;

5.6.2. избирательное и обоснованное распределение документов и информации между работниками;

5.6.3. рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

5.6.4. знание работником требований нормативно-методических документов по защите информации и сохранении тайны;

5.6.5. наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

5.6.6. организация порядка уничтожения информации;

5.6.7. своевременное выявление нарушений требований системы данных;

5.6.8. воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты сведений при работе с конфиденциальными документами;

5.6.9. не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору, работникам кадровой службы и в исключительных случаях, по письменному разрешению директора, руководителю структурного подразделения.

Защита персональных данных сотрудника на электронных носителях.

5.7. Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем.

Внешняя защита

5.8. Для защиты конфиденциальной информации создаются целенаправленные и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ к данным.

5.9. 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.

5.10. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности школы.

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

5.11.1. требования к защите информации;

5.11.2. порядок учета и контроля деятельности посетителей в школе, пропускной режим;

5.11.3. порядок охраны территории, зданий, помещений, транспортных средств.

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

5.13. По возможности персональные данные обезличиваются.

5.14. Кроме мер защиты персональных данных, установленных законодательством, в школе могут вырабатываться дополнительные меры защиты персональных данных работников.

6. Права и обязанности работника

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

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

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

6.3. Работник обязан:

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

6.4. Работники ставят работодателя в известность об изменении персональных данных в порядке, установленном законодательством РФ.

7. 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. Работники школы несут ответственность за нарушение режима защиты, обработки и порядка использования персональных данных в соответствии с законодательством Российской Федерации.

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

7.4. Каждый сотрудник школы, получающий доступ к источнику, содержащему персональные данные, несет персональную ответственность за сохранность носителя и сохранение конфиденциальности информации.

7.5. 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.

7.6. 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.

7.7. Должностные лица, в обязанность которых входит работа с персональными данными сотрудника, обязаны обеспечить каждому работнику возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.