

Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение «Колледж «Звёздный»

ПРИНЯТ
Педагогическим советом
СПб ГБ ПОУ
«Колледж «Звёздный»
Протокол от «30» 08 2018 года № 08

ПРИНЯТ
С учетом мнения
Совета обучающихся
СПб ГБ ПОУ «Колледж «Звёздный»
Протокол от «19» 11 2019 года № 09

УТВЕРЖДЕН
Приказом СПб ГБ ПОУ
«Колледж «Звёздный»

от «31» 08 2018 года № 129-1

ЛОКАЛЬНЫЙ АКТ № 25

Положение об обработке и защите персональных данных работников
Санкт-Петербургского государственного бюджетного профессионального
образовательного учреждения «Колледж «Звёздный»

Санкт-Петербург
2018

1. Общие положения

1.1. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Колледж «Звёздный» (далее – образовательное учреждение). Под работниками подразумеваются лица, заключившие трудовой договор с предприятием.

1.2. Цель настоящего Положения - защита персональных данных работников образовательного учреждения от несанкционированного доступа и разглашения. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

1.3. Настоящее Положение разработано на основании:

- 1.3.1. Конституции Российской Федерации,
- 1.3.2. Трудового кодекса Российской Федерации,

1.3.3. других действующих нормативных правовых актах Российской Федерации.

2. Понятие и состав персональных данных

2.1. Персональными данными является любая информация, прямо или косвенно относящаяся к субъекту персональных данных - определенному или определяемому физическому лицу.

2.2. Состав персональных данных работника:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- размер заработной платы;
- наличие судимостей;
- адрес места жительства и домашний телефон;
- 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;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным работника;
- рекомендации, характеристики;
- прочие сведения, которые могут идентифицировать человека.

Из указанного списка работодатель вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора.

2.3. Данные документы являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 50 лет срока хранения, если иное не определено законом.

3. Обязанности работодателя

3.1. Работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.1.1. обработка персональных данных работника осуществляется 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.

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

3.1.3. Все 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 также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.1.4. 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, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

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

3.1.6. 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.

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

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

4. Обязанности работника

Работник обязан:

4.1. Передавать работодателю или его представителю комплект достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом Российской Федерации.

4.2. Своевременно сообщать работодателю об изменении своих персональных данных.

5. Права работника

Работник имеет право:

5.1. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством Российской Федерации.

5.2. Требовать исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных трудовым законодательством. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные

оценочного характера сотрудник имеет право дополнить заявлением, выражаящим его собственную точку зрения.

5.3. Требовать извещения работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.4. Обжаловать в суде любые неправомерные действия или бездействие работодателя при обработке и защите его персональных данных.

5.5. Определять своих представителей для защиты своих персональных данных.

6. Сбор, обработка и хранение персональных данных

6.1. Обработка персональных данных работника - 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 работника.

6.2. Все 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.

6.3. 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.

6.4. Работник представляет работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами. Представление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

6.5. При поступлении на работу работник заполняет личный листок по учету кадров и автобиографию.

6.5.1. Личный листок по учету кадров представляет собой перечень вопросов о персональных данных работника.

6.5.2. При заполнении личного листка по учету кадров работник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркиваний, прочерков, помарок в строгом соответствии с записями, которые содержатся в его личных документах.

6.5.3. Автобиография - документ, содержащий описание в хронологической последовательности основных этапов жизни и деятельности принимаемого работника.

6.5.4. Автобиография составляется в произвольной форме, без помарок и исправлений.

6.5.5. Личный листок по учету кадров и автобиография работника хранятся в личном деле работника. В личном деле также хранятся иные документы персонального учета, относящиеся к персональным данным работника.

6.5.6. Личное дело работника оформляется после издания приказа о приеме на работу.

6.5.7. Все документы личного дела подшиваются в папку-скоросшиватель. На ней указываются фамилия, имя, отчество работника, номер личного дела.

6.5.8. К каждому личному делу прилагается фотография работника размером 3x4.

6.5.10. Личное дело ведется на протяжении всей трудовой деятельности работника.

Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

7. Передача персональных данных

7.1. 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 конфиденциальность. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, 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 Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

8. Доступ к персональным данным работника

8.1. Внутренний доступ (доступ внутри образовательного учреждения).

Право доступа к персональным данным сотрудника имеют:

- директор образовательного учреждения;
- заместители директора;
- инспектор по кадрам;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения) по согласованию с директором образовательного учреждения;
- при переводе из одного структурного подразделения в другое доступ к персональным данным сотрудника может иметь руководитель нового подразделения по согласованию с директором образовательного учреждения;
- сотрудники бухгалтерии - к тем данным, которые необходимы для выполнения конкретных функций;
- сам работник, носитель данных.

8.2. Внешний доступ.

Персональные данные вне образовательной организации могут представляться в государственные и негосударственные функциональные структуры по их запросам:

- Комитет по образованию Санкт-Петербурга;
- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военные комиссариаты;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;

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

8.4. Другие организации.

Сведения о работнике (в том числе уволенном) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

8.5. Родственники и члены семей.

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

9. Защите персональных данных работника

9.1. 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.

9.2. 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.

9.3. Защита персональных данных представляет собой жестко регламентированный процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, обеспечивающий надежную безопасность информации в процессе управленческой и производственной деятельности образовательного учреждения.

9.4. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральным законом.

9.5. «Внутренняя защита».

9.5.1. 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 образовательной организации.

9.5.2. Для обеспечения 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 конфиденциальности;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- разъяснительная работа с сотрудниками 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 и, в исключительных случаях, по разрешению директора – заместителю директора или руководителю структурного подразделения.

9.5.3. Защита персональных данных сотрудника на электронных носителях.

Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

9.6. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке предприятия и в том объеме, который позволяет не разглашать излишний объем персональных сведений о работниках предприятия.

9.7. Передача информации, содержащей сведения о персональных данных работников организации, по телефону, факсу, электронной почте без письменного согласия работника запрещается.

9.8. Личные дела и документы, содержащие персональные данные работников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

9.9. Передача информации, содержащей сведения о персональных данных работников образовательной организации по средствам электронного документооборота между Управлением ПФР, ИФНС, Ростат, ФСС производится при усиленной квалифицированной электронной подписью (далее УКЭП), которая хранится в защищенном месте (сейфе) и через компьютер с ограниченным правом доступа.

9.10. Передача информации, содержащей сведения о персональных данных работников образовательной организации по средствам электронного документооборота между банковскими системами производится при усиленной квалифицированной электронной подписи, которая хранится в защищенном месте (сейфе) и через компьютер с ограниченным правом доступа.

9.11. «Внешняя защита».

9.11.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Результатом, которого может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

9.11.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности образовательного учреждения, которое не должно знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

9.11.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

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

9.13. По возможности персональные данные обезличиваются.

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

10. Ответственность за разглашение информации, связанной с персональными данными работника

10.1. 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.