УТВЕРЖДАЮ
Директор ГАПОУ БТЭиР
имени Героя Советского Союза М.А.Афанасьева

_____С.М. Кравченко

Приказ № 396 о/д от «25» октября 2016г.

ПОЛОЖЕНИЕ

об особенностях обработки персональных данных, осуществляемых с использованием средств автоматизации в ГАПОУ «Брянский техникум энергомашиностроения и радиоэлектроники имени Героя Советского Союза М.А.Афанасьева»

1. Основные понятия

Персональные данные (ПДн) — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных — действия (операции) с персональными данными, совершаемые работодателем в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работника или других лиц, либо иным образом затрагивающих права и свободы работника или других лиц.

Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) — система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Конфиденциальность персональных данных — обязательное для соблюдения работодателем или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия работника или наличия иного законного основания.

Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами РФ не распространяется требование соблюдения конфиденциальности.

Оператор – лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

2. Общие положения

2.1. Настоящее Положение разработано в целях защиты ПДн, содержащихся в базах данных централизованной бухгалтерии, кадровой работе ГАПОУ «Брянский техникум энергомашиностроения и радиоэлектроники имени Героя Советского Союза М.А.Афанасьева» (далее по тексту - Оператор) при их обработке в информационной системе ПО 1С «Бухгалтерия», ПП Microsoft Excel и Microsoft Office в централизованной бухгалтерии и кадровой службе учреждения от нарушения конфиденциальности, целостности и доступности.

2.2. Положение разработано в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и определяет особенности обработки персональных данных Субъектов ПДн в ПСПДн Оператора.

2.3. Сбор, хранение, использование и распространение информации о частной жизни Субъекта ПДн без письменного его согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания.

2.4. Должностные лица, в обязанность которых входит обработка персональных данных Субъектов ПДн, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы.

2.5. Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

2.6. Ограничение прав Субъектов ПДн на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с действующим законодательством.

2.7. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о Субъектах ПДн, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

2.8. Неправомерность деятельности органов государственной власти и организаций по сбору ПДн может быть установлена в судебном порядке по требованию Субъектов ПДн согласно законодательства Российской Федерации.

2.9. Настоящее Положение утверждается Руководителем и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным Субъектов ПДн.

3. Перечень сведений, содержащих персональные данные Субъекта ПДн

3.1. Персональные данные граждан:
- ФИО;
- дата рождения;
- место рождения;
- семейное положение;
- гражданство;
- данные из документа удостоверяющего личность гражданина (номер, серия, дата выдачи, кем выдан);
- место жительства;
- номер контактного телефона;
- сведения о месте работы или учебы членов семьи;
- социальное положение;
- образование, профессия;
- ИНН;
- реквизиты СНИЛС;

сведения о трудовой деятельности, в том числе о стаже работы;
- сведения о социальных льготах;
- сведения о воинском учете;
- сведения о званиях и чинах;
- фотография;
- общие сведения о состоянии здоровья.

4. Требования по обработке персональных данных

4.1. В целях обеспечения прав и свобод человека и гражданина Оператор при обработке персональных данных Субъекта ПДн обязан соблюдать следующие общие требования:

4.2. Если персональные данные Субъекта ПДн, а именно граждан, возможно, получить только у третьей стороны, то Субъект ПДн должен быть

уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить Субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Субъекта ПДн дать письменное согласие на их получение.

4.3. Оператор не имеет права получать и обрабатывать персональные данные Субъекта ПДн о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

4.4. При принятии решений, затрагивающих интересы Субъекта ПДн, Оператор не имеет права основываться на персональных данных Субъекта ПДн, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4.5. Защита персональных данных Субъекта ПДн от неправомерного их использования или утраты должна быть обеспечена Оператором за счет его средств в порядке, установленном Федеральным законодательством.

4.6. Субъекта ПДн и их представители должны быть ознакомлены под роспись с документами Оператора, устанавливающими порядок обработки персональных данных Субъекта ПДн, а также об их правах и обязанностях в этой области.

5. Сбор, обработка и хранение персональных данных

5.1. Сбор персональных данных Субъектов ПДн ведется согласно требованиям, изложенным в пунктах 4.1 и 4.2 настоящего Положения.

5.2. Круг лиц, допущенных к работе с документами и материалами, содержащими персональные данные Субъекта ПДн, определяется приказом № 106 от 14.04.2011г.

5.3. При передаче персональных данных Субъекта ПДн Оператор должен соблюдать следующие требования:

- не сообщать персональные данные Субъекта ПДн третьей стороне без письменного согласия Субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта ПДн, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные Субъекта ПДн в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные Субъекта ПДн, 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.
- разрешать доступ к персональным данным Субъекта ПДн только специально уполномоченным лицам, определенных приказом ГАПОУ «Брянский техникум энергомашиностроения и радиоэлектроники имени Героя Советского Союза М.А.Афанасьева» - передавать персональные данные Субъекта ПДн их представителям в порядке установленным Федеральными законами РФ, и ограничивать эту информацию только теми персональными данными Субъекта ПДн, которые определены нормативнымиактами.

5.4. 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.

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

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

5.7. С сотрудниками, ответственными за хранение ПДн, а также с сотрудниками, владеющими ПДн в силу своих должностных обязанностей, заключаются соглашения о неразглашении персональных данных Субъектов ПДн.

5.8. Автоматизированная обработка и хранение персональных данных Субъекта ПДн производится с использованием программного обеспечения «1с Бухгалтерия», «1С Зарплата», и ПП Microsoft Excel и Microsoft Office на автоматизированных рабочих местах в общем количестве - 4 (далее - АРМ) только после выполнения всех основных мероприятий по защите информации. Хранение ПД осуществляется на корневых дисках АРМ.

5.9. Помещения (кабинет гл. бухгалтера, кабинет бухгалтерии), в которых хранятся персональные данные Субъектов ПДн, оборудованы надежными замками и сигнализацией на вскрытие помещений.

5.10. Помещения в рабочее время при отсутствии в них ответственных сотрудников должны быть закрыты.

5.11. Проведение уборки в этих помещениях должно производиться в присутствии соответствующих сотрудников.

6. Доступ к персональным данным Субъекта ПДн

6.1. Внутренний доступ.

Список работников, имеющих доступ к персональным данным Субъектов ПДн (с их полномочиями) определяется приказом по учреждению.

6.2. Внешний доступ.

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые компании и агентства;
- органы социального страхования;
- органы Пенсионного Фонда России;
- Казначейство;
-Департамент образования и науки Брянской области;
- Администрация Брянского района.

7. Защита персональных данных

7.1. Под угрозой или опасностью утраты, изменения, искажения 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.
Защита персональных данных представляет собой комплекс организационно - технических мер позволяющих, предупреждать нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, а именно:
• Криптографическое средство защиты «КрипмоПроCSP» версия 3.хучетный номер: ОК-CSP3-0270229, серийный номер СР300-О0000-ОООQВР-ОО4Е2АV-6FYZY
• Лицензионная антивирусная защита (Антивирус Касперского 2010)
• Наличие разделенных локальных сетей
• Наличие выхода на канал связи с установкой A DSL;
• Наличие паролей доступа в ОС Windows и паролей входа в «1С Зарплата»

7.1.1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации.

7.1.2. Для защиты персональных данных Субъектов ПДн необходимо соблюдать ряд мер:
- ограничение состава сотрудников, связанных с обработкой персональных данных;
- строгое избирательное и обоснованное распределение документов информации между сотрудниками;
- знание сотрудником 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 сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа сотрудниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- порядок приема, учета и контроля деятельности посетителей;
- порядок охраны территории, зданий, помещений

7.2. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для постороннего лица, пытающегося совершить несанкционированный доступ и овладение информацией.

7.3. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности управления образования Брянского района, 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 управлении образования.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных Субъекта ПДн

Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональных данных и обязательное условие обеспечения эффективности этой системы.

8.1. Руководитель, разрешающий доступ сотрудника к информации содержащей персональные данные Субъекта ПДн, несет персональную ответственность за данное разрешение.

8.2. Каждый сотрудник, получающий для работы информацию, содержащую персональные данные, несет единоличную ответственность за сохранность носителя и данной информации.

8.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных Субъекта ПДн, несут ответственность в соответствии с федеральными законами.

9. Конфиденциальность персональных данных

9.1. Работодателем и третьими лицами, получающими доступ к Пдн, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных пункте 9.2 настоящего Положения.

9.2. Обеспечение конфиденциальности Пдн не требуется:

1) в случае обезличивания Пдн;
2) в отношении общедоступных Пдн.