

Частное образовательное учреждение  
дополнительного профессионального образования  
«Промбезопасность»

«Утверждаю»

Директор ЧОУ ДПО «Промбезопасность»



С.М. Аленин

2017 г.

**ПОЛОЖЕНИЕ  
о порядке обработки и обеспечении безопасности  
персональных данных**

г. Иваново

2017 год

Настоящее Положение определяет порядок сбора, обработки и защиты персональных данных работников и слушателей частного образовательного учреждения дополнительного профессионального образования «Промбезопасность» (далее по тексту – Учебный центр) и разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон);
- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации»;
- Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСБ России от 10.07.2014 № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";
- методических материалов, принятых уполномоченными федеральными органами исполнительной власти;
- Уставом и локальными нормативными актами Учебного центра.

## 1. Общие положения

### 1.1. В Положении используются следующие термины и понятия:

персональные данные – 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, 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;

информационная система персональных данных – информационная 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;

обработка персональных данных без использования средств автоматизации (неавтоматизированная) – обработка персональных данных, содержащихся в

информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

## **2. Условия проведения обработки персональных данных**

### **2.1. Обработка персональных данных осуществляется:**

- после получения письменного согласия субъекта персональных данных, составленного по форме согласно приложению № 1 к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;
- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ивановской области;
- после принятия необходимых организационных и технических мероприятий по защите персональных данных, в соответствии с действующим законодательством.

## **3. Организационные мероприятия по защите персональных данных**

3.1. Приказом директора Учебного центра назначается работник, ответственный за защиту персональных данных.

3.2. По форме согласно приложению № 2 определяется перечень лиц, допущенных к обработке персональных данных в связи с необходимостью выполнения своих служебных обязанностей.

3.3. Приказом директора Учебного центра (лицом его заменяющим) создается Комиссия по организации информационной безопасности для проведения работ по классификации и оценки защищённости информационных систем персональных данных и обеспечению защиты информации в Учреждении.

3.4. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей персональные данные, по форме согласно приложению № 3 к настоящему Положению.

### **3.5. Запрещается:**

- обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;
- осуществлять ввод персональных данных под диктовку.

#### **4. Технические мероприятия по защите персональных данных**

Технические мероприятия по защите персональных данных включают в себя:

4.1. Исключение возможности несанкционированного доступа к персональным данным в Учреждении лицам, не допущенным к обработке персональных данных в установленном порядке.

4.2. Установку, настройку и сопровождение технических и программных средств защиты информации, средств предотвращения несанкционированного доступа и утечки информации по техническим каналам.

#### **5. Условия обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации**

5.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требования к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и методических материалов, принятых уполномоченными федеральными органами исполнительной власти.

5.2. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:

- при отсутствии установленных и настроенных сертифицированных средств защиты информации;
- при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

#### **6. Условия обработки персональных данных без использования средств автоматизации**

6.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 15.09.2008 № 687.

6.2. Общие правила организации и особенности обработки персональных данных без использования средств автоматизации.

6.2.1 Персональные данные при их неавтоматизированной обработке должны обособляться от другой информации путем фиксации их на отдельных материальных носителях персональных данных<sup>1</sup>, в специальных разделах или на полях форм (бланков).

6.2.2 Для обработки персональных данных различных категорий, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6.2.3 Уточнение персональных данных при осуществлении их неавтоматизированной обработки должно производиться путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

6.2.4 Работники Учебного центра, осуществляющие неавтоматизированную обработку персональных данных, должны быть проинформированы о факте такой обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления неавтоматизированной обработки, установленных нормативными правовыми актами органов исполнительной власти Российской Федерации, а также настоящим Положением.

### 6.3. Правила ведения документов, содержащих персональные данные.

6.3.1. При использовании в Учреждении типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкции по ее заполнению, карточки, журналы и пр.) должны содержать сведения о целях неавтоматизированной обработки персональных данных, наименование и адрес оператора<sup>2</sup>, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый субъект персональных данных, указанный в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в этом документе, не нарушая законных прав и интересов других субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

6.4. Правила раздельной обработки персональных данных при несовместимости целей их обработки.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

---

<sup>1</sup> В настоящем документе под «материальным носителем персональных данных» понимается любой носитель информации на магнитной, магнитооптической, оптической или бумажной основе.

<sup>2</sup> В настоящем Положении под «оператором» понимается Учебный центр.

– при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

– при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

6.5. Обработка персональных данных сотрудников организаций в рамках проведения анализа Учебным центром на соответствие профессиональной квалификации указанных сотрудников требованиям, установленным действующим трудовым законодательством Российской Федерации, осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 15.09.2008 № 687.

## **7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных**

В соответствии со ст. 24 Федерального закона № 152 «О персональных данных» лица, виновные в нарушении требований настоящего Федерального закона, несут граждансскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

### **7.1. Ответственность работодателя.**

Работодатель как юридическое лицо может быть привлечен к административной ответственности за нарушение порядка сбора, хранения, использования или распространения персональных данных.

Помимо организации, ответственность за нарушение несет ее руководитель как должностное лицо. Под должностным лицом понимается лицо, выполняющее организационно-распорядительные или административно-хозяйственные функции.

### **7.2. Ответственность работника, имеющего доступ к персональным данным.**

Согласно ст. 90 ТК РФ работник, по вине которого было допущено нарушение норм, регулирующих получение, обработку и защиту персональных данных других работников, может быть привлечен к дисциплинарной и материальной, а также к гражданско-правовой, административной и уголовной ответственности.

### **7.3. Административная ответственность работника, имеющего доступ к персональным данным.**

На основании ст. ст. 2, 3, 5, 6 Закона о персональных данных персональные данные относятся к информации, доступ к которой ограничен. В соответствии со ст. 13.14 КоАП РФ разглашение подобной информации (за исключением случаев, если такое разглашение влечет уголовную ответственность) лицом, получившим доступ к ней в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа:

- на граждан - от 500 до 1000 руб.;
- на должностных лиц - от 4 000 до 5 000 руб.

Следовательно, если будет установлено, что разглашение персональных данных произошло по вине работника, ответственного за хранение, обработку и использование персональных данных других работников, то его могут привлечь к административной ответственности в виде штрафа.

7.4. Дисциплинарная ответственность работника, имеющего доступ к персональным данным.

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 ТК РФ). Согласно ст. 192 ТК РФ за совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания:

- 1) замечание;
- 2) выговор;
- 3) увольнение по соответствующим основаниям.

7.5. Уголовная ответственность работника, имеющего доступ к персональным данным.

Уголовная ответственность за незаконные действия, нарушающие права личности в области защиты персональных данных, установлена в Уголовном кодексе РФ. Так, согласно ст. 137 УК РФ "Нарушение неприкосновенности частной жизни", незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан, наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до одного года, либо арестом на срок до 4х месяцев, либо лишением свободы на срок до 2х лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3х лет.

7.6. Материальная ответственность работника, имеющего доступ к персональным данным.

Статьей 90 ТК РФ предусмотрена материальная ответственность за виновное нарушение норм, регулирующих получение, обработку и защиту персональных данных работников. Так, в результате незаконного 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 под 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. 7 ч. 1 ст. 243 ТК РФ

материальная ответственность в полном размере причиненного ущерба возлагается на работника в случае разглашения сведений, составляющих охраняемую законом тайну.

7.7. Гражданко-правовая ответственность работника, имеющего доступ к персональным данным.

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 (бездействием), 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. Следовательно, если в результате нарушения норм, регулирующих хранение, обработку и использование персональных данных работника, допущенного лицом, ответственным за осуществление вышеперечисленных действий с персональными данными, работнику причинен имущественный ущерб или моральный вред, то он подлежит возмещению в денежной форме в соответствии со статьями Гражданского кодекса РФ.

## 8. Контроль соблюдения

8.1. Контроль соблюдения настоящего Положения осуществляется директором Учебного центра.