



Автономная некоммерческая организация
дополнительного профессионального образования
«Учебно-курсовой комбинат»

УТВЕРЖДАЮ
Директор
АНО ДПО «Учебно-курсовой комбинат»
Н.М. Плотникова
20 мая 2019 г.

**ИНСТРУКЦИЯ
О ПОРЯДКЕ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ
В АНО ДПО «Учебно-курсовой комбинат»**

20 мая 2019 г.

г. Коркино

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция разработана с целью защиты интересов АНО ДПО «Учебно-курсовой комбинат» (далее – Организация) и субъектов персональных данных, в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными.

1.2. Данная инструкция предназначена для использования всеми работниками Организации, допущенными к работе с персональными данными.

1.3. Отнесение информации к сведениям, содержащим персональные данные, осуществляется в соответствии с «Положением об обработке персональных данных, осуществляемой без использования средств автоматизации» и с «Положением об обработке персональных данных с использованием средств автоматизации».

1.4. Работники Организации, доступ которых к персональным данным необходим для выполнения ими своих служебных обязанностей, должны быть ознакомлены под подпись с настоящей Инструкцией и предупреждены о возможной ответственности за её нарушение.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Информация** – сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.2. **Документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.3. Доступ к информации – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

2.5. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.6. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.7. Обработка персональных данных – 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 (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.8. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.9. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

3. ПОРЯДОК РАБОТЫ СО СВЕДЕНИЯМИ, СОДЕРЖАЩИМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

3.1. При обработке персональных данных на бумажных документах, съёмных носителях (дисках, флеш-носителях и т.п.), компьютерах и других технических средствах, работники Организации обязаны следить как за сохранностью самих бумажных документов, съёмных носителей и компьютеров и других технических средств, так и за сохранностью содержащейся в них информации, а именно не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с персональными данными.

3.2. Запрещается хранение или оставление бумажных документов и съёмных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий. Напечатанные документы, содержащие персональные данные, должны изыматься из принтеров немедленно. Хранение бумажных документов и съёмных носителей, содержащих персональные данные, допускается только в специальных закрытых шкафах, сейфах и помещениях, к которым исключён доступ лиц, не допущенных к обработке соответствующих персональных данных.

3.3. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съёмные носители.

3.4. Запрещается использовать для передачи персональных данных съёмные носители, не учтённые в «Журнале учёта машинных носителей информации в АНО ДПО «Учебно-курсовой комбинат»».

3.5. Запрещается выносить документы, съёмные носители или переносные компьютеры, содержащие персональные данные, за пределы служебных помещений Организации, если это не требуется для выполнения служебных (трудовых) обязанностей и если на это не дано разрешение руководителя Организации или ответственного за организацию обработки персональных данных.

3.6. Бумажные документы с персональными данными, у которых истёк срок хранения, лишние или испорченные копии документов с персональными данными, должны быть уничтожены без возможности их восстановления (например, в shredders или путем разрезания).

3.7. Большие объёмы бумажных документов с персональными данными, съёмные носители с персональными данными, а также встроенные в компьютеры носители с персональными данными должны уничтожаться под контролем ответственного за организацию обработки персональных данных, способом, исключающим дальнейшее восстановление информации.

3.8. Мониторы компьютеров, использующихся для обработки персональных данных, должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуск к обработке персональных данных.

3.9. Категорически запрещается упоминать в разговоре с третьими лицами сведения, содержащие персональные данные.

3.10. Запрещается в нерабочее время или за пределами служебных помещений упоминать в разговоре с кем-либо, включая любых работников Организации, сведения, содержащие персональные данные.

3.11. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки персональных данных, администратора безопасности ИСПДн, руководства, или лица, уполномоченного руководством на обсуждение данных вопросов.

4. ПОРЯДОК ДОСТУПА ЛИЦ В ПОМЕЩЕНИЯ

4.1. При обеспечении доступа лиц соблюдаются требования законодательства РФ по защите персональных данных.

4.2. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности работников организации и определяет порядок пропуска работников Организации и иных организаций и учреждений, обучающихся Организации в помещения.

4.3. Контроль за порядком обеспечения доступа лиц в помещения возлагается на руководителя организации.

4.4. Не допускается нахождение работников Организации в помещениях в нерабочее для них время без разрешения руководителя.

4.5. Нахождение посетителей допускается только в рабочее время.

4.6. В помещения ИСПДн пропускаются:

- беспрепятственно – директор Организации и работники, имеющие допуск к работе с персональными данными и с целью выполнения должностных обязанностей;

- с разрешения руководителя Организации, в сопровождении ответственного за организацию обработки персональных данных или руководителя - сотрудники контролирующих органов, сотрудники пожарных и аварийных служб, сотрудники полиции;

- ограниченно –работники, не имеющие допуска к работе с персональными данными или не имеющие функциональных обязанностей в помещении, работники сторонних организаций и учреждений для выполнения договорных отношений

4.7.Посетители пропускаются в помещения ИСПДнОрганизации в рабочее время в сопровождении работников, допущенных к обработке персональных данных.

4.8.В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

4.9.Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством Организации.

4.10.В целях предотвращения несанкционированного доступа к сведениям, содержащим персональные данные, работы проводятся только под контролем ответственного за организацию обработки персональных данных или руководителя организации.

4.11.Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных сотрудников запираются на ключ. Помещение должно быть оборудовано специальными инженерными средствами, такими как усиленные двери, запирающиеся решетки на окнах и т.п.

4.12.Руководитель организации, либо работники, уполномоченные хранить ключи от сейфов и помещений должны вести «Журнал учета ключей от сейфов и помещений в АНО ДПО «Учебно-курсовой комбинат».

4.13.Оборудование в помещении должно размещаться таким образом, чтобы исключить возможность бесконтрольного доступа к нему посторонних лиц. Мониторы компьютеров должны быть ориентированы таким образом, чтобы исключить возможность просмотра отображаемой на них информации лицами, не имеющими допуска к обработке персональных данных.

4.14.Окна помещений, в которых ведётся обработка персональных данных, должны быть оборудованы шторами или жалюзи.

5. ТРЕБОВАНИЯ ПО ТЕХНИЧЕСКОМУ УКРЕПЛЕНИЮ

5.1.Руководитель организации обеспечивает обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности и должны руководствоваться следующими основными требованиями:

- двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек.

5.2.Конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол.

5.3.Стекла в рамах должны быть надежно закреплены в пазах.

5.4.Рамы указанных оконных проемов оборудуются запорными устройствами.

6. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1.РаботникиОрганизации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную,

административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

6.2. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним доступ), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) Организации, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник Организации, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Организации (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

6.3. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

6.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

6.5. Должность руководителя Организации за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.