

**1. Общие положения**

1.1. Положение о защите персональными данных работников, клиентов и контрагентов (далее – Положение) АНО «Школа охраны 42» (далее – Организация) разработано в соответствии с Конституцией РФ, Трудовым кодексом, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ, Федеральным законом от 30.12.2020 № 519-ФЗ и иными нормативно-правовыми актами, действующими на территории России.

1.2. Цель настоящего Положения – защита персональных данных работников, клиентов и контрагентов Организации от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

1.3. Для целей настоящего Положения используются следующие основные понятия:

под персональными данными (далее – ПД) понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных;

под угрозами безопасности ПД понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

под уровнем защищенности ПД понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПД при их обработке в информационной системе.

1.4. Настоящее Положение и изменения к нему утверждаются директором Организации и вводятся приказом. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.5. Настоящее Положение вступает в силу с момента его утверждения директором Организации и действует бессрочно, до замены его новым Положением.

**2. Защита персональных данных**

2.1. Организация принимает следующие меры по защите ПД:

2.1.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите ПД.

2.1.2. Разработка политики конфиденциальности в отношении обработки ПД.

2.1.3. Установление правил доступа к ПД, обеспечение регистрации и учета всех действий, совершаемых с ПД.

2.1.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

2.1.5. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.1.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

2.1.7. Соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ.

2.1.8. Обнаружение фактов несанкционированного доступа к ПД.

2.1.9. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.1.10. Обучение работников, непосредственно осуществляющих обработку ПД, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Организации в отношении обработки ПД, локальным актам по вопросам обработки персональных данных.

2.1.11. Осуществление внутреннего контроля сбора, обработки, передачи персональных данных.

2.1.12. Определение типа угроз безопасности и уровней защищенности ПД, которые хранятся в информационных системах.

2.2. Угрозы защищенности персональных данных.

2.2.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

2.2.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.

2.2.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

2.3. Уровни защищенности персональных данных

2.3.1. Первый уровень защищенности. Если организация отнесла информационную систему к первому типу угрозы или если тип угрозы второй, но организация обрабатывает специальные категории ПД более 100 тыс. физических лиц без учета работников.

2.3.2. Второй уровень защищенности. Если тип угрозы второй и работодатель обрабатывает специальные категории ПД работников вне зависимости от их количества или специальные категории ПД менее чем 100 тыс. физических лиц, или любые другие категории ПД более чем 100 тыс. физических лиц, или при третьем типе угрозы организация обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

2.3.3. Третий уровень защищенности. Если при втором типе угрозы организация обрабатывает общие ПД работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы организация обрабатывает специальные категории ПД работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы организация обрабатывает биометрические ПД, или при третьем типе угрозы организация обрабатывает общие ПД более чем 100 тыс. физических лиц.

2.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы организация обрабатывает только общие ПД работников или менее чем 100 тыс. физических лиц.

2.4. При четвертом уровне защищенности персональных данных АНО «Школа охраны 42»:

обеспечивает режим безопасности помещений, в которых размещает информационную систему;

обеспечивает сохранность носителей информации;

утверждает перечень работников, допущенных до ПД;

2.5. При третьем уровне защищенности ПД дополнительно к мерам, перечисленным в пункте 2.4 настоящего Положения, Организация назначает ответственного за обеспечение безопасности ПД в информационной системе.

2.6. При втором уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4, 2.5 настоящего Положения, Организация ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

2.7. При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4—2.6 настоящего Положения, Организация:

обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к ПД в системе;

создает отдел, ответственный за безопасность ПД в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

2.8. В целях защиты ПД на бумажных носителях Организация:

приказом назначает ответственного за обработку ПД;

использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

ограничивает допуск в помещения, где хранятся документы, которые содержат ПД работников, клиентов и контрагентов;

хранит документы, содержащие ПД работников, клиентов и контрагентов в шкафах, запирающихся на ключ;

хранит трудовые книжки работников в сейфе в отделе кадров.

2.9. В целях обеспечения конфиденциальности документы, содержащие ПД работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и службы охраны труда работодателя. Документы, содержащие ПД клиентов и контрагентов, оформляются, ведутся и хранятся работниками бухгалтерии, работниками учебного отдела.

2.10. Работники отдела кадров, бухгалтерии и учебно-методического отдела Организации, допущенные к ПД работников, клиентов и контрагентов, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПД работников не допускаются.

2.11. Передача ПД по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия работника, клиента и контрагента на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.12. Передача информации, содержащей сведения о ПД работников и клиентов, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

**3. Гарантии конфиденциальности персональных данных**

3.1. Все работники организации, осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением и требованиями законодательства РФ.

3.2. Работники, клиенты и контрагенты вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

3.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.