

Государственное бюджетное учреждение Ленинградской области центр помощи детям-сиротам и
детям, оставшимся без попечения родителей
«Ивангородский центр по содействию семейному воспитанию для детей
с ограниченными возможностями здоровья»

(ГБУ ЛО «Ивангородский центр для детей с ОВЗ»)

РАССМОТРЕНО

УТВЕРЖДЕНО

Общим собранием ГБУ ЛО «Ивангородский
центр для детей с ОВЗ»

Протокол №2 от 24.12.2019

Приказ №7 от 10.01.2020

ПОЛОЖЕНИЕ
о защите персональных данных
ГБУ ЛО «Ивангородский центр для детей с ОВЗ»

1. Общие положения

1.1. Положение о защите персональных данных ГБУ ЛО «Ивангородский центр для детей с ОВЗ» (далее – Работодатель) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории России.

1.2. Цель настоящего Положения – защита персональных данных работников ГБУ ЛО «Ивангородский центр для детей с ОВЗ» от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

1.3. В целях настоящего Положения:

- 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 ГБУ ЛО «Ивангородский центр для детей с ОВЗ» и вводятся приказом.

2. Защита персональных данных

2.1. Работодатель принимает следующие меры по защите ПД:

2.1.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД.

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

2.1.3. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

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

2.1.5. Обнаружение фактов несанкционированного доступа к ПД.

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

2.1.7. Осуществление внутреннего контроля и аудита.

2.1.8. 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 работодатель отнес информационную систему к первому типу угрозы или если тип угрозы второй, но работодатель 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 работодатель обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

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

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

2.4. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещает информационную систему;

- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных до ПД;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

2.5. В целях защиты ПД на бумажных носителях работодатель:

- приказом назначает ответственного за обработку ПД;
- ограничивает допуск в помещения, где хранятся документы, которые содержат ПД работников;
- хранит документы, содержащие ПД работников в шкафах, к которым ограничен доступ или которые запираются на ключ;
- хранит трудовые книжки работников в сейфе в отделе кадров.

2.6. В целях обеспечения конфиденциальности документы, содержащие ПД работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и службы охраны труда работодателя.

2.7. Работники отдела кадров, бухгалтерии и службы охраны труда работодателя, допущенные к ПД работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПД работников не допускаются.

2.8. Допуск к документам, содержащим ПД работников, внутри организации предоставляется сотрудникам организации, чье должностные обязанности предусматривают обработку ПД.

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

2.10. Передача информации, содержащей сведения о ПД работников, 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, требованиями законодательства РФ.

3.2. Работник 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.