**КОМИТЕТ МОЛОДЕЖНОЙ ПОЛИТИКИ МУРМАНСКОЙ ОБЛАСТИ**

**ГОСУДАРСТВЕННОЕ ОБЛАСТНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ МОЛОДЕЖНОЙ ПОЛИТИКИ «РЕГИОНАЛЬНЫЙ ЦЕНТР РАЗВИТИЯ ДОБРОВОЛЬЧЕСТВА И ПОДДЕРЖКИ МОЛОДЕЖНЫХ ДВИЖЕНИЙ»**

# П Р И К А З

25.12.2023

№ 105 -ОД

г. Мурманск

**Об утверждении Положения о защите персональных данных в ГОБУМП «Региональный центр развития добровольчества и поддержки молодежных движений»**

Во исполнение ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

**ПРИКАЗЫВАЮ:**

1. Утвердить и ввести в действие Положение о защите персональных данных в ГОБУМП «Региональный центр развития добровольчества и поддержки молодежных движений» с 26.12.2023.
2. Контроль за исполнением настоящего приказа оставляю за собой.

**Директор** **Л.Л. Мостовой**

Приложение № 1
к приказу № 105 - ОД от 25.12.2023 г.

# ПОЛОЖЕНИЕ
## о защите персональных данных в ГОБУМП «

### 1. Общие положения

1.1. Положение о защите персональных данных государственного областного бюджетного учреждения молодежной политики «Региональный центр развития добровольчества и поддержки молодежных движений» (далее – ГОБУМП «РЦРДИПМД», Учреждение) 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 ГОБУМП «РЦРДИПМД» 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 ГОБУМП «РЦРДИПМД» или лицом, его заменяющим и вводятся приказом. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

### 2. Защита персональных данных

2.1. Учреждение принимает следующие меры по защите ПД:

2.1.1. Назначает лицо, ответственное за организацию обработки ПД, которое осуществляет обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите ПД.

2.1.2. Устанавливает правила доступа к ПД, обеспечивает регистрацию и учет всех действий, совершаемых с ПД.

2.1.3. Устанавливает индивидуальные пароли доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

2.1.4. Применяет прошедшие в установленном порядке процедуры оценки соответствия средств защиты информации.

2.1.5. Устанавливает сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

2.1.6. Соблюдает условия, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ.

2.1.7. Обнаруживает факты несанкционированного доступа к ПД.

2.1.8. Восстанавливает ПД, модифицированные или уничтоженные вследствие несанкционированного доступа к ним.

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

2.1.10. Осуществляет внутренний контроль и аудит.

2.1.11. Определяет тип угрозы безопасности и уровни 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 Учреждение:

- обеспечивает режим безопасности помещений, в которых размещаете 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. При третьем уровне защищенности ПД дополнительно к мерам, перечисленным в пункте 2.4 настоящего Положения, работодатель 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, работодатель 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, работодатель:

- 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 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, 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 МАУ МП «Дом молодежи».

2.10. Работники отдела кадров, бухгалтерии МАУ МП «Дом молодежи», допущенные к ПД работников, 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 на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.12. 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 Учреждения, 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.