Приложение№1

«УТВЕРЖДЕНО»
приказом директора МАУ ДПО ЦРО
от 22.08.2022 № 129

ПОЛОЖЕНИЕ
о защите персональных данных

I. Общие положения

1.1. Положение защите персональных данных МАУ ДПО ЦРО разработано в соответствии с Конституцией Российской Федерации, ст.85, ст.90, ст.351.1 Трудового кодекса Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Уставом МАУ ДПО ЦРО, лицензией на осуществление образовательной деятельности (регистрационный номер лицензии: № Л035-01219-10/00267015), выданной Министерством образования и спорта Республики Карелия.

1.2. Настоящее Положение определяет политику МАУ ДПО ЦРО (далее – Учреждение) как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных и является элементом системы мер, принимаемых Учреждением для защиты обрабатываемых персональных данных от несанкционированного доступа, уничтожения, искажения или разглашения.

1.3. Положение об обработке и защите персональных данных (далее Положение) Учреждения определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных.

1.4. Персональные данные относятся к категории конфиденциальной информации.

1.5. Изменения в Положение могут быть внесены в установленном действующим законодательством порядке.

II. Условия и порядок обработки персональных данных

2.1. Обработка персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и карьерном росте, а также обеспечения личной безопасности работников, сохранности имущества, контроля количества и качества выполняемой работы, обеспечения работников установленными законодательством Российской Федерации условий труда, гарантий и компенсаций.

Обработка персональных данных слушателей кусов повышения квалификации может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в повышении квалификации, обеспечения личной

безопасности и сохранности имущества, контроля качества предоставляемой образовательной услуги.

Обработка персональных данных граждан, обратившихся в психолого-медико-педагогическую комиссию при МАУ ДПО ЦРО осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в определении образовательного маршрута для несовершеннолетнего, обеспечения личной безопасности и сохранности имущества, контроля качества предоставляемой услуги.

Обработка персональных данных посетителей может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, обеспечения безопасности работников, в частности, в отношении профилактики террористических актов, сохранности личного и имущества Учреждения.

2.2. Оператор определяет объем, содержание обрабатываемых персональных данных работников, посетителей, руководствуясь Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным Законом «Об образовании в Российской Федерации» и иными федеральными законами.

2.3. Все персональные данные работника предоставляются работником, за исключением случаев, предусмотренных федеральным законом. Если персональные данные работника возможно получить только у третьей стороны, то Оператор обязан заранее уведомить об этом работника и получить его письменное согласие. Оператор должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

Все персональные данные несовершеннолетнего в возрасте до 14 лет (малолетнего) предоставляются его родителями (законными представителями). Если персональные данные несовершеннолетнего возможно получить только у третьей стороны, то его родители (законные представители) должны быть уведомлены об этом заранее. От них должно быть получено письменное согласие на получение персональных данных от третьей стороны. Родители (законные представители) ребенка должны быть проинформированы о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

Персональные данные несовершеннолетнего в возрасте старше 14 лет могут быть предоставлены им самим с письменного согласия своих законных представителей - родителей, усыновителей или попечителя. Если персональные данные ребенка возможно получить только у третьей стороны, то несовершеннолетний, его родители (законные представители) должны быть уведомлены об этом заранее. От него и его родителей (законных представителей) должно быть получено письменное согласие на получение персональных данных от третьей стороны. Несовершеннолетние старше 14 лет и его родители (законные представители) должны быть проинформированы о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

Персональные данные посетителей предоставляются самим посетителем один раз при входе в образовательное учреждение на добровольной основе.

2.4 Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Персональные данные слушателей курсов повышения квалификации - информация, необходимая Учреждению в связи с отношениями, возникающими между обучающимся и Учреждением.

Персональные данные посетителя - информация, необходимая оператору для обеспечения безопасности работников, в частности, в отношении профилактики террористических актов, сохранности личного и школьного имущества.

2.5. К персональным данным Субъекта, которые обрабатывает Оператор, относятся:

- фамилия, имя, отчество (в т. ч. предыдущие),
- паспортные данные или данные документа, удостоверяющего личность,
- дата рождения, место рождения,
- гражданство,
- отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения,
- данные документов о профессиональном образовании, профессиональной переподготовки, повышении квалификации, стажировке,
- данные документов о подтверждении специальных знаний,
- данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений и сведения о наградах и званиях,
- знание иностранных языков,
- семейное положение и данные о составе и членах семьи,
- сведения об отсутствии судимости,
- сведения о социальных льготах, пенсионном обеспечении и страховании,
- данные документов об инвалидности (при наличии),
- данные медицинского заключения (при необходимости),
- стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке,
- должность, квалификационный уровень,
- сведения о заработной плате (доходах), банковских картах,
- адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства, адрес электронной почты,
- номер телефона (домашний, мобильный),
- данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории РФ (ИНН),
- данные страхового свидетельства государственного пенсионного страхования,
- иная необходимая информация, которую Субъект добровольно сообщает о себе для получения услуг, предоставляемых Учреждением, если ее обработка не запрещена законом.

2.6. Обработка персональных данных работников, слушателей курсов, граждан, обратившихся в ПМПК, посетителей включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, представление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.7. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем:

2.7.1. Получения оригиналов необходимых документов (паспорт, СНИЛС, заявление, трудовая книжка, автобиография, иные документы, представляемые специалисту по кадрам).

2.7.2. Копирования оригиналов документов.

2.7.3. Внесения сведений в учетные формы (на бумажных и электронных носителях).

2.7.4. Формирования персональных данных в ходе кадровой работы.

2.7.5. Внесения персональных данных в информационные системы персональных данных.

2.8. При сборе персональных данных работник, осуществляющий сбор (получение) персональных данных непосредственно от работников, слушателей курсов, граждан, обратившихся и проходящих обследование на ПМПК, посетителей, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа представить их персональные данные.

III. Порядок и сроки хранения персональных данных

3.1. Персональные данные субъектов персональных данных хранятся на бумажных и/или электронных носителях в специально предназначенных для этого помещениях.

3.2. В процессе хранения персональных данных субъектов персональных данных должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;

- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящим Положением;

- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

3.3. Доступ к персональным данным субъектов персональных данных имеют лица, назначенные соответствующим приказом директора.

3.4. Лица, имеющие доступ к персональным данным обязаны использовать персональные данные работников, слушателей курсов, граждан, обратившихся и проходящих обследование на ПМПК, посетителей лишь в целях, для которых они были предоставлены.

3.5. Ответственным за обработку и хранение персональных данных (ПД) является лицо, назначенное приказом директора.

3.6. Персональные данные работника отражаются в личной карточке работника (форма Т-2), которая заполняется после издания приказа о его приеме на работу, и личном деле. Личные карточки и личные дела работников хранятся в специально оборудованных шкафах, к которым обеспечен контролируемый доступ.

Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом.

Документы, содержащие персональные данные клиентов ПМПК, поступившие от клиента, родителя (законного представителя), сведения о клиенте, поступившие от третьих лиц с письменного согласия клиента, родителя (законного представителя); иная информация, которая касается отношений обучения, консультирования, диагностики, коррекции, сопровождения клиента, хранятся в сейфе на бумажных носителях и на электронных носителях с ограниченным доступом.

Персональные данные посетителей отражаются в Журнале учета посетителей.

3.7. Сроки хранения персональных данных определяются в соответствии с номенклатурой дел МАУ ДПО ЦРО.

3.8. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

3.9. Оператор обеспечивает за счет собственных средств защиту персональных данных от неправомерного их использования или утраты в соответствии с требованиями, установленными законодательством Российской Федерации.

IV. Передача персональных данных

4.1. При передаче персональных данных работников и иных субъектов персональных данных Учреждения другим юридическим и физическим лицам Учреждение должно соблюдать следующие требования:

- персональные данные работника не могут быть сообщены третьей стороне без письменного согласия работника, слушателя курсов, родителей (законных представителей) несовершеннолетнего (малолетнего) ребенка, за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника (иного субъекта персональных данных), а также в случаях, установленных федеральным законом;

- лица, получающие персональные данные субъекта персональных данных должны предупреждаться о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

Учреждение должно требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъектов персональных данных,

обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

4.2. Передача персональных данных работника его представителям может быть осуществлена в установленном действующим законодательством порядке только в том объеме, который необходим для выполнения указанными представителями их функций.

V. Порядок защиты персональных данных в ИСПДн

5.1. Обработка персональных данных осуществляется на законной и справедливой основе.

5.2. Определение уровня защищенности персональных данных при их обработке в ИСПДн, осуществляется в порядке, установленном законодательством Российской Федерации.

5.3. Работником Учреждения, имеющим право осуществлять обработку персональных данных в ИСПДн, предоставляется уникальный логин и пароль для доступа к соответствующей ИСПДн. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными обязанностями работников.

Информация вносится в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

5.4. Обеспечение безопасности обрабатываемых персональных данных в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

- определение угроз безопасности персональных данных при их обработке;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным Учреждения, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными.
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных.
- постоянный контроль за обеспечением уровня защищенности персональных данных в ИСПДн;

5.5. Администратор безопасности ИСПДн, организует и контролирует ведение учета материальных носителей персональных данных и обеспечивает:

- своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в Учреждении;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- постоянный контроль за обеспечением уровня защищенности персональных данных;

- знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- при обнаружении нарушений порядка представления персональных данных незамедлительное приостановление представления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

- разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

5.6. Ответственными за выполнение требований по защите персональных данных при их обработке являются лица, назначенные приказом директора, эксплуатирующих, а также использующих информационные системы, пользователи информационных систем, администратор безопасности.

5.7. Обмен персональными данными при их обработке Учреждением может осуществляется только по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения сертифицированных программных и технических средств.

5.8. Доступ работников, допущенных к обработке персональных данных в ИСПДн, предусматривает обязательное прохождение процедуры идентификации и аутентификации пользователя.

5.9. В случае выявления нарушений порядка обработки персональных данных в ИСПДн уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

5.10. В случае выявления обнаружения инцидентов, которые повлекли неправомерную передачу ПД (атак на информационные ресурсы) Оператор обязан:

- уведомить о случившемся Роскомнадзор в течение 24 часов;

- провести внутреннее расследование и уведомить службу о его результатах в течение 72 часов;

- представить сведения о лицах, действия которых стали причиной инцидента (при наличии).

VI. Права субъектов на обеспечение защиты персональных данных

В целях обеспечения защиты персональных данных работники, слушатели курсов, граждане, пользующиеся услугами ПМПК (родители (законные представители) малолетнего несовершеннолетнего гражданина), посетители имеют право:

- получать полную информацию о своих персональных данных и их обработке;

- свободного бесплатного доступа к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении работника, иного субъекта персональных данных.

- требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. Указанное требование должно быть оформлено письменным заявлением работника на имя директора Учреждения.

При отказе директора Учреждения исключить или исправить персональные данные работник, иной субъект персональных данных имеет право заявить в письменном виде директору учреждения о своем несогласии, с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник, граждане, пользующиеся услугами ПМПК имеет право дополнить заявлением, выражающим его собственную точку зрения.

- требовать об извещении Учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

- обжаловать в суде любые неправомерные действия или бездействия учреждения при обработке и защите его персональных данных.

VII. Обязанности Учреждения

В соответствии с требованиями Закона о персональных данных Учреждение обязано:

-) предоставлять субъекту персональных данных по его запросу информацию, касающуюся обработки его персональных данных, либо на законных основаниях предоставить отказ в течение десяти дней с даты получения запроса субъекта персональных данных или его представителя, с возможностью направления в Роскомнадзор уведомления о продлении срока предоставления запрашиваемой информации до 5 рабочих дней;

-) по требованию субъекта персональных данных уточнять, блокировать или удалять обрабатываемые персональные данные, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих эти факты;

-) вести журнал учета обращений субъектов персональных данных, в котором должны фиксироваться запросы субъектов персональных данных на получение персональных данных, а также факты предоставления персональных данных по этим запросам;

-) уведомлять субъекта персональных данных об обработке персональных данных в том случае, если персональные данные были получены не от субъекта персональных данных.

Исключение составляют следующие случаи:

- субъект персональных данных уведомлен об осуществлении обработки Учреждением его персональных данных;

- персональные данные получены Учреждением в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, или на основании федерального закона;

- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

- Учреждение осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

-- предоставление субъекту персональных данных сведений, содержащихся в уведомлении об обработке персональных данных, нарушает права и законные интересы третьих лиц;

-) в случае достижения цели обработки персональных данных незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором;

-) в случае изменения сведений об обработке персональных данных, проинформировать Роскомнадзор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения.

VIII. Обязанности субъекта персональных данных по обеспечению достоверности его персональных данных

8.1. В целях обеспечения достоверности персональных данных работники обязаны:

- при приеме на работу представлять уполномоченным работникам Учреждения достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.

- в случае изменения персональных данных работника: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей и т.п.) сообщать об этом в течение 5 рабочих дней с даты их изменений.

IX. Контроль обеспечения безопасности персональных данных

9.1. Целью контроля является соблюдение работниками, обрабатывающими персональные данные, требований по обеспечению безопасности персональных данных.

9.2. Задачами контроля являются:

- установление фактического положения дел по обеспечению безопасности персональных данных при их обработке:

- выявление проблемных вопросов в организации обеспечения безопасности персональных данных.

- обеспечение соблюдения законодательства Российской Федерации в области персональных данных.

- выработка мер по оказанию методической и практической помощи работникам, обрабатывающими персональные.

X. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

10.1. Оценкой вреда, который может быть причинен субъектам персональных данных, в случае нарушения требований по обработке и обеспечению безопасности персональных данных является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных.

10.2. К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав субъектов персональных данных или иным образом затрагивающие их права, свободы и законные интересы.

10.3. В целях недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определения соотношения вреда, который может быть причинен субъектам персональных данных при обработке персональных данных, должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных.

XI. Ответственность

11.1. Работники, допущенные к обработке персональных данных, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут персональную

ответственность за несоблюдение требований по обеспечению безопасности персональных данных, установленных в соответствии с законодательством Российской Федерации и настоящим Положением.

11.2. В случаях нарушения порядка обеспечения безопасности персональных данных и нанесения Учреждению материального или иного ущерба, виновные лица несут дисциплинарную, административную, гражданско-правовую, уголовную и иную ответственность, предусмотренную законодательством Российской Федерации.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
5B8514E92BEA938045BFBCA8D0EE50FB42A79C24
Владелец: Иконникова Любовь Викторовна
Действителен: с 05.10.2021 до 05.01.2023