

«УТВЕРЖДЕНО»
приказом директора
МАУ ДПО ЦРО
от 11.04.2025 № 87 о/д

**РЕГЛАМЕНТ
ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ
В МУНИЦИПАЛЬНОМ АВТОНОМНОМ УЧРЕЖДЕНИИ ДОПОЛНИТЕЛЬНОГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ПЕТРОЗАВОДСКОГО ГОРОДСКОГО
ОКРУГА «ЦЕНТР РАЗВИТИЯ ОБРАЗОВАНИЯ»
(МАУ ДПО ЦРО)**

1. Информация о документе

1.1. Настоящий Регламент предоставления доступа к персональным данным в МАУ ДПО ЦРО (далее - Регламент) определяет порядок предоставления работникам и третьим лицам доступа к персональным данным в МАУ ДПО ЦРО (далее - Учреждение). Настоящий Регламент принят в целях обеспечения безопасности персональных данных при их обработке в Учреждение.

Настоящий документ обязаны знать и использовать в работе все работники Учреждения, допущенные к обработке персональных данных, а также ответственные за обработку и обеспечение безопасности персональных данных в МАУ ДПО ЦРО.

1.2. Внешние нормативные и распорядительные документы:

- Конституция Российской Федерации; Гражданский кодекс Российской Федерации.
- Трудовой кодекс Российской Федерации.
- Налоговый кодекс Российской Федерации.
- Федеральный закон от 27.07.2006 " 152-ФЗ "О персональных данных".
- Федеральный закон от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации".
- Федеральный закон от 06.12.2011 N 402-ФЗ "О бухгалтерском учете".
- Федеральный закон от 15.12.2001 N 167-ФЗ "Об обязательном пенсионном страховании в Российской Федерации".
- Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Приказ ФСТЭК России от 18.02.2014 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Внутренние нормативные и распорядительные документы МАУ ДПО ЦРО:

- Устав МАУ ДПО ЦРО
- Лицензия на осуществление образовательной деятельности.
- Договоры, заключаемые между Учреждением и физическими лицами.
- Согласие субъектов персональных данных на обработку их персональных данных.
- Политика защиты и обработки персональных данных.
- Положение о работе с персональными данными работников Учреждения.
- Положение об обработке и защите персональных данных работников Учреждения
- Приказ о назначении ответственных по работе с персональными данными.
- Приказ об утверждении перечня сотрудников, допущенных к работе с персональными данными в Учреждении.

2. Порядок предоставления допуска к обработке персональных данных

2.1. К обработке персональных данных в Учреждение допускаются работники, должности которых указаны в документе «Перечень функциональных подразделений и должностей, допущенных к обработке персональных данных» (далее – Перечень) (Приложение №1).

2.2. Предоставление допуска к обработке персональных данных работникам, должности которых не включены в Перечень, запрещено.

2.3. Допуск к обработке персональных данных предоставляется работнику Учреждения исключительно после выполнения следующих мероприятий:

- подписания работником обязательства о неразглашении персональных данных (Типовая форма соглашения о конфиденциальности работника - Приложении № 2);

- ознакомления работника под роспись с внутренними нормативными и распорядительными документами в области обработки и обеспечения безопасности персональных данных;

- прохождения работником инструктажа по правилам обработки и обеспечения безопасности персональных данных с внесением соответствующей записи в журнал инструктажей;

- выдачи работнику экземпляра Памятки о правилах обработки персональных данных (Приложение № 3).

3. Допуск к обработке персональных данных лиц, не являющихся работниками Учреждения

3.1. В случае, если допуск к обработке персональных данных необходимо предоставить лицам, не являющимся работниками Учреждения (физическим лицам, привлекаемым по договорам гражданско-правового характера, представителям контрагентов и т.п.), с таким лицом должно быть подписано соглашение о неразглашении персональных данных (Типовая форма соглашения о неразглашении персональных данных - Приложение № 4).

4. Инструктаж по правилам обработки и обеспечения безопасности персональных данных

4.1. Инструктаж и ознакомление с внутренними нормативными и распорядительными документами в области обработки и обеспечения безопасности персональных данных в данном случае проводится по усмотрению Ответственного за обеспечение безопасности персональных данных.

4.2. В Учреждении проводятся первичные и периодические инструктажи по порядку обработки и обеспечения безопасности персональных данных.

4.3. Первичный инструктаж проводится при приеме (переводе) работника на должность, предполагающую допуск к обработке персональных данных, перед началом рабочей деятельности.

4.4. Периодический инструктаж проводится согласно утвержденному плану внутренних проверок состояния обработки и обеспечения безопасности персональных данных.

4.5. Инструктаж по порядку обработки и обеспечения безопасности персональных данных включает следующие темы:

- общие требования к порядку обработки персональных данных;
- правила обработки персональных данных в информационных системах;
- правила неавтоматизированной обработки персональных данных (обработки бумажных носителей);

- правила использования средств антивирусной и парольной защиты;

- порядок действий при возникновении внештатных ситуаций;

- ответственность за нарушение правил обработки и обеспечения безопасности персональных данных.

4.6. Запись о проведенном инструктаже заносится в Журнал учёта инструктажей по безопасности (далее - Журнал).

Запись должна содержать:

- дату проведения инструктажа;
- Ф.И.О. и подпись лица, проводившего инструктаж;
- Ф.И.О. и подпись лица, прошедшего инструктаж.

5. Порядок предоставления доступа к информационным системам персональных данных (ИСПДн)

5.1. Права доступа к ИСПДн предоставляется на постоянной или временной основе.

5.2. Права доступа к ИСПДн предоставляются работнику на основании Заявки на предоставление, изменение или прекращение прав доступа к ИСПДн (далее - Заявка).

5.3. Доступ лиц к персональным данным в информационных системах персональных данных осуществляется после обязательного прохождения процедуры идентификации и аутентификации.

5.4. Процедура предоставления доступа работника к персональным данным в ИСПДн предусматривает:

- подачу непосредственным руководителем работника Заявки.
- уведомление непосредственного руководителя работника Администратором ИСПДн о результате ее исполнения;
- выдача работнику персонального идентификатора (логина) и первичного пароля. Пользователь должен сменить пароль при первом входе в ИСПДн.

5.5. Основанием для изменения прав доступа работника к ИСПДн является:

- перевод работника на должность, в рамках функционального подразделения или Учреждения, функциональные обязанности которой требуют расширения или сокращения прав доступа к персональным данным;
- изменение процесса (процессов) обработки персональных данных в Учреждении и/или требований законодательства РФ в области обработки и обеспечения безопасности персональных данных, при которых расширяются или сокращаются права доступа к персональным данным, закрепленные за определенными должностями работников;
- изменения в организационно-штатной структуре Учреждения;
- служебная необходимость, в рамках которой работнику требуется временное (разовое) расширение прав на обработку персональных данных;
- проведение в отношении работника служебного расследования, в рамках которого такому работнику необходимо ограничить права доступа к персональным данным.

5.6. Изменение прав доступа работника к персональным данным осуществляется на основании Заявки.

5.7. В случае изменений в процессе (процессах) обработки персональных данных или в организационно-штатной структуре Учреждения, соответствующие изменения должны быть внесены в документ «Перечень лиц, допущенных к обработке персональных данных в МАУ ДПО ЦРО».

5.8. Основанием для прекращения прав доступа работника к ИСПДн является:

- нарушение работником требований организационно-распорядительной документации в области обработки и обеспечения безопасности персональных данных;
- перевод работника на другую должность или в другое функциональное подразделение, не требующих участия в процессах обработки персональных данных;
- достижение заявленных целей, для которых работнику предоставлялся временный доступ к ИСПДн;
- прекращение трудовых отношений с работником.

5.9. Прекращение прав доступа работника к ИСПДн осуществляется на основании Заявки, направленной непосредственным руководителем работника.

5.10. Предоставление, изменение или прекращение прав доступа работника к персональным данным осуществляется Администратором ИСПДн на основании Заявки непосредственного руководителя данного работника.

5.11. Под Администратором ИСПДн в настоящем регламенте понимается работник Учреждения, ответственный за эксплуатацию ИСПДн, в том числе за создание (изменение, удаление) учетных записей пользователей в ИСПДн.

5.12. Заявка подготавливается в виде служебной записки (документальной или электронной) и должна содержать:

- Ф.И.О. и должность работника, которому предоставляется доступ;
- наименование информационной системы, к которой необходимо предоставить доступ;
- основания для предоставления доступа;
- необходимые права доступа в системе (роль).

5.13. Срок выполнения Заявки должен быть минимальным, но не превышать 4-х рабочих дней, с момента ее получения Администратором ИСПДн.

Администратор ИСПДн уведомляет направившего Заявку о результате ее исполнения.

6. Пересмотр регламента

6.1. Пересмотр настоящего регламента осуществляется в следующих случаях, но не реже одного раза в три года:

- при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;
- при существенном изменении процессов обработки персональных данных МАУ ДПО ЦРО.

Соглашение
о неразглашении конфиденциальной информации МАУ ДПО ЦРО

г. Петрозаводск

«___» _____ 202_ г.

Муниципальное автономное учреждение дополнительного профессионального образования Петрозаводского городского округа «Центр развития образования», именуемое в дальнейшем МАУ ДПО ЦРО, Учреждение, в лице директора Иконниковой Любови Викторовны, действующего на основании Устава, с одной стороны, и

(ФИО, должность, подразделение)
зарегистрированный по адресу: _____,
паспорт РФ: серия _____ № _____, выдан «___» _____ 20__ г.

именуемый в дальнейшем «Работник», с другой стороны, совместно именуемые в дальнейшем «Стороны», заключили настоящее соглашение о нижеследующем.

1. Предмет соглашения

1. Работник, в связи с исполнением своих должностных обязанностей, получает доступ к персональным данным сотрудников, слушателей курсов повышения квалификации, граждан, проходящих обследование ТПМПК, МАУ ДПО ЦРО, иных лиц, участвующих в мероприятиях, организованных Учреждением, а также к сведениям, содержащим иную конфиденциальную информацию, доступ к которым ограничен Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне» и иными правовыми актами, и **обязуется не разглашать ставшие ему известными персональные данные сотрудников слушателей курсов повышения квалификации, граждан, проходящих обследование ТПМПК, МАУ ДПО ЦРО, иных лиц, участвующих в мероприятиях, организованных Учреждением, иные сведения, содержащие конфиденциальную информацию, за исключением случаев предусмотренных законодательством Российской Федерации.**

2. Под конфиденциальной информацией в настоящем соглашении понимается речевая, аудиовизуальная, документированная информация с ограниченным доступом и иная информация, содержащая охраняемую в соответствии с действующим законодательством тайну Учреждения, а также персональные данные сотрудников, слушателей курсов повышения квалификации Учреждения, иных лиц, участвующих в мероприятиях, организованных Учреждением. Конфиденциальная информация, содержащаяся в локальной сети Учреждения, также имеет ограниченный доступ.

К конфиденциальной информации по настоящему соглашению в частности, но не ограничиваясь, относится любая или вся, настоящая или будущая, техническая, финансовая, деловая информация, статистика, данные, схемы, планы, спецификации, документы, идеи, концепции, продукты, процессы, технологии, цены, пароли доступа к информационным системам и другая информация, которая отнесена к конфиденциальной действующим законодательством Российской Федерации и локальными правовыми актами Учреждения и была передана Работнику для выполнения последним своих трудовых обязанностей.

3. Не могут являться конфиденциальной информацией сведения:

- которые до момента заключения настоящего соглашения были публично обнародованы;
- которые стали общедоступны во время действия настоящего соглашения, но без виновного участия Работника.

4. Вся конфиденциальная информация, полученная Работником в материальной (схемы, рисунки, письма, фотографии и пр.) и нематериальной формах, является собственностью Учреждения и используется только на условиях настоящего соглашения.

2. Работник обязуется:

2.1. Знать требования Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Положения о персональных данных МАУ ДПО ЦРО, Положения о конфиденциальной информации и коммерческой тайне МАУ ДПО ЦРО.

2.2. Не разглашать и не передавать третьим лицам сведения, являющиеся конфиденциальной информацией, ставшие ему известными в связи с исполнением трудовых обязанностей, а также защищать вышеуказанные сведения от посягательств и попыток ее обнародовать третьими лицами.

2.3. Использовать сведения, полученные при исполнении своих трудовых обязанностей, лишь в интересах Учреждения.

2.4. В случае увольнения из МАУ ДПО ЦРО вернуть все сведения, полученные на материальных носителях, а также их копии, в течение одного дня с момента получения соответствующего требования о возврате.

2.5. Не использовать конфиденциальную информацию после увольнения из Учреждения.

3. Ответственность

3.1. В случае разглашения Работником сведений, являющихся конфиденциальной информацией, трудовой договор с Работником подлежит расторжению в соответствии с подпунктом «в» пункта 6 статьи 81 Трудового кодекса Российской Федерации.

3.2. В случае разглашения сведений, являющихся конфиденциальной информацией, Работник обязан в полном объеме возместить понесенные в результате такого разглашения Учреждением убытки.

3.3. В случае разглашения конфиденциальной информации Работник может быть привлечен к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

4. Срок действия соглашения

Настоящее Соглашение действует бессрочно. Прекращение отношений по трудовому договору не является основанием для прекращения обязательств Сторон по настоящему соглашению.

5. Заключительные положения

Настоящее Соглашение составлено на двух страницах, на одном листе, в двух экземплярах, каждый из которых имеет одинаковую юридическую силу, по одному для каждой Стороны.

Директор МАУ ДПО ЦРО
_____ Л.В. Иконникова

Работник
_____ / _____

М.П.

**Обязательство
о неразглашении информации, содержащей персональные данные**

г. Петрозаводск

« ___ » _____ 202__ г.

Я, _____,
(Ф.И.О.)

(должность)

предупрежден(а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом (должностной инструкцией) мне будет предоставлен допуск к информации, содержащей персональные данные субъектов персональных данных. Настоящим добровольно принимаю на себя обязательства:

1. Не осуществлять незаконную передачу персональных данных и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц незаконно получить от меня информацию, содержащую персональные данные, сообщать об этом непосредственному руководителю.

3. Выполнять требования, установленные Федеральным законом "О персональных данных", принятыми в соответствии с ним иными нормативными правовыми актами и локальными нормативными актами МАУ ДПО ЦРО в области защиты персональных данных.

4. Не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные, в том числе и после прекращения права на допуск к информации, содержащей персональные данные.

Я предупрежден(а) о том, что в случае нарушения данного обязательства, а также положений, предусмотренных нормами Трудового [Кодекса](#) Российской Федерации, Федерального [закона](#) "О персональных данных", буду привлечен(а) к дисциплинарной и/или иной юридической ответственности в соответствии с законодательством Российской Федерации.

« ___ » _____ 202__ г.

(подпись)

(расшифровка подписи)

ПАМЯТКА **о правилах обработки персональных данных в МАУ ДПО ЦРО**

Согласно ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных, за исключением случаев, предусмотренных настоящим Федеральным законом.

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в [пунктах 2 - 11 части 1 статьи 6](#), [части 2 статьи 10](#) и [части 2 статьи 11](#) Федерального закона, возлагается на оператора.

В случаях, предусмотренных Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом электронной подписью.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

- 1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- 2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- 3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- 4) цель обработки персональных данных;

- 5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- 6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- 7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- 8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- 9) подпись субъекта персональных данных.

Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

Приложение № 4

к регламенту предоставления доступа
к персональным данным

от «__» _____ 202__ г.

**Перечень должностей работников, допущенных к работе с персональными данными
(Перечень должностей МАУ ДПО ЦРО)**

№ п/п	Вид персональных данных	Должность	Цель доступа	Права доступа ¹	Срок доступа
1	Общие, специальные	Руководитель, заместитель руководителя, специалист по кадрам Начальник отдела	Обеспечение уставной деятельности	Персональные данные всех работников, персональные данные родственников работника персональные данные физических лиц, претендующих на замещение вакантных должностей Персональные данные третьих лиц по договорам	На период исполнения должностных обязанностей
2	Общие	Начальники отделов	Обеспечение уставной деятельности	Персональные данные работников отдела, персональные данные третьих лиц по договорам персональные данные физических лиц, обрабатываемые в рамках мероприятий, проводимых Отделом	На период исполнения должностных обязанностей
3	Общие	Ведущий специалист, специалист, старший методист, методист, специалист по кадрам	Для выполнения должностных обязанностей	Персональные данные физических лиц, обрабатываемые в рамках мероприятий, проводимых Отделами Персональные данные третьих лиц, на которых оформлены заявления (согласия, доверенности и т.п.), в том числе участников мероприятий	На период исполнения должностных обязанностей

¹ Доступ предоставляется после подписания Обязательства о неразглашении персональных данных в соответствии с приложением к Перечню должностей

№ п/п	Вид персональных данных	Должность	Цель доступа	Права доступа¹	Срок доступа
4	Общие	Вахтер	Для обеспечения пропускного режима	Персональные данные посетителей	На период исполнения должностных обязанностей
5	Общие, специальные	Руководитель ПМПК, психологи, логопеды, дефектологи	Для выполнения должностных обязанностей, подготовка заключения комиссии	Персональные данные третьих лиц, на которых оформлены заявления (согласия, доверенности и т.п.), обрабатываемые в рамках работа ТПМПК	На период исполнения должностных обязанностей
6	Общие	Начальник отдела, ведущий специалист, специалист, тьютор, техник-программист	Для выполнения должностных обязанностей	Персональные данные слушателей курсов повышения квалификации	На период исполнения должностных обязанностей
7	Общие	Заместитель директора, техник-программист, ведущий специалист, специалист	Для осуществления функций в части обеспечения безопасности персональных данных	Персональные данные всех работников, персональные данные при обработке, функционирование в ИСПДн для подключения к ЗСПД	На период исполнения должностных обязанностей