

**ПОЛИТИКА**  
**в отношении обработки и защиты персональных данных**  
**в ПАО «Среднеуральский медеплавильный завод»**

## 1 Общие положения

1.1 Настоящие положение регламентирует основные обязательства ПАО «СУМЗ» (далее – предприятие или оператор) в области обработки и защиты персональных данных – политику обработки и защиты персональных данных (далее – Политика) и определяет цели, задачи и основные мероприятия по обеспечению безопасности персональных данных от несанкционированного доступа, неправомерного их использования или утраты.

1.2 Положение разработано в соответствии с законодательными и иными нормативными правовыми актами Российской Федерации (РФ):

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждено постановлением Правительства РФ от 15.09.2008 № 687);

- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства РФ от 01.11.2012 № 1119).

1.3 Требования настоящего положения являются основой для разработки локальных нормативных актов предприятия по обеспечению безопасности персональных данных.

1.4 Требования распространяются на работников предприятия, включая работников, работающих по договору подряда, на работников сторонних организаций, взаимодействующих с предприятием на основании соответствующих нормативных правовых и организационно-распорядительных документов, а также на физических лиц, находящихся в гражданско-правовых отношениях с предприятием.

## 2 Термины и принятые сокращения

2.1 **персональные данные, ПДн:** Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту ПДн).

2.2 **обработка ПДн:** Любое действие/операция или совокупность действий/операций, совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

2.3 **автоматизированная обработка ПДн:** Обработка ПДн с помощью средств вычислительной техники.

2.4 **информационная система персональных данных, ИСПДн:** Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**2.5 ПДн, сделанные общедоступными субъектом ПДн:** ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн либо по его просьбе.

**2.6 блокирование ПДн:** Временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

**2.7 уничтожение ПДн:** Действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

### **3 Обработка персональных данных**

#### **3.1 Получение ПДн:**

**3.1.1** Все ПДн следует получать от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

**3.1.2** Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

**3.1.3** Документы, содержащие ПДн, создают путем:

- копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);
- внесения сведений в учетные формы;
- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

#### **3.2 Обработка ПДн:**

**3.2.1** Обработку ПДн осуществляют:

- с согласия субъекта ПДн на обработку его ПДн;
- в случаях, когда обработка ПДн необходима для выполнения возложенных законодательством РФ функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка ПДн, сделанных общедоступными субъектом ПДн.

**3.2.2** Цели обработки ПДн:

- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений;
- обеспечение пропускного и внутриобъектового режимов, установленных на предприятии;
- оказание услуг гражданам РФ;
- оказание медицинских и медико-социальных услуг.

**3.2.3** Категории субъектов ПДн:

- физические лица, состоящие/состоявшие в трудовых взаимоотношениях с предприятием и/или работающие (работавшие) по договорам гражданско-правового характера;
- близкие родственники лиц, состоящих/состоявших в трудовых взаимоотношениях с предприятием и/или работающих/работавших по договорам гражданско-правового характера;

- физические лица – претенденты на замещение вакантной должности;
- физические лица – практиканты/стажеры;
- физические лица, являющиеся контрагентами (возможными контрагентами) предприятия, индивидуальные предприниматели, а также физические лица – работники организаций, оказывающих предприятию услуги или выполняющие работу;

- физические лица – являющиеся пациентами предприятия.

#### 3.2.4 Обработку ПДн ведут:

- с использованием средств автоматизации с передачей по внутренней сети предприятия, имеющей выход в сеть международного информационного обмена Интернет. Используемые линии связи могут иметь выход за пределы контролируемой зоны предприятия;

- без использования средств автоматизации.

### 3.3 Хранение ПДн:

3.3.1 ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

3.3.2 ПДн, зафиксированные на бумажных носителях, хранят в запираемых шкафах или в специально выделенных помещениях для хранения ПДн.

3.3.3 ПДн субъектов, обрабатываемые с использованием средств автоматизации, в разных целях хранят в разных папках (вкладках).

3.3.4 Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках).

3.3.5 Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляют не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении целей.

### 3.4 Уничтожение ПДн.

3.4.1 Уничтожение документов (носителей), содержащих ПДн, производят путем сожжения, дробления (измельчения). Для уничтожения бумажных документов допускается применение shreddera.

3.4.2 ПДн на электронных носителях уничтожают путем стирания или форматирования носителя.

3.4.3 Уничтожение производит комиссия. Факт уничтожения ПДн подтверждают актом об уничтожении, подписанным членами комиссии.

### 3.5 Передача ПДн:

3.5.1 Предприятие поручает обработку ПДн третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;

- передача предусмотрена законодательством РФ или иным применимым законодательством в рамках установленной законодательством РФ процедуры.

3.5.2 Перечень третьих лиц, которым передают ПДн, указан в согласии на обработку ПДн, подписанном субъектом ПДн.

## **4 Защита персональных данных**

4.1 В соответствии с требованиями нормативных документов на предприятии должна быть создана система защиты персональных данных (СЗПДн), включающая в себя следующие подсистемы:

- правовая;
- организационная;
- техническая.

4.2 Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПДн.

4.3 Подсистема организационной защиты включает в себя организацию структуры управления СЗПДн, разрешительной системы, защиты информации при работе с работниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

4.4 Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

4.5 Основные меры защиты ПДн, применимые предприятием:

4.5.1 Назначение администратора информационной безопасности, который осуществляет организацию защиты ПДн, обучение и инструктаж, внутренний контроль за соблюдением предприятием и его работниками требований по защите ПДн.

4.5.2 В случае необходимости могут быть дополнительно назначены администраторы информационной безопасности отдельных ИСПДн.

4.5.3 Определение актуальных угроз безопасности ПДн при их обработке в ИСПДн и разработка мер и мероприятий по защите ПДн.

4.5.4 Разработка локальных нормативных актов, регламентирующих обработку и обеспечение безопасности ПДн.

4.5.5 Установление правил доступа к ПДн, обрабатываемых в ИСПДн, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн в ИСПДн.

4.5.6 Установление индивидуальных паролей доступа работников в ИСПДн в соответствии с их должностными обязанностями.

4.5.7 Применение средств защиты информации и средств криптографической защиты информации, прошедших в установленном порядке процедуру оценки соответствия.

4.5.8 Регулярное обновление применяемых средств защиты информации, средств криптографической защиты информации, а также системного и прикладного ПО.

4.5.9 Соблюдение условий, обеспечивающих сохранность ПДн, и исключаящих несанкционированный к ним доступ.

4.5.10 Выявление фактов несанкционированного доступа к ПДн и принятия соответствующих мер.

4.5.11 Принятие мер по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.5.12 Обучение работников предприятия, непосредственно осуществляющих обработку ПДн, в рамках требований законодательства РФ в части защиты ПДн, в том числе применения документов, определяющим политику предприятия в отношении обработки ПДн, локальным нормативным актам по вопросам обработки ПДн.

4.5.13 Осуществление внутреннего контроля и аудита.

## **5 Основные права субъекта ПДн и обязанности оператора**

### **5.1 Основные права субъекта ПДн:**

5.1.1 Субъект ПДн имеет право требовать от оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.1.2 Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые оператором способы обработки ПДн;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании законодательства РФ;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством РФ;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных законодательством РФ;
- информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом ФЗ № 152-ФЗ «О персональных данных» или другими федеральными законами.

5.1.3 Субъект ПДн имеет право обжаловать действия или бездействия оператора.

5.1.4 Субъект ПДн имеет право обращаться к оператору и направлять ему запросы.

### **5.2 Обязанности Оператора**

Оператор обязан:

- при сборе ПДн предоставить субъекту ПДн по его просьбе информацию о имеющихся ПДн;

- в случаях, если ПДн были получены не от субъекта ПДн, уведомить субъекта ПДн;

- в случае отказа субъекта ПДн в предоставлении ПДн, разъяснить субъекту юридические последствия такого отказа;

- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;

- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

- давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.

## **6 Ответственность**

6.1 Администратор информационной безопасности несет ответственность за эффективность мер по защите ПДн и контроль установленных мер.

6.2 Руководители подразделений несут ответственность за исполнение требований настоящего положения и реализацию обязательств политики обработки и защиты персональных данных в подчиненных подразделениях.

6.3 Работники предприятия, виновные в нарушении порядка обращения с ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.