1. **Назначение и область действия документа**

1.1 Политика ФГУП «Завод имени Морозова» (далее – Предприятие) в отношении обработки персональных данных (далее – Политика) определяет позицию и намерения Предприятия в области обработки и реализации требований к защите персональных данных лиц, состоящих в договорных, гражданско-правовых и иных отношениях с Предприятием, соблюдения действующего законодательства Российской Федерации в области информационной безопасности, а так же требований Федерального закона от 27.06.2006 года №152-ФЗ «О персональных данных», основной целью которого является обеспечение 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.

1.2 Политика предназначена для изучения и неукоснительного исполнения всеми работниками Предприятия, а также подлежит доведению до сведения лиц, состоящих в договорных, гражданско-правовых и иных отношениях с Предприятием (далее – граждане), партнеров и других заинтересованных сторон.

1. **Термины и определения**

***Персональные данные*** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

***Обработка персональных данных*** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

***Автоматизированная обработка персональных данных*** - обработка персональных данных с помощью средств вычислительной техники;

***Оператор*** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

***Распространение персональных данных*** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

***Трансграничная передача персональных данных*** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1. **Общие положения**

3.1 Понимая важность и ценность информации о Субъекте персональных данных, Предприятие, являясь Оператором персональных данных, обеспечивает надежную защиту предоставленных ему персональных данных. Предприятие обрабатывает персональные данные только тех лиц, которые состоят в договорных, гражданско-правовых и иных отношениях с Предприятием, а именно:

* лиц, состоящих в трудовых отношениях с Предприятием (работники Предприятия);
* лиц, являющихся соискателями должностей на Предприятии.

Обработка персональных данных работников Предприятия осуществляется в строгом соответствии с трудовым законодательством РФ. Предприятие не осуществляет распространение или раскрытие персональных данных без согласия гражданина, если иное не предусмотрено федеральным законом.

3.2 Правовым основанием обработки персональных данных является осуществление возложенных на Предприятие законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, Федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» № 27-ФЗ от 01.04.1996 г., «О персональных данных» № 152-ФЗ от 27.07.2006 г., «Об электронной подписи» № 63-ФЗ от 06.04.2011 г., а также в целях организации учета работников Предприятия для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами.

3.3 При обработке персональных данных Предприятие придерживается следующих принципов:

* Предприятие осуществляет обработку персональных данных только на законной основе;
* обработка персональных данных Предприятием ограничивается достижением конкретных, заранее определенных и законных целей;
* Предприятие не допускает объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
* до начала сбора/получения персональных данных, Предприятие определяет конкретные законные цели обработки персональных данных;
* Предприятие собирает только те персональные данные, которые являются необходимыми и достаточными для заявленной цели обработки;
* Предприятие систематически принимает меры по удалению или уточнению неполных или неточных данных;
* Предприятие уничтожает либо обезличивает персональные данные по достижении целей обработки или в случае утраты необходимости в достижении целей, если иное не предусмотрено соглашением между Предприятием и субъектом персональных данных либо если Предприятие не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими Федеральными законами;
* Предприятие не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта (если иное не предусмотрено действующим законодательством Российской Федерации);
* Предприятие не осуществляет сбор и обработку персональных данных граждан, касающихся расовой, национальной принадлежности, политических, религиозных, философских и иных убеждений, интимной жизни, членства в общественных объединениях, в том числе в профессиональных союзах.

3.4 В случае осуществления Предприятием трансграничной передачи персональных данных граждан на территорию иностранного государства, указанная трансграничная передача должна осуществляться с соблюдением требований действующего законодательства Российской Федерации, а также иных международно-правовых актов. При этом получающей стороной могут быть страны, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иные иностранные государства при условии обеспечения адекватных защитных мер прав субъектов персональных данных.

1. **Права субъектов персональных данных**

4.1 Субъект персональных данных, персональные данные которого обрабатываются Предприятием, имеет право:

* требовать от Предприятия уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
* отозвать свое согласие на обработку персональных данных;
* требовать устранения неправомерных действий Предприятия в отношении его персональных данных;
* обжаловать действия (бездействие) Предприятия в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) или в судебном порядке в случае, если гражданин считает, что Предприятие осуществляет обработку его персональных данных с нарушением требований Закона «О персональных данных» или иным образом нарушает его права и свободы;
* на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4.2 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

* подтверждение факта обработки персональных данных Предприятием;
* правовые основания и цели обработки персональных данных;
* сведения о применяемых на Предприятии способах обработки персональных данных;
* наименование и место нахождения Предприятия;
* сведения о лицах (за исключением работников Предприятия), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Предприятием или на основании Федерального закона;
* перечень обрабатываемых персональных данных, относящихся к субъекту персональных данных, от которого поступил запрос и источник их получения, если иной порядок предоставления таких данных не предусмотрен Федеральным законом;
* сроки обработки персональных данных, в том числе сроки их хранения;
* порядок осуществления гражданином прав, предусмотренных Федеральным законом «О персональных данных» №152-ФЗ от 27.06.2006 г.;
* информацию об осуществляемой или о предполагаемой трансграничной передаче персональных данных.
1. **Сведения о реализуемых требованиях к защите персональных данных**

5.1 Предприятие при обработке персональных данных принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

К таким мерам относятся:

* назначение лица, ответственного за организацию обработки персональных данных, и лиц, ответственных за обеспечение безопасности персональных данных;
* определение угроз безопасности персональных данных при их обработке;
* разработка и утверждение локальных актов по вопросам обработки и защиты персональных данных;
* оценка вреда, который может быть причинен гражданам в случае нарушения Федерального закона «О персональных данных» №152-ФЗ от 27.06.2006 г., соотношение указанного вреда и принимаемых Предприятием мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» №152-ФЗ от 27.06.2006 г.;
* ознакомление работников Предприятия, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами по вопросам обработки и защиты персональных данных, и обучение работников Предприятия;
* соблюдение условий, исключающих несанкционированный доступ к материальным носителям персональных данных и к средствам защиты персональных данных;
* применение технических мер защиты, включая:
	+ средства идентификации и аутентификации субъектов доступа и объектов доступа;
	+ средства разграничения доступа на сетевом, прикладном и общесистемном уровнях;
	+ средства межсетевого экранирования;
	+ средства регистрации и учета действий пользователей на сетевом, прикладном и общесистемном уровнях;
	+ антивирусные средства защиты;
	+ сертифицированные средства криптографической защиты информации;
	+ средства обнаружения и предотвращения вторжений;
	+ средства обеспечения целостности информационных систем и персональных данных;
	+ средства обеспечения доступности персональных данных;
	+ средства анализа защищенности;
	+ средства выявления инцидентов и реагирование на них;
	+ средства контроля физического доступа в помещения, в которых осуществляется обработка персональных данных.
* оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию новой информационной системы Предприятия;
* обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
* восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
* установление правил доступа к персональным данным, обрабатываемым в информационных системах Предприятия, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными;
* осуществление внутреннего контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации.
1. **Лица ответственные за организацию обработки персональных данных**

6.1 На Предприятии создано подразделение, ответственное за организацию обработки персональных данных (бюро по ПД ИТР) и выполняющее следующие функции:

* осуществление внутреннего контроля за соблюдением Предприятием и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
* доведение до сведения работников Предприятия положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, внутренних требований к защите персональных данных;
* организация приема и обработки обращений и запросов субъектов персональных данных или их представителей.