Утверждена

приказом управляющего ОСФР по Костромской области от «\_07\_» \_\_03\_\_ 2023 г. № \_125\_

[**ПОЛИТИКА ОТДЕЛЕНИЯ ФОНДА ПЕНСИОННОГО И СОЦИАЛЬНОГО СТРАХОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО КОСТРОМСКОЙ ОБЛАСТИ В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И РЕАЛИЗАЦИИ ТРЕБОВАНИЙ К ИХ ЗАЩИТЕ**](https://sfr.gov.ru/about/polpfr_persdan/~4642)

г. Кострома, 2023 г**.**

1. **Общие положения**

Настоящий документ определяет цели обработки персональных данных Отделением Фонда пенсионного и социального страхования Российской Федерации по Костромской области (далее - ОСФР), принципы их обработки, а также содержит сведения о передаче персональных данных взаимодействующим организациям и о реализуемых требованиях к защите персональных данных.

Правила, порядок, процедуры и практические приемы обработки и защиты персональных данных определяются системой законодательных актов Российской Федерации, нормативных правовых актов СФР, распорядительных актов ОСФР.

1. **Цели обработки персональных данных**

2.1. Обработка персональных данных осуществляется ОСФР в следующих целях:

- индивидуальный (персонифицированный) учет застрахованных лиц в системе обязательного пенсионного страхования;

- пенсионное обеспечение граждан;

- ведение федеральных регистров лиц, имеющих право на дополнительные меры государственной поддержки и государственной социальной помощи;

- администрирование страховых взносов в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования;

- обеспечение прав и льгот Героев Советского Союза, Героев Социалистического Труда, Героев Российской Федерации, полных кавалеров ордена Славы, полных кавалеров ордена Трудовой Славы и членов их семей;

- обеспечение социальной защиты ветеранов и инвалидов Великой Отечественной войны и ветеранов и инвалидов боевых действий;

- рассмотрение обращений граждан;

- регулирование трудовых отношений и иных непосредственно связанных с ними отношений с работниками ОСФР;

- выполнение других задач, возлагаемых на ОСФР законодательством Российской Федерации.

1. **Перечень действий с персональными данными**
	1. ОСФР осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных. Обработка персональных данных осуществляется как с использованием, так и без использования средств автоматизации.
	2. Хранение персональных данных осуществляется в течение срока, определенного законодательством Российской Федерации.
2. **Принципы обработки персональных данных**
	1. Обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации и ограничивается достижением конкретных целей, определенных законодательством Российской Федерации в сфере обработки персональных данных.
	2. Обработке подлежат персональные данные, которые отвечают целям их обработки.
	3. Не допускается избыточность обработки персональных данных.

4.4 При обработке персональных данных обеспечивается точность персональных данных, их достаточность и актуальность по отношению к целям обработки.

1. **Источники персональных данных**

5.1. Персональные данные предоставляются в ОСФР в соответствии с законодательством Российской Федерации:

- субъектами персональных данных или их представителями;

- страхователями (плательщиками страховых взносов) или их представителями;

- взаимодействующими с ОСФР органами исполнительной власти, кредитными организациями, негосударственными пенсионными фондами, управляющими компаниями, внебюджетными фондами, иностранными компетентными органами в рамках реализации международных договоров (соглашений) Российской Федерации и другими органами и организациями в целях обеспечения пенсионных прав граждан;

- судебными органами.

1. **Передача персональных данных**
	1. Предоставление обрабатываемых персональных данных производится в соответствии с законодательством Российской Федерации органам исполнительной власти, кредитным организациям, негосударственным пенсионным фондам, управляющим компаниям, внебюджетным фондам, иностранным компетентным органам в рамках реализации международных договоров (соглашений) Российской Федерации, судебным органам и другим взаимодействующим организациям.
	2. Распространение персональных данных работников ОСФР производится с их согласия, персональных данных остальных категорий субъектов персональных данных - в соответствии с требованиями законодательства Российской Федерации и международных договоров (соглашений) Российской Федерации.
2. **Реализуемые требования к защите персональных данных**

7.1. Реализация требований к защите персональных данных от неправомерного или случайного доступа к персональным данным, их уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с персональными данными в ОСФР осуществляется правовыми, организационными и техническими (программно- и аппаратно- реализуемыми) мерами.

7.1.1. Правовые меры:

- заключение соглашений об информационном обмене с взаимодействующими организациями и включение в них требований об обеспечении конфиденциальности предоставляемых персональных данных;

- издание актов ОСФР, рекомендаций и инструкций по вопросам обработки персональных данных, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

7.1.2. Организационные меры:

- документальное оформление требований к безопасности обрабатываемых данных;

- назначение лица, ответственного за организацию обработки персональных данных;

- издание системы нормативных (руководящих) документов по организации защиты данных;

- распределение ответственности по вопросам защиты данных между должностными лицами и работниками ОСФР;

- установление персональной ответственности работников ОСФР за обеспечение безопасности обрабатываемых данных;

- контроль выполнения подразделениями, должностными лицами и работниками органов ОСФР требований нормативных документов по защите данных;

- своевременное выявление угроз безопасности данных и принятие соответствующих мер защиты;

- регламентирование порядка применения средств ввода-вывода данных и контроль его выполнения;

- содержание штата специалистов по защите информации, организация системы их профессиональной подготовки и повседневной деятельности;

- придание мероприятиям защиты информации характера обязательных элементов производственного процесса ОСФР, а требованиям по их исполнению - элементов производственной дисциплины;

- доведение до работников ОСФР требований по защите данных и обучение их правилам работы в АИС.

7.1.3. Технические (программно- и аппаратно- реализуемые) меры:

- резервное копирование информационных ресурсов;

- применение прикладных программных продуктов, отвечающих требованиям защиты данных;

- организация контроля доступа в помещения и здания ОСФР, их охрана в нерабочее время;

- систематический анализ безопасности данных и совершенствование системы их защиты;

- применение технических средств защиты, сертифицированных компетентными государственными органами (организациями) на соответствие требованиям безопасности;

- своевременное применение критических обновлений общесистемного и прикладного программного обеспечения;

- оптимальная настройка операционной системы и прикладного программного обеспечения вычислительных средств, применяемых для обработки данных;

- использование корпоративной информационно-телекоммуникационной сети для обеспечения информационного взаимодействия с центральным аппаратом и другими территориальными органами СФР;

- шифрование данных при передаче и хранении (криптографическая защита);

- использование электронной подписи;

- применение межсетевых защитных (фильтрующих) экранов;

- антивирусный мониторинг и детектирование;

- мониторинг процессов и действий пользователей наиболее важных аппаратных и информационных ресурсов;

- оборудование зданий и помещений системами безопасности (пожарной и охранной сигнализации, пожаротушения, телевизионного наблюдения, СКУД и т.п.);

- хранение парольной и ключевой информации на индивидуальных электронных ключах;

- применение средств обнаружения и предотвращения компьютерных атак;

- применение в архитектуре вычислительных систем технологий и средств повышения надежности их функционирования и обеспечения безопасности информации;

- применение средств технической укреплённости зданий и помещений.

Начальник отдела по защите информации А.Н. Комаров