Приложение № 1
к приказу ОСФР Республике Калмыкия
от «5» 11 2025 г. № 320

ПОЛИТИКА
обработки персональных данных в ОСФР по Республике Калмыкия

Настоящий документ определяет цели обработки персональных данных Отделением Фонда пенсионного и социального страхования Российской Федерации по Республике Калмыкия (далее – Отделение), выполняющим обработку персональных данных, 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 Фонда пенсионного и социального страхования Российской Федерации (далее – СФР), распорядительных актов Отделения.

1. Цели обработки персональных данных

Обработка персональных данных осуществляется в следующих целях:

1) Ведение кадрового и бухгалтерского учета.

2) Обеспечение соблюдения пенсионного законодательства Российской Федерации.

3) Обеспечение соблюдения законодательства о государственной социальной помощи Российской Федерации.

4) Обеспечение пропускного режима на территорию оператора.

2. Перечень действий с персональными данными

Отделение осуществляет обработку персональных данных: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступа), блокирование, удаление и уничтожение персональных данных. Обработка персональных данных осуществляется как с использованием, так и без использования средств автоматизации.

Хранение персональных данных осуществляется в течение срока, определенного законодательством Российской Федерации.

3. Принципы обработки персональных данных

Обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации и ограничивается достижением указанных в п. 1 Политики конкретных целей, определенных законодательством Российской Федерации в сфере обработки персональных данных.

Обработке подлежат персональные данные, которые отвечают целям их обработки.

Не допускается избыточность обработки персональных данных.

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

4. Источники персональных данных

Отделению персональные данные предоставляются в соответствии с законодательством Российской Федерации:

- субъектами персональных данных или их представителями;
- страхователями (плательщиками страховых взносов) или их представителями;
- взаимодействующими с СФР 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 и социальных прав граждан;
- судебными органами.

5. Передача персональных данных

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 с СФР организациям.

Отделение не осуществляет трансграничную передачу персональных данных субъектов.

Распространение персональных данных работников Отделения производится с их согласия, персональных данных остальных категорий субъектов персональных данных – в соответствии с требованиями законодательства Российской Федерации.

6. Реализуемые требования к защите персональных данных

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, осуществляется правовыми, организационными и техническими (программно и аппаратно реализуемыми) мерами.

6.1. Правовые меры:

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

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

6.2. Организационные меры:

- документальное оформление требований к безопасности обрабатываемых данных;

- назначение лица, ответственного за организацию обработки персональных данных;

- издание системы руководящих документов по организации защиты данных;

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

- установление персональной ответственности работников за обеспечение безопасности обрабатываемых данных;

- контроль выполнения подразделениями, должностными лицами и работниками Отделения 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, а требованиям по их исполнению - элементов производственной дисциплины;

- доведение до работников Отделения требований по защите данных и обучение их правилам работы в информационных системах.

6.3. 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 Отделения, 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 информации;

- 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 подразделений Отделения;

- 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 видео-наблюдения 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 укрепленности зданий и помещений;

- противопожарная защита зданий и помещений.