УТВЕРЖДЕНО
Председателем Совета
ПК «Коллективный Резерв»
Приказ № 1/2026

ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (152-ФЗ) И РЕГЛАМЕНТ ИБ

Потребительского Кооператива «Коллективный Резерв» (с Пояснительной запиской)

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К ПОЛИТИКЕ ПДН И РЕГЛАМЕНТУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Правовое назначение и нормативная база. Настоящий документ объединяет публичную Политику обработки персональных данных (во исполнение ч. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных») и Технический регламент защиты информации в АСКС (во исполнение ст. 19 ФЗ № 152-ФЗ и Постановления Правительства РФ № 1119).

1.2. Какие регуляторные и технические риски закрывает документ:

• **Полная защита при проверках Роскомнадзора (152-ФЗ):** Документ фиксирует, что персональные данные граждан РФ обрабатываются исключительно для исполнения уставных обязательств по Закону РФ № 3085-1 (ведение реестра пайщиков ст. 12, оформление членской книжки, возврат паевых взносов), локализованы на сервере на территории РФ, а сторонние зарубежные CDN и шрифты полностью отключены (`css/vendor/`, `js/vendor/`).

• **Исключение утечки ПДн при компрометации дампа базы данных:** В БД отсутствуют открытые текстовые поля с паспортом, ИНН, датой рождения, адресами или банковскими счетами. Все указанные атрибуты хранятся исключительно в зашифрованном виде (`AES-256-GCM`, `CryptoService`) с версионированием ключей (`pd_key_version`), а поиск дубликатов ИНН ведётся по слепому индексу `inn_hash` (`HMAC-SHA256`).

• **Персональная ответственность должностных лиц при просмотре ПДн:** Каждое обращение члена Совета, Ревизора или бухгалтера к анкете кандидата, реквизитам возврата пая или акту восстановления доступа автоматически записывается в неизменяемый журнал `document_access_log`.

• **Защита межкооперативного обмена («Союз-Шлюз»):** При обмене данными между кооперативами по ст. 31 Закона № 3085-1 действует принцип **Zero-PII** (передаются только агрегированные обезличенные количества без ФИО и телефонов пайщиков).

1.3. Связь с программными модулями АСКС. Исполнение норм обеспечивается сервисами `CryptoService`, `PersonalDataService`, `FileStorage`, `LedgerAuditService`, `Csp`, `RateLimiter`, `Session`, а также конфигурацией веб-сервера `deploy/nginx/security.conf`.

2. ЦЕЛИ, ПРАВОВЫЕ ОСНОВАНИЯ И ОБЪЁМ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Оператором персональных данных является Потребительский Кооператив. Обработка персональных данных осуществляется на основании:

1. Согласия субъекта персональных данных, подписанного простой электронной подписью в составе единого пакета вступления (`ВС`, `admission_bundle`) либо пакета подтверждения пая (`ПП`,

genesis_rebind_confirm_bundle);

2. Закона РФ от 19.06.1992 № 3085-1 (ст. 10 - рассмотрение заявления о приёме; ст. 12 - обязательное ведение реестра членов кооператива и членской книжки; ст. 14 - расчёты при выходе).

2.2. Кооператив обрабатывает исключительно минимально необходимый перечень данных: фамилия, имя, отчество; дата рождения (dob_enc); серия и номер паспорта, дата и орган выдачи (passport_enc); ИНН (inn_enc + слепой индекс inn_hash); адрес регистрации и адрес доставки (registration_address_enc, delivery_address_enc); абонентский номер телефона; идентификатор аккаунта Telegram (telegram_chat_id); банковские реквизиты для выплаты возврата пая (в зашифрованном поле таблицы share_refunds). Специальные категории ПДн и биометрические ПДн Кооперативом не собираются и не обрабатываются.

3. ПОЛЕВОЕ ШИФРОВАНИЕ (AES-256-GCM) И КРИПТОГРАФИЧЕСКОЕ ХРАНЕНИЕ

3.1. Все чувствительные персональные данные пайщиков, кандидатов и их доверенных лиц (user_proxies) перед записью в СУБД MySQL проходят обязательное симметричное аутентифицированное шифрование в режиме **AES-256-GCM** (PersonalDataService, CryptoService):

• для каждого поля генерируется уникальный криптографически стойкий 96-битный вектор инициализации (IV);

• целостность шифротекста контролируется 128-битным тегом аутентификации GCM;

• мастер-ключ шифрования и секретный ключ хеширования (PD_PEPPER_KEY) хранятся в защищённом окружении .env вне дерева веб-доступа с поддержкой бесшовной ротации ключей через атрибут pd_key_version.

3.2. Учётные пароли пользователей хранятся в виде необратимых криптографических хэшей Argon2id / bcrypt. В системных логах (Logger) реализовано автоматическое маскирование любых полей, содержащих пароли, одноразовые коды, паспортные данные, ИНН и токены.

4. ИЗОЛЯЦИЯ ФАЙЛОВОГО ХРАНИЛИЩА, КОНТРОЛЬ ДОСТУПА (RBAC) И ЖУРНАЛИРОВАНИЕ

4.1. Все первичные файлы и сканы документов, содержащие персональные данные (акты выдачи представителю АД, заявления о восстановлении доступа, сметы и оправдательные документы фондов), сохраняются сервисом FileStorage со случайными криптографическими именами и проверкой MIME-типа (finfo) в защищённом каталоге /var/www/coop-storage/, расположенном **вне корневой директории веб-сервера**.

4.2. Выдача защищённых файлов осуществляется исключительно через контроллеры act_download.php и FileController после проверки полномочий текущего пользователя (AuthGuard). Каждое обращение должностного лица к персональным данным пайщика, анкете вступления или банковским реквизитам возврата пая в обязательном порядке фиксируется в неизменяемой таблице document_access_log (с защитой триггерами от UPDATE и DELETE).

5. СЕТЕВАЯ ЗАЩИТА, ЦЕЛОСТНОСТЬ РЕЕСТРА И ПРАВА СУБЪЕКТА ПДН

5.1. Веб-интерфейс АСКС защищён строгой политикой Content-Security-Policy (includes/Csp.php) с одноразовым криптографическим атрибутом nonce на каждом сценарии, защитой от межсайтовой подделки запросов (X-CSRF-Token), принудительной регенерацией сессии при входе и смене роли (Session.php, флаги Secure; HttpOnly; SameSite=Lax) и

обязательной двухфакторной аутентификацией (2FA) для членов Совета, Председателя и Ревизионной комиссии.

5.2. Финансовые и реестровые записи в таблице `audit_ledgers` связаны сквозной криптографической хэш-цепочкой (`trg_audit_ledgers_hash` + `ledger_chain_head`), в которой хэш каждой новой проводки вычисляется от хэша предыдущей записи. Ежесуточный ревизионный скрипт `cron/revisor_audit.php` проверяет непрерывность цепочки и при малейшем нарушении автоматически замораживает расходные операции фондов (`fund_freezes`).

5.3. Пайщик вправе в любой момент просмотреть свои персональные данные в разделе `/profile`, актуализировать их через регламентную процедуру `PersonalDataChangeService`, а после прекращения членства в Кооперативе и истечения установленных законодательством РФ сроков хранения бухгалтерской и корпоративной отчётности (5 лет по ФЗ № 402-ФЗ) - потребовать прекращения обработки и обезличивания своих персональных данных.
