

ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ООО «УК «Прогресс Менеджмент»

УТВЕРЖДЕНО

Приказом Генерального директора
ООО «УК «Прогресс Менеджмент»

№ 3 от «01» ноября 2025 г.

_____ / Петров Е.С. /

1. ОБЩИЕ ПОЛОЖЕНИЯ И ПРАВОВЫЕ ОСНОВАНИЯ

1.1. Настоящая Политика разработана в соответствии с требованиями следующих нормативных актов:

- **Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»** (далее — ФЗ-152), в том числе в редакции изменений, внесённых Федеральным законом от 14.07.2022 № 266-ФЗ (расширение обязанностей оператора в части утечек, новые требования к согласию на обработку с использованием систем ИИ, разграничение оснований трансграничной передачи ПД);
- **Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»** — устанавливает уровни защищённости (УЗ-1 — УЗ-4) и состав организационных и технических мер для каждого уровня;
- **Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных»** — определяет конкретные меры защиты в разрезе уровней защищённости;
- **Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов»:** обязывает устанавливать и верифицировать сведения о клиентах; период хранения записей — не менее 5 лет после прекращения деловых отношений.

1.2. Настоящая Политика действует в отношении всей деятельности ООО «УК «Прогресс Менеджмент» (далее — Оператор) по обработке персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление и уничтожение персональных данных.

2. КАТЕГОРИИ СУБЪЕКТОВ И СОСТАВ ОБРАБАТЫВАЕМЫХ ДАННЫХ

2.1. Клиенты — физические лица (инвесторы, выгодоприобретатели, бенефициарные владельцы)

Обрабатываемые данные: фамилия, имя, отчество; дата и место рождения; гражданство; реквизиты документа, удостоверяющего личность; ИНН; СНИЛС; адрес регистрации и фактического проживания; контактный телефон; адрес электронной почты; сведения о финансовом положении (уровень доходов, источник происхождения денежных средств) — в объёме, необходимом для исполнения требований ФЗ-115; сведения о деловой репутации.

Правовое основание: исполнение договора (ст. 6 ч. 1 п. 5 ФЗ-152); исполнение требований законодательства (ст. 6 ч. 1 п. 2 ФЗ-152); согласие субъекта (ст. 9 ФЗ-152).

2.2. Работники и кандидаты на вакантные должности

Обрабатываемые данные: полный объём данных, предусмотренный трудовым законодательством (ст. 86 ТК РФ); специальные категории ПД (состояние здоровья — исключительно для целей социального страхования, листков нетрудоспособности).

2.3. Представители контрагентов — юридических лиц

Обрабатываемые данные: ФИО, должность, контактная информация, данные документа, удостоверяющего личность, доверенность и полномочия.

2.4. Посетители официального сайта Оператора

Обрабатываемые данные: технические идентификаторы (IP-адрес, cookie-файлы, идентификаторы браузера, данные о действиях на сайте, собираемые Яндекс.Метрикой или аналогичными сервисами веб-аналитики).

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

№	Цель обработки	Категория субъектов	Правовое основание
1	Идентификация клиента в соответствии с требованиями ФЗ-115	Клиенты, бенефициарные владельцы	ФЗ-115, ст. 6 ч. 1 п. 2 ФЗ-152
2	Заключение и исполнение гражданско-правовых договоров	Клиенты, контрагенты	Ст. 6 ч. 1 п. 5 ФЗ-152
3	Рассмотрение обращений и жалоб	Клиенты, иные субъекты	Ст. 6 ч. 1 п. 2 ФЗ-152
4	Кадровое делопроизводство, расчёт зарплаты	Работники	Трудовой кодекс РФ
5	Обеспечение безопасности, пропускной режим	Посетители офиса	Ст. 6 ч. 1 п. 5 ФЗ-152
6	Веб-аналитика сайта	Посетители сайта	Согласие (cookie-баннер)

4. СРОКИ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Сроки хранения определяются требованиями законодательства и внутренними политиками хранения документов:

- **Документы по идентификации клиентов (ФЗ-115):** не менее **5 (пяти) лет** со дня прекращения деловых отношений с клиентом или со дня совершения финансовой операции;
- **Трудовые документы на работников:** в соответствии с Перечнем типовых управленческих архивных документов (Приказ Росархива от 20.12.2019 № 236), как правило — **50 или 75 лет** для документов по личному составу;
- **Договоры и переписка по гражданско-правовым сделкам:** не менее **5 (пяти) лет** после истечения срока действия договора;
- **Данные веб-аналитики (cookie):** в соответствии с настройками конкретного сервиса, но не более **13 (тринадцати) месяцев**.

4.2. По истечении срока хранения ПД подлежат уничтожению или обезличиванию в срок, не превышающий 30 (тридцати) календарных дней, с составлением акта об уничтожении.

5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ

5.1. Передача ПД третьим лицам без согласия субъекта ПД допускается исключительно в случаях, прямо предусмотренных законодательством:

- запросы Банка России в порядке надзора;
- запросы Федеральной службы по финансовому мониторингу (Росфинмониторинг);
- запросы органов дознания, следствия, прокуратуры и суда;
- передача сведений в налоговые органы (ФНС) в объёме, предусмотренном НК РФ;
- передача сведений специализированному депозитарию, регистратору в рамках сделок секьюритизации.

5.2. **Трансграничная передача ПД** (передача иностранным получателям) осуществляется только после уведомления Роскомнадзора и оценки уровня защиты в стране-получателе либо на основании согласия субъекта ПД с оговоркой о рисках такой передачи (ст. 12 ФЗ-152 в редакции ФЗ-266 от 14.07.2022).

6. ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ

6.1. Информационная система персональных данных (ИСПД) Оператора отнесена к **уровню защищённости УЗ-3** (иные актуальные угрозы; не специальные категории ПД; менее 100 000 субъектов) в соответствии с Постановлением Правительства № 1119.

6.2. Применяемые меры защиты:

- **Организационные:** назначен ответственный за обработку ПД (DPO); проводится ежегодный инструктаж сотрудников; введены режим коммерческой тайны и NDA;
- **Технические:** разграничение прав доступа к ИСПД по принципу минимально необходимых привилегий; применение сертифицированных ФСТЭК средств защиты информации (антивирус,

межсетевой экран); шифрование каналов передачи ПД (протокол TLS 1.2/1.3); резервное копирование данных;

- **Физические:** ограничение физического доступа к серверному оборудованию.

6.3. В случае выявления инцидента безопасности ПД (утечки) Оператор обязан уведомить Роскомнадзор в течение **24 часов** с момента обнаружения (первичное уведомление) и не позднее **72 часов** — с указанием установленных причин и принятых мер (в соответствии с требованиями Ф3-266).

7. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Субъект ПД вправе:

- получить подтверждение факта обработки ПД и ознакомиться с ними (ст. 14 Ф3-152);
- требовать уточнения, блокирования или уничтожения ПД, если они неполные, устаревшие, неточные или обрабатываются незаконно (ст. 21 Ф3-152);
- отозвать согласие на обработку ПД путём направления письменного заявления; при этом прекращение обработки ПД на основании закона (Ф3-115, НК РФ) не зависит от отзыва согласия;
- обжаловать действия Оператора в уполномоченном органе по защите прав субъектов ПД (Роскомнадзор) или в судебном порядке.

7.2. Для реализации своих прав субъект ПД направляет письменное заявление по адресу Оператора или на электронную почту. Оператор рассматривает заявление и направляет ответ в срок, не превышающий **10 (десяти) рабочих дней**.

Генеральный директор: _____ Петров Е.С.