



ORIENTFINANSBANK

**«УТВЕРЖДЕНО»
Первым Заместителем
Председателя Правления
Туйбоев Ш.Ш.**

от 19.08.2026

**«ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ЧАКБ «ОРИЕНТ ФИНАНС» В МОБИЛЬНОМ ПРИЛОЖЕНИИ «OFB
CORPORATE» ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ И ИНДИВИДУАЛЬНЫХ
ПРЕДПРИНИМАТЕЛЕЙ**

Ташкент 2026

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ЧАКБ «ОРИЕНТ ФИНАНС»
в Мобильном приложении «OFB CORPORATE» для юридических лиц и
индивидуальных предпринимателей

| 1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящая Политика конфиденциальности персональных данных (далее — Политика) действует в отношении всей информации, которую ЧАКБ «Ориент Финанс» (далее — Банк) может получить о Пользователе (уполномоченном представителе юридического лица или индивидуального предпринимателя) в процессе использования им Мобильного приложения дистанционного банковского обслуживания юридических лиц «OFB CORPORATE» (далее — Мобильное приложение «OFB CORPORATE»).
- 1.2. Использование Мобильного приложения «OFB CORPORATE» означает безоговорочное согласие Пользователя с настоящей Политикой и указанными в ней условиями обработки его Персональной информации. В случае несогласия с этими условиями Пользователь должен воздержаться от использования Мобильного приложения «OFB CORPORATE».

| 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- 2.1. В настоящей Политике используются следующие термины и определения:
 - 2.1.1. **Банк** — Частный акционерно-коммерческий банк «Ориент Финанс» (ЧАКБ «Ориент Финанс»).
 - 2.1.2. **Клиент** — юридическое лицо или индивидуальный предприниматель, заключивший с Банком Договор на банковское обслуживание / Договор дистанционного банковского обслуживания.
 - 2.1.3. **Пользователь** — уполномоченный представитель Клиента (руководитель, главный бухгалтер или иное доверенное лицо), зарегистрированный в Системе ДБО и использующий Мобильное приложение «OFB CORPORATE» от имени и в интересах Клиента.
 - 2.1.4. **Мобильное приложение «OFB CORPORATE»** — специализированное программное обеспечение Банка для мобильных устройств, предназначенное для дистанционного банковского обслуживания

юридических лиц и индивидуальных предпринимателей.

- 2.1.5. **Обработка персональной информации (Обработка)** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональной информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональной информации.
- 2.1.6. **Персональные данные** — любые данные, относящиеся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных / Пользователю).
- 2.1.7. **Персональная информация** — любая информация, которую Пользователь в явной или неявной форме предоставляет о себе в процессе использования Мобильного приложения «OFB CORPORATE», включая Персональные данные.
- 2.1.8. **Удаление персональных данных** — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе.

| 3. ОБРАБАТЫВАЕМАЯ ПЕРСОНАЛЬНАЯ ИНФОРМАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

- 3.1. Пользователи, являющиеся уполномоченными представителями Клиентов, передают Банку Персональные данные на основании договоров, заключаемых между Клиентом и Банком. Порядок Обработки таких данных определяется соответствующими договорами и законодательством Республики Узбекистан.
- 3.2. **В рамках Мобильного приложения «OFB CORPORATE» Банк обрабатывает следующие типы информации:**
- 3.2.1. Информация, предоставляемая Пользователем самостоятельно: фамилия, имя, отчество, должность, номер телефона, адрес электронной почты, логин, данные документов, удостоверяющих личность, а также иные данные, вводимые при заполнении форм, заявок и распоряжений в Приложении;
- 3.2.2. Автоматически передаваемые технические данные: IP-адрес, сетевой

идентификатор, уникальный идентификатор устройства (UUID/IMEI), данные из cookies, модель устройства, тип и версия операционной системы, версия Мобильного приложения «OFB CORPORATE», параметры активной сессии, время подключения;

3.2.3. Информация о местоположении (геолокация): данные о геопозиции устройства, автоматически передаваемые с согласия Пользователя для поиска ближайших филиалов/банкоматов и защиты от аномальных географических входов;

3.2.4. Информация об установленных приложениях (Antifraud): сведения о списке установленных на устройстве приложений, получаемые путем анализа через разрешение QUERY_ALL_PACKAGES исключительно в целях предотвращения мошенничества, защиты от удаленного управления и оценки рисков;

3.2.5. Биометрические данные устройства: При использовании аутентификации по Touch ID / Face ID Банк не получает и не хранит биометрические образцы Пользователя. Сверка биометрических данных происходит локально в защищенном модуле устройства (Secure Enclave). Банк получает только технический статус успешной проверки от операционной системы;

3.2.6. Разрешения устройства (Permissions): Мобильное приложение «OFB CORPORATE» может запрашивать доступ к:

- *Камере*: для сканирования QR-кодов, документов и фотофиксации при идентификации;
- *Геолокации*: для защиты от несанкционированного доступа из нетипичных регионов и локации офисов;
- *Push-уведомлениям*: для доставки одноразовых кодов (OTP), подтверждения корпоративных платежей и информирования о движении по счетам.

3.3. Настоящая Политика применима только к OFB CORPORATE. Банк не контролирует и не несет ответственность за системы третьих лиц. В таких системах у Пользователя может собираться или запрашиваться иная Персональная информация, а также могут совершаться иные действия.

| 4. ЦЕЛИ СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

4.1. Банк осуществляет Обработку только той Персональной информации,

которая необходима для корректного оказания услуг корпоративного банковского обслуживания, а также обеспечения информационной безопасности и предотвращения мошенничества.

4.2. Персональная информация Пользователя используется в следующих целях:

4.2.1. Идентификация и аутентификация Пользователя как уполномоченного лица Клиента;

4.2.2. Предоставление сервисов корпоративного ДБО (формирование и подписание платежных поручений, просмотр выписок, управление корпоративными картами и депозитами);

4.2.3. Связь с Пользователем, направление уведомлений, запросов и информации по операциям Клиента, обработка заявок и распоряжений;

4.2.4. Предотвращение мошенничества, выявление подозрительных операций и повышение безопасности доступа (Antifraud);

4.2.5. Выявление признаков вредоносного ПО и инструментов удаленного доступа (включая средства перехвата/экранирования, overlay, spoofing);

4.2.6. Обнаружение аномального поведения устройства, связанного с риском мошенничества;

4.2.7. Дополнительная риск-оценка при авторизации и выполнении корпоративных транзакций;

4.2.8. Выполнение требований законодательства Республики Узбекистан в сфере противодействия легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового поражения (ПОД/ФТ/ФРОМУ);

4.2.9. Улучшение качества работы Мобильного приложения «OFB CORPORATE» и оптимизация его функционала.

| 5. ПОРЯДОК ХРАНЕНИЯ И ОГРАНИЧЕНИЯ ИСПОЛЬЗОВАНИЯ ДАННЫХ АНТИФРОД-СИСТЕМЫ

5.1. Данные об установленных приложениях на устройстве обрабатываются в режиме реального времени и хранятся исключительно в течение периода, необходимого для целей предотвращения мошенничества и обеспечения безопасности (не дольше срока активной сессии и/или проведения риск-оценки согласно внутренним регламентам безопасности Банка).

5.2. Данные об установленных приложениях **НЕ используются** для рекламы,

маркетингового профилирования, а также не передаются третьим лицам в маркетинговых целях.

| 6. УСЛОВИЯ ПЕРЕДАЧИ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ТРЕТЬИМ ЛИЦАМ

- 6.1. Банк вправе передать Персональную информацию Пользователя третьим лицам в следующих случаях:
 - 6.1.1. Пользователь либо Клиент выразил свое прямое согласие на такие действия;
 - 6.1.2. Передача необходима для исполнения распоряжения Пользователя/Клиента в рамках банковского обслуживания;
 - 6.1.3. Передача предусмотрена законодательством Республики Узбекистан, международным законодательством и/или запросами уполномоченных государственных органов с соблюдением установленной процедуры;
 - 6.1.4. В целях защиты прав и законных интересов Банка в случаях, когда у Банка имеются основания полагать, что Пользователь нарушает условия настоящей Политики, договора ДБО или законодательства РУз.

| 7. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ПОРЯДОК ИХ РЕАЛИЗАЦИИ

- 7.1. Пользователь имеет право:
 - 7.1.1. Получать информацию, касающуюся обработки его персональных данных Банком;
 - 7.1.2. Требовать уточнения, блокирования или уничтожения персональных данных в случае, если они являются неполными, устаревшими или неточными;
 - 7.1.3. Отозвать свое согласие на обработку персональных данных путем направления письменного заявления в Банк;
- 7.2. Ограничения: Отзыв согласия не влечет за собой немедленного уничтожения персональных данных в случаях, когда их хранение требуется Банку в соответствии с законодательством Республики Узбекистан (включая банковское законодательство, архивное дело и нормы ПОД/ФТ/ФРОМУ — не менее 5 лет после прекращения отношений).

| 8. ПОРЯДОК И СРОКИ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

- 8.1. Персональные данные Пользователей хранятся в течение всего срока действия Договора на банковское обслуживание Клиента, а также в течение сроков, установленных нормативно-правовыми актами Республики Узбекистан (включая законодательство о банковской деятельности и ПОД/ФТ/ФРОМУ — не менее 5 лет после прекращения договора).
- 8.2. Технические данные, данные сессий и системные логи, собираемые в целях информационной безопасности и антифрода, хранятся в течение срока активной сессии и/или периода, необходимого для проведения риск-оценки и расследования инцидентов безопасности.

| 9. МЕРЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

- 9.1. Банк предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных в соответствии с Законом РУз от 02.07.2019 № ЗРУ-547 «О персональных данных»:
 - 9.1.1. Сетевая безопасность и шифрование: использование защищенных каналов передачи данных (TLS/SSL) и шифрование базы данных;
 - 9.1.2. Контроль доступа: применение принципа наименьших привилегий и двухфакторной аутентификации клиентов;
 - 9.1.3. Защита мобильного приложения: применение средств обфускации кода в релизных сборках, детектирование признаков компрометации устройства и защита от несанкционированного захвата экрана;
 - 9.1.4. Мониторинг и антифрод: круглосуточный мониторинг событий ИБ, автоматическое логирование действий и применение специализированных антифрод-систем;
 - 9.1.5. Организационные меры: регулярный аудит ИБ, проведение проверок на проникновение.

| 10. ИЗМЕНЕНИЕ ПОЛИТИКИ КОНФИДЕНЦИАЛЬНОСТИ

- 10.1. Банк имеет право в одностороннем порядке вносить изменения в настоящую Политику. Новая редакция Политики вступает в силу с момента ее размещения на официальном сайте Банка по адресу www.ofb.uz и/или публикации в Мобильном приложении «OFB CORPORATE».