Политика конфиденциальности
ТОО «Prosper Payment Solutions»

1. Общие положения

1.1. Настоящая Политика конфиденциальности (далее — Политика) разработана и применяется ТОО «Prosper Payment Solutions» (далее — Компания) в целях исполнения требований законодательства Республики Казахстан, включая Закон РК «О персональных данных и их защите» и Закон РК «Об информатизации», а также иных нормативных правовых актов РК.
1.2. Политика определяет принципы и правила обработки персональных и иных данных пользователей и клиентов сервиса Prosper Pay (далее — Пользователь), порядок сбора, использования, хранения, защиты и удаления информации, меры информационной безопасности, классификацию данных, порядок доступа, права субъектов данных и ответственность.
1.3. Политика применяется совместно с Политикой информационной безопасности, внутренними правилами Компании и документами, разработанными во исполнение Единых требований в области ИКТ и ИБ, утвержденных постановлением Правительства РК от 20.12.2016 № 832 (далее — Единые требования).
1.4. Политика распространяется на всех работников Компании, пользователей, контрагентов и партнеров, получающих доступ к сервису Prosper Pay, информационным системам и инфраструктуре Компании. В случае противоречия внутренних документов требованиям законодательства применяются нормы законодательства РК, внутренние документы подлежат актуализации.

2. Основания и цели обработки

2.1. Обработка данных осуществляется на следующих основаниях: согласие субъекта персональных данных; заключение и исполнение договора с Пользователем; исполнение требований законодательства (включая ПОД/ФТ и финансовый мониторинг); законные интересы Компании при соблюдении баланса прав и свобод Пользователя.
2.2. Цели обработки: идентификация Пользователя; предоставление доступа и функционала сервиса; ведение учета операций; исполнение договорных и законных обязанностей; улучшение качества сервиса; обеспечение безопасности, предотвращение мошенничества; восстановление доступа при утрате учетных данных; информирование в допустимых законом пределах.
2.3. Компания применяет принципы минимизации, ограниченности цели, достоверности, актуальности, ограничения сроков хранения, целостности и конфиденциальности (privacy by design / by default).

3. Состав обрабатываемых данных

3.1. Персональные данные: фамилия, имя, отчество (при наличии), ИИН, контактные данные (телефон, e-mail), данные, получаемые из государственных баз данных в пределах и порядке, предусмотренных законом, а также сведения от Работодателя Пользователя, необходимые для предоставления сервиса.
3.2. Финансовые и операционные данные: информация о начислениях и выплатах (заработная плата, компенсационные и иные выплаты), история операций и транзакций, сведения о движении денежных средств в рамках сервиса.
3.3. Технические и статистические данные: количество и длительность сессий, IP-адрес, данные геолокации (в т.ч. geoip), модель устройства, язык ОС и браузера, тип соединения, cookies и иные метаданные.

4. Классификация данных и управление доступом

4.1. Компания классифицирует данные по уровням конфиденциальности:
Уровень 1 (высококонфиденциальные): идентификационные и финансовые данные, аутентификационные сведения (логины, пароли, биометрия), секретные вопросы.
Уровень 2 (конфиденциальные): контактные данные, IP-адреса, геолокация. Доступ — по служебной необходимости.
Уровень 3 (общедоступные): агрегированная статистика, не позволяющая идентифицировать лицо.
4.2. Доступ предоставляется по принципам «необходимость и достаточность» и «разделение обязанностей», на основании ролей (RBAC), с обязательным журналированием действий и периодическим пересмотром прав.
4.3. Все пользователи, имеющие доступ к конфиденциальной информации, подписывают соглашения о конфиденциальности и неразглашении; аналогичные обязательства включаются в договоры с контрагентами.

5. Передача данных третьим лицам

5.1. Компания не продает персональные данные и не передает их третьим лицам, за исключением случаев:
(1) наличия согласия Пользователя;
(2) необходимости предоставления услуг в рамках сервиса или через доверенных партнеров;
(3) требований уполномоченных государственных органов в пределах их компетенции;
(4) передачи обезличенной статистики, не позволяющей идентифицировать лицо.
5.2. При передаче вовлеченным третьим лицам Компания заключает соглашения о защите данных, устанавливающие цели и пределы обработки, требования к ИБ, порядок реагирования на инциденты, возврата/уничтожения данных и право Компании на аудит.

6. Место хранения, сроки хранения и удаление данных

6.1. Все данные, обрабатываемые и (или) хранимые Компанией в рамках сервиса Prosper Pay, размещаются и хранятся на территории Республики Казахстан, за исключением случаев, прямо предусмотренных законодательством РК.
6.2. Персональные данные хранятся не дольше, чем этого требуют цели их обработки, либо в течение срока, прямо установленного законодательством РК, договорами с Пользователями или внутренними актами Компании при условии их соответствия законодательству.
6.3. По истечении сроков хранения либо при достижении целей обработки данные подлежат уничтожению или обезличиванию способами, исключающими возможность их восстановления и дальнейшего использования, за исключением случаев обязательного хранения по закону. Факт уничтожения оформляется актом по установленной форме.

7. Меры информационной безопасности и реагирование на инциденты

7.1. Организационные меры: утвержденная Политика ИБ; назначение ответственных за ИБ и комплаенс; фоновые проверки при найме в пределах закона; обучение и аттестация персонала; регламенты приема/перемещения/увольнения (отзыв доступов, возврат активов).
7.2. Технические меры: защита каналов связи (TLS 1.2+), шифрование на хранении (не ниже AES-256), сегментация сети, межсетевые экраны и WAF, антифрод и DLP, средства

обнаружения и предотвращения атак, управление уязвимостями, централизованное логирование с защитой от изменения, контроль целостности, антивирусная защита.
7.3. Безопасная разработка: SSDLC, анализ угроз, статический/динамический анализ кода, тесты на проникновение, управление изменениями и конфигурациями, документирование релизов.
7.4. Физическая безопасность: СКУД, охранная сигнализация, видеонаблюдение, регламенты посещений и пропускного режима, чистый стол и чистый экран.
7.5. Непрерывность и резервирование: планы BCP/DRP с целевыми RPO/RTO, географически распределенное резервное хранение, регулярное тестирование процедур восстановления.
7.6. Управление инцидентами: формализованный порядок регистрации, классификации, расследования и реагирования; уведомление субъектов данных и уполномоченных органов в сроки и порядке, установленных законодательством; реализация корректирующих мероприятий и профилактики.

8. Использование Интернета, почты и мобильных устройств

8.1. Передача данных по публичным сетям допускается только по защищенным каналам с применением криптографических средств. Удаленный и мобильный доступ разрешаются при документировании, мониторинге и применении средств криптографической защиты; беспроводной доступ — по требованиям Единых требований и внутренних регламентов.

9. Управление поставщиками и аутсорсерами

9.1. До предоставления доступа к данным или системам проводится оценка поставщика (due diligence). Договоры включают требования к ИБ и защите данных, показатели качества услуг, обязательства по уведомлению об инцидентах, порядок возврата/уничтожения данных и право Компании на аудит соблюдения.

10. Права субъекта персональных данных

10.1. Пользователь вправе получать сведения о наличии, составе и источниках своих персональных данных, целях, правовых основаниях и сроках их обработки, а также о передаче данных третьим лицам.
10.2. Пользователь вправе требовать изменения, дополнения, блокирования или удаления персональных данных в случаях и порядке, установленных законодательством РК, а также отзывать согласие на обработку, если иное не вытекает из закона или обязательного хранения.
10.3. Обращения субъектов данных рассматриваются Компанией в сроки и порядке, предусмотренные законодательством РК и внутренними регламентами.

11. Ответственность

11.1. За нарушение правил обработки и защиты данных Компания, ее должностные лица и сотрудники несут ответственность в соответствии с законодательством РК. Возможны административная, гражданско-правовая и уголовная ответственность (в т.ч. по статьям УК РК о незаконном сборе, распространении или использовании персональных данных и по статьям КоАП РК о нарушении норм защиты информации).

12. Актуализация Политики

12.1. Политика подлежит пересмотру при изменении законодательства, технологий, рисков, архитектуры сервиса, а также не реже одного раза в два года. Новая редакция вступает в силу с даты утверждения приказом директора и подлежит публикации на сайте https://ppsolutions.kz/ и (или) в мобильном приложении Prosper Pay.

Все вопросы, предложения и комментарии по вопросам обработки и защиты данных направляются ТОО «Prosper Payment Solutions» на электронную почту: info@ppsolutions.kz