Политика конфиденциальности и обработки персональных данных в системе DCXAI

1. Общие положения

1.1. Настоящая Политика конфиденциальности и обработки персональных данных (далее — **Политика**) определяет порядок и условия сбора, обработки, хранения, передачи, защиты и уничтожения персональных данных в информационной системе электронного документооборота **DCXAI** (далее — **Система**), правообладателем и поставщиком которой является ТОО «ABS LAB», БИН 250140007338 (далее — **Компания**). Место нахождения Компании: Республика Казахстан, город Астана, улица Керей, Жәнібек хандар, дом 32, бизнес-центр Grey Plaza.

1.2. Политика разработана в соответствии с законодательством Республики Казахстан и является общедоступным документом. Действующая редакция Политики размещается на официальном сайте Компании по адресу https://abslab.kz/docs/dcxai/privacy/ru/ (версия на казахском языке — https://abslab.kz/docs/dcxai/privacy/kk/) и доступна пользователям Системы из её интерфейса.

1.3. Политика распространяется на персональные данные **пользователей Системы** — работников и уполномоченных представителей организаций-заказчиков, которым предоставлен доступ к Системе.

1.4. Политика не регулирует обработку персональных данных, осуществляемую организацией-заказчиком самостоятельно вне Системы, а также обработку данных на интернет-ресурсах третьих лиц, ссылки на которые могут содержаться в Системе.

1.5. Использование Системы означает, что пользователь ознакомлен с настоящей Политикой. Согласие на сбор и обработку персональных данных, когда оно требуется, оформляется отдельно в порядке, предусмотренном разделом 6 Политики.

2. Термины и определения

Термины, используемые в Политике, применяются в значениях, установленных Законом Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (далее — **Закон о ПД**):

Термин	Значение
Персональные данные (ПД)	Сведения или совокупность сведений о субъекте персональных данных, дополненные одним или несколькими идентификаторами
Субъект	Физическое лицо, к которому относятся персональные данные
Собственник базы, содержащей ПД	Лицо, реализующее право владения, пользования и распоряжения базой (цифровым объектом), содержащей персональные данные
Оператор	Лицо, осуществляющее сбор, обработку и защиту персональных данных
Третье лицо	Лицо, не являющееся субъектом, собственником и (или) оператором, но связанное с ними в связи с обработкой персональных данных
Обработка ПД	Действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, анонимизацию, блокирование, уничтожение и удаление персональных данных
ПД ограниченного доступа	Персональные данные, доступ к которым ограничен законодательством Республики Казахстан
Трансграничная передача	Передача персональных данных за пределы территории Республики Казахстан
Заказчик	Юридическое лицо, заключившее с Компанией договор на предоставление доступа к Системе, работникам которого предоставляется доступ к Системе
Пользователь	Физическое лицо — работник или уполномоченный представитель Заказчика, имеющее учётную запись в Системе
ЭЦП	Электронная цифровая подпись в значении Закона Республики Казахстан «Об электронном документе и электронной цифровой подписи»

3. Правовая основа

Обработка персональных данных в Системе осуществляется в соответствии с:

- Конституцией Республики Казахстан;
- Законом Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»;
- Трудовым кодексом Республики Казахстан;
- Гражданским кодексом Республики Казахстан;
- Законом Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи»;
- законодательством Республики Казахстан об информатизации и цифровом развитии;

- Законом Республики Казахстан «О Национальном архивном фонде и архивах»;
- Правилами сбора, обработки персональных данных, утверждёнными уполномоченным органом;
- Правилами определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач;
- Правилами защиты персональных данных (в редакции, введённой в действие с 12 июля 2026 года);
- иными нормативными правовыми актами Республики Казахстан.

4. Распределение ролей сторон

4.1. Система предоставляется по модели SaaS: программное обеспечение и база данных размещаются в инфраструктуре, эксплуатируемой Компанией.

4.2. В отношении персональных данных, размещаемых в Системе Заказчиком и его Пользователями (сведения о работниках, содержание документов, маршруты согласования):

- **Заказчик** выступает **собственником базы, содержащей персональные данные**, и определяет цели и состав обрабатываемых персональных данных, а также перечень лиц, имеющих к ним доступ;
- **Компания** выступает **оператором (третьим лицом)**, осуществляющим обработку персональных данных **по поручению и в интересах Заказчика** в объёме, необходимом для функционирования Системы, на основании договора. Условия обработки по поручению фиксируются в договоре и (или) отдельном соглашении об обработке персональных данных.

4.3. В отношении сведений, которые Компания обрабатывает для собственных целей (администрирование учётных записей и лицензий, техническая поддержка, обеспечение информационной безопасности, исполнение требований законодательства), **Компания выступает собственником и (или) оператором**.

4.4. Компания не определяет самостоятельно состав и содержание документов, размещаемых Пользователями в Системе, и не использует их для целей, не предусмотренных договором с Заказчиком и настоящей Политикой.

5. Категории субъектов и состав обрабатываемых персональных данных

5.1. Компания придерживается принципа минимизации: обрабатываются только те персональные данные, которые необходимы и достаточны для достижения целей обработки.

5.2. В Системе обрабатываются следующие категории данных Пользователей:

Группа	Состав данных	Источник
Учётные данные	Логин (имя пользователя), идентификатор учётной записи в системе управления доступом, статус активности, язык интерфейса, роли и права доступа	Заказчик (при заведении учётной записи)
Идентификационные данные	Фамилия, имя, отчество, индивидуальный идентификационный номер (ИИН)	Заказчик, регистрационное свидетельство ЭЦП
Контактные данные	Служебный адрес электронной почты, служебный номер телефона	Заказчик
Служебные (кадровые) сведения	Должность, структурное подразделение, наименование и БИН организации, руководитель, уровень в иерархии согласования	Заказчик
Данные об электронной подписи	Открытый ключ и реквизиты регистрационного свидетельства ЭЦП, ИИН/БИН владельца свидетельства, значение подписи, дата и время подписания, результат проверки подписи	Пользователь (при подписании), удостоверяющий центр
Данные о действиях в Системе	Создание, согласование, подписание, отклонение и передача документов; резолюции, задания и поручения; комментарии; даты и время действий; исполнители и адресаты	Система (автоматически)
Содержание документов и вложений	Реквизиты и текст документов, прикреплённые файлы, сведения о контрагентах (наименование, БИН/ИИН, адрес, представитель, банковские реквизиты), а также любые персональные данные, включённые Пользователями в содержание документов	Пользователь
Технические данные (журналы)	IP-адрес, сведения о браузере и устройстве, дата и время входа и действий, идентификатор сессии, события доступа к данным	Система (автоматически)
Обращения в поддержку	Содержание обращения, контактные данные заявителя, приложенные материалы	Пользователь

5.3. **Персональные данные ограниченного доступа.** ИИН, сведения кадрового характера и содержание документов с ограничительными пометками обрабатываются как персональные данные ограниченного доступа с применением мер, предусмотренных разделом 12 Политики.

5.4. **Биометрические данные.** Компания не собирает и не хранит биометрические данные. В мобильном приложении может использоваться биометрическая разблокировка средствами операционной системы устройства (отпечаток пальца, распознавание лица): проверка выполняется самим устройством,

биометрический шаблон хранится в его защищённой среде, в Систему не передаётся и Компании не доступен — приложение получает только результат проверки (раздел 16). Если биометрические механизмы применяются на стороне государственных сервисов подписания (мобильная ЭЦП), их обработка осуществляется оператором такого сервиса, а не Компанией.

5.5. Пользователям не следует размещать в Системе персональные данные, не относящиеся к целям деловой переписки и документооборота Заказчика, в том числе сведения о состоянии здоровья, религиозных и политических убеждениях, если иное прямо не предусмотрено внутренними документами Заказчика и законодательством.

6. Цели обработки и правовые основания

6.1. Персональные данные обрабатываются исключительно в целях, указанных ниже.

№	Цель обработки	Состав данных	Правовое основание
1	Предоставление доступа к Системе, идентификация и аутентификация Пользователя, разграничение прав доступа	Учётные, идентификационные, контактные, служебные данные	Исполнение договора с Заказчиком; обработка в связи с трудовыми отношениями (статья 9 Закона о ПД)
2	Организация электронного документооборота: создание, маршрутизация, согласование, подписание, регистрация, хранение и поиск документов	Все категории по п. 5.2	Исполнение договора; трудовые отношения; законодательство о документировании и архивном деле
3	Подписание документов ЭЦП и проверка подлинности подписи	Данные об ЭЦП, ИИН/БИН	Закон «Об электронном документе и электронной цифровой подписи»; согласие Пользователя при использовании ключа ЭЦП
4	Формирование заданий и поручений, контроль исполнительской дисциплины	Идентификационные, служебные данные, данные о действиях	Трудовые отношения; локальные акты Заказчика
5	Ведение журналов доступа и действий, расследование инцидентов, обеспечение информационной безопасности	Технические данные, данные о действиях	Требования законодательства о защите персональных данных
6	Техническая поддержка, устранение ошибок, восстановление данных	Учётные, контактные данные, содержание обращений, минимально необходимые данные Системы	Исполнение договора с Заказчиком
7	Уведомления Пользователей о событиях в Системе (поступление документа на согласование, наступление срока исполнения)	Контактные, служебные данные	Исполнение договора; трудовые отношения
8	Работа интеллектуальных сервисов: поиск, подсказки, автозаполнение и ответы по содержанию документа	Текст запроса, реквизиты и текст документа, вложения	Исполнение договора с Заказчиком; при использовании внешней модели — согласие субъекта на трансграничную передачу (статья 16 Закона о ПД)
9	Исполнение обязательных требований законодательства, ответы на законные запросы государственных органов	Необходимый объём данных	Требования законодательства Республики Казахстан

6.2. Персональные данные не используются в маркетинговых целях, не передаются в рекламные сети и не являются предметом возмездной передачи третьим лицам.

6.3. Обработка персональных данных Пользователей осуществляется **без получения отдельного согласия** в случаях, предусмотренных статьёй 9 Закона о ПД, в том числе когда обработка необходима для исполнения договора, стороной которого является субъект или выгодоприобретателем которого он выступает, а также когда она осуществляется в связи с трудовыми отношениями между Пользователем и Заказчиком.

6.4. В случаях, когда законодательство требует согласия субъекта, оно оформляется в письменной или электронной форме и содержит сведения, предусмотренные статьёй 8 Закона о ПД: наименование (Ф.И.О.) собственника и (или) оператора, Ф.И.О. субъекта, срок действия согласия, перечень собираемых персональных данных, указание на возможность передачи третьим лицам и на наличие трансграничной передачи.

6.5. **Отзыв согласия.** Субъект вправе отозвать согласие, направив уведомление по контактам, указанным в разделе 15. Обработка персональных данных прекращается **в течение пятнадцати рабочих дней** со дня получения уведомления, за исключением случаев, когда законодательство Республики Казахстан допускает обработку без согласия субъекта (в частности, при наличии неисполненных обязательств, а также в отношении документов, подлежащих обязательному хранению).

7. Порядок обработки и автоматизированные операции

7.1. Обработка персональных данных осуществляется смешанным способом: автоматизированно (в Системе) и без использования средств автоматизации (при оформлении документов на бумажном носителе на стороне Заказчика).

7.2. Автоматизированные операции Системы включают маршрутизацию документов по заданным Заказчиком маршрутам согласования, формирование заданий, расчёт сроков исполнения, нумерацию и регистрацию документов, поиск по документам, а также интеллектуальные функции, предусмотренные разделом 17.

7.3. Решения, порождающие юридические последствия для субъекта (согласование, подписание, отклонение документа, выдача поручения), принимаются уполномоченными Пользователями. Система фиксирует такие решения, но не принимает их исключительно автоматизированным способом без участия человека.

7.4. Каждое действие с документом фиксируется в журнале Системы с указанием исполнителя, даты и времени. Записи журналов не подлежат изменению Пользователями.

8. Электронная цифровая подпись

8.1. Подписание документов в Системе осуществляется с использованием ЭЦП Пользователя одним из способов: с применением программного обеспечения для работы с ключами ЭЦП на рабочем месте Пользователя либо посредством мобильного подписания (в том числе по QR-коду) через уполномоченные сервисы.

8.2. Закрытый ключ ЭЦП Пользователя **не передаётся в Систему и не хранится в ней**. Формирование подписи происходит на устройстве Пользователя либо в защищённой среде сервиса подписания. В Системе хранятся значение подписи, открытая часть регистрационного свидетельства и сведения о результате проверки подписи.

8.3. Пользователь обязан обеспечивать конфиденциальность закрытого ключа ЭЦП. Компания не несёт ответственности за последствия компрометации ключа, произошедшей по вине Пользователя.

8.4. Сведения об ЭЦП хранятся в составе подписанного документа в течение срока хранения соответствующего документа и служат подтверждением его подлинности и целостности.

9. Передача персональных данных третьим лицам

9.1. Компания передаёт персональные данные третьим лицам только в объёме, необходимом для достижения целей, указанных в разделе 6, и при условии соблюдения такими лицами требований по конфиденциальности и защите персональных данных.

9.2. Категории получателей:

Категория получателя	Назначение передачи	Передаваемые данные
Заказчик (работодатель Пользователя)	Организация документооборота, контроль исполнения	Данные Пользователя в Системе
Оператор центра обработки данных (хостинг-провайдер)	Размещение и эксплуатация серверной инфраструктуры на территории Республики Казахстан	Данные Системы в составе инфраструктуры
Удостоверяющий центр и операторы сервисов подписания	Проверка подлинности ЭЦП, мобильное подписание	ИИН/БИН, реквизиты регистрационного свидетельства, значение хеша подписываемого документа
Поставщики каналов уведомлений (электронная почта, SMS)	Направление служебных уведомлений	Служебный адрес электронной почты / номер телефона, текст уведомления
Операторы штатных платформ доставки push-уведомлений операционных систем устройств	Доставка уведомлений в мобильное приложение	Push-токен устройства, тип события и идентификатор документа (без содержания документа)
Сервис диагностики и отчётов об ошибках мобильного приложения	Выявление и устранение сбоев	Технические сведения об устройстве и приложении, данные о сбое, идентификатор установки
Поставщик облачных языковых моделей (при соответствующей конфигурации Системы)	Работа интеллектуальных сервисов	Текст запроса и относящегося к нему фрагмента документа (раздел 17)
Государственные органы	Исполнение законных запросов	Данные в объёме, предусмотренном запросом и законодательством

9.3. Актуальный перечень привлечённых Компанией третьих лиц с указанием наименования, местонахождения и назначения предоставляется Заказчику по запросу. Компания информирует Заказчика об изменении состава таких лиц.

9.4. Компания не осуществляет распространение персональных данных Пользователей в общедоступных источниках.

10. Трансграничная передача

10.1. Содержание документов, учётные и служебные данные Пользователей за пределы Республики Казахстан **не передаются**: их сбор, обработка и хранение производятся в инфраструктуре, расположенной на территории Республики Казахстан. Исключение составляют технические данные мобильного приложения — push-токен устройства и диагностические сведения о сбоях, которые обрабатываются платформами доставки уведомлений и сервисом диагностики за пределами Республики Казахстан

(раздел 16), а также случай, когда по договору с Заказчиком интеллектуальные сервисы Системы используют внешнюю языковую модель: тогда за пределы Республики Казахстан передаётся содержание запроса и относящегося к нему фрагмента документа (раздел 17).

10.2. Если для оказания отдельных услуг потребуется передача персональных данных за пределы Республики Казахстан, такая передача осуществляется в соответствии со статьёй 16 Закона о ПД — только при обеспечении принимающей стороной защиты персональных данных и при наличии согласия субъекта либо иного основания, предусмотренного законом. Сведения о таких передачах доводятся до Заказчика до начала передачи.

11. Место и сроки хранения, уничтожение

11.1. **Место хранения.** Накопление и хранение персональных данных осуществляется в базах данных, размещённых в центрах обработки данных на территории Республики Казахстан. Там же хранятся резервные копии.

11.2. **Сроки хранения.** Персональные данные хранятся в течение срока, необходимого для достижения целей обработки, если иной срок не установлен законодательством или номенклатурой дел Заказчика:

Категория	Срок хранения
Документы и вложения	В соответствии со сроком, установленным номенклатурой дел Заказчика для соответствующего вида документа (в Системе задаётся параметром срока хранения дела), но не менее срока, предусмотренного законодательством об архивном деле
Учётные данные Пользователя	В течение срока действия учётной записи и 12 месяцев после её блокирования
Журналы доступа и действий	3 года с даты события
Обращения в техническую поддержку	1 год с даты закрытия обращения
Данные, обрабатываемые по договору с Заказчиком	В течение срока действия договора и 30 календарных дней после его прекращения (для возврата или уничтожения данных)

11.3. **Уничтожение.** По достижении целей обработки, при прекращении договора с Заказчиком либо по обоснованному требованию уполномоченного лица персональные данные подлежат уничтожению (удалению) в порядке, предусмотренном статьёй 18 Закона о ПД, с составлением акта. Уничтожение выполняется способом, исключающим восстановление данных, в том числе в резервных копиях — по мере их плановой ротации.

11.4. При прекращении договора Заказчику предоставляется возможность выгрузки данных в течение 30 календарных дней, после чего данные уничтожаются, если законодательство не требует иного.

12. Меры защиты персональных данных

12.1. Компания принимает организационные и технические меры, необходимые и достаточные для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования и распространения.

Организационные меры:

- назначение лица, ответственного за организацию обработки персональных данных, и осуществление им внутреннего контроля;
- утверждение перечня бизнес-процессов, в которых обрабатываются персональные данные, и перечня работников, имеющих доступ к персональным данным, с определением уровня доступа;
- утверждение перечня персональных данных, необходимого и достаточного для выполнения осуществляемых задач;
- подписание работниками обязательств о неразглашении, ознакомление работников с требованиями законодательства о персональных данных;
- регламент реагирования на инциденты информационной безопасности;
- периодический пересмотр прав доступа и внутренний контроль соблюдения Политики.

Технические меры:

- ролевая модель доступа и централизованная аутентификация, поддержка единого входа и многофакторной аутентификации;
- передача данных исключительно по защищённым каналам (TLS/HTTPS);
- шифрование хранимых данных и резервных копий; для персональных данных ограниченного доступа — средства криптографической защиты не ниже уровня, установленного применимыми стандартами (СТ РК 1073-2007);
- журналирование событий системы управления базами данных и действий пользователей при доступе к персональным данным ограниченного доступа;
- сегментация сети, межсетевое экранирование, антивирусная защита, управление уязвимостями и обновлениями;
- резервное копирование и периодическая проверка восстановления;
- разграничение сред разработки, тестирования и эксплуатации; запрет использования реальных персональных данных в тестовых средах без обезличивания.

12.2. Доступ работников Компании к данным Заказчика предоставляется по принципу минимально необходимых привилегий, на время выполнения конкретной задачи технической поддержки, с фиксацией в журнале.

13. Действия при нарушении безопасности персональных данных

13.1. При выявлении нарушения безопасности персональных данных (несанкционированный доступ, утечка, уничтожение или изменение данных) Компания:

1) незамедлительно принимает меры по локализации и устранению нарушения;

2) уведомляет уполномоченный орган в сфере защиты персональных данных **в течение одного рабочего дня** с момента обнаружения нарушения, с указанием контактных данных лица, ответственного за организацию обработки персональных данных, принятых мер и сведений, необходимых для последующего уведомления субъектов;

3) незамедлительно информирует Заказчика, персональные данные которого затронуты, для организации уведомления субъектов;

4) регистрирует инцидент во внутреннем журнале и проводит расследование с оценкой причин и мер по недопущению повторения.

13.2. Порядок и форма уведомления определяются нормативными правовыми актами уполномоченного органа.

14. Права субъекта персональных данных

14.1. В соответствии со статьёй 24 Закона о ПД субъект вправе:

- знать о наличии у собственника и (или) оператора персональных данных, относящихся к нему, а также получать информацию об условиях доступа к его персональным данным;
- получать сведения о третьих лицах, которым переданы его персональные данные;
- требовать изменения и дополнения своих персональных данных при наличии оснований, подтверждённых соответствующими документами;
- требовать блокирования персональных данных при наличии сведений о нарушении условий их сбора и обработки;
- требовать уничтожения (удаления) персональных данных, сбор и обработка которых были осуществлены с нарушением законодательства, а также в иных случаях, предусмотренных законом;
- отзывать согласие на сбор и обработку персональных данных;
- защищать свои права и законные интересы, в том числе требовать возмещения причинённого вреда;
- обжаловать действия (бездействие) собственника, оператора и третьего лица в уполномоченный орган или в суд.

14.2. **Порядок обращения.** Обращение направляется по адресу электронной почты, указанному в разделе 15, и должно содержать: фамилию, имя, отчество субъекта, сведения, позволяющие его идентифицировать (в том числе наименование организации и должность), существо требования и способ направления ответа.

14.3. **Сроки рассмотрения.** Компания рассматривает обращение и предоставляет ответ в сроки, установленные Законом о ПД: по требованиям об изменении, дополнении и уничтожении персональных данных, а также о предоставлении сведений об их обработке — **в течение трёх рабочих дней** со дня получения обращения; прекращение обработки при отзыве согласия — **в течение пятнадцати рабочих дней**. Если Пользователь является работником Заказчика, Компания вправе перенаправить обращение Заказчику как собственнику базы, уведомив об этом заявителя.

14.4. В удовлетворении требования может быть отказано, если это противоречит законодательству Республики Казахстан либо если данные подлежат обязательному хранению (в том числе подписанные ЭЦП документы, входящие в документальный фонд Заказчика). Отказ доводится до субъекта в письменной форме с обоснованием.

15. Контакты

15.1. Вопросы, обращения и требования, связанные с обработкой персональных данных, направляются на адрес электронной почты: **info@abslab.kz**. По этому же адресу доступно лицо, ответственное за организацию обработки персональных данных.

16. Особенности мобильного приложения

16.1. Настоящий раздел описывает обработку персональных данных в мобильном приложении DCXAI. Остальные разделы Политики применяются к мобильному приложению в полном объёме.

16.2. **Разрешения устройства.** Приложение запрашивает доступ к камере (сканирование QR-кода при подписании документа), к уведомлениям и к файлам устройства (просмотр и прикрепление вложений). Разрешения запрашиваются при первом использовании соответствующей функции и могут быть отозваны в настройках устройства; отказ ограничивает работу только этой функции.

16.3. **Биометрический вход.** Разблокировка приложения по отпечатку пальца или изображению лица выполняется средствами операционной системы устройства. Биометрический шаблон хранится в защищённой среде устройства, в Систему не передаётся и Компании не доступен — приложение получает только результат проверки. Биометрический вход отключается в настройках приложения с переходом на вход по паролю.

16.4. **Подписание документов.** Мобильное приложение не хранит закрытые ключи электронной цифровой подписи. Подписание выполняется через уполномоченный сервис мобильного подписания, которому передаются идентификатор и хеш подписываемого документа, а также ИИН подписывающего лица. Обработка данных в таком сервисе осуществляется его оператором в соответствии с законодательством Республики Казахстан.

16.5. **Push-уведомления.** Для доставки уведомлений о поступлении документа на согласование или подписание и о наступлении срока исполнения обрабатываются push-токен устройства, тип события и идентификатор документа. Доставка осуществляется штатными платформами push-уведомлений операционных систем устройства, серверы которых расположены за пределами Республики Казахстан, что является трансграничной передачей в значении статьи 16 Закона о ПД. Содержание документов и вложения в push-уведомлениях не передаются. Уведомления отключаются в настройках приложения или устройства.

16.6. **Диагностика и отчёты об ошибках.** Для выявления и устранения сбоев обрабатываются технические сведения: модель устройства, версия операционной системы и приложения, идентификатор установки, данные о сбое и предшествующих ему действиях. Эти сведения передаются во внешний сервис диагностики, обработка в котором может осуществляться за пределами Республики Казахстан. Диагностические данные не используются для рекламы и профилирования.

16.7. **Данные на устройстве.** Токены доступа хранятся в защищённом хранилище операционной системы. Приложение не сохраняет документы для офлайн-доступа: данные, отображаемые в текущей сессии, находятся во временной памяти и удаляются при выходе из учётной записи и при удалении приложения. При утрате устройства Пользователю следует обратиться к Заказчику или по адресу, указанному в разделе 15, для блокирования учётной записи.

16.8. **Геолокация и рекламные идентификаторы.** Приложение не собирает данные о местоположении устройства и не использует рекламные идентификаторы; персональные данные не передаются в рекламные и аналитические сети маркетингового назначения.

16.9. **Распространение через магазины приложений.** Настоящая Политика доступна по публичной ссылке в карточке приложения. Сведения, декларируемые в Google Play (раздел «Безопасность данных») и в App Store (сведения о конфиденциальности), соответствуют настоящей Политике. Учётная запись Пользователя создаётся и удаляется Заказчиком; обращения по вопросам удаления учётной записи и данных направляются по адресу, указанному в разделе 15.

17. Интеллектуальные сервисы Системы

17.1. Система может предоставлять функции интеллектуальной обработки текста: поиск по документам с учётом смысла запроса, подсказки и автозаполнение полей при создании документа, определение подходящего шаблона по загруженному файлу, формирование ответов на вопросы по содержанию документа. Состав доступных функций определяется договором с Заказчиком.

17.2. **Передаваемые данные.** Для выполнения запроса обрабатываются: текст запроса Пользователя, реквизиты и текст документа либо его фрагмента, извлечённый текст вложенного файла, идентификаторы Пользователя и сессии. Если документ содержит персональные данные, они обрабатываются в составе такого запроса.

17.3. **Место обработки.** Обработка выполняется одним из двух способов, определяемым конфигурацией Системы по договору с Заказчиком: (1) языковой моделью, размещённой в инфраструктуре Компании на территории Республики Казахстан, либо (2) с привлечением внешнего поставщика облачных языковых моделей, вычислительные мощности которого расположены за пределами Республики Казахстан. Во втором случае имеет место трансграничная передача персональных данных в значении статьи 16 Закона о ПД. Применяемый вариант доводится до Заказчика до начала обработки и фиксируется в договоре.

17.4. **Условия привлечения внешнего поставщика.** Передача осуществляется по защищённому каналу и только в объёме, необходимом для формирования ответа на конкретный запрос. Наименование поставщика и условия обработки данных на его стороне — включая то, могут ли переданные данные использоваться для улучшения и обучения моделей, — определяются договором Компании с поставщиком и доводятся до Заказчика до начала обработки. Заказчик вправе отказаться от использования внешней модели, выбрав обработку в инфраструктуре Компании либо отключив интеллектуальные сервисы.

17.5. **Характер результатов.** Результаты работы интеллектуальных сервисов носят вспомогательный характер: они предлагаются Пользователю для проверки и не являются решением, порождающим юридические последствия. Согласование, подписание, отклонение документа и выдача поручения выполняются уполномоченными Пользователями в порядке, предусмотренном разделом 7 Политики.

17.6. **Журналы взаимодействий.** Запросы, сформированные ответы и оценки их качества, оставленные Пользователями, сохраняются в Системе для контроля качества и разбора обращений в течение не более одного года, после чего удаляются.

17.7. **Отключение.** Заказчик вправе отключить интеллектуальные сервисы полностью либо для отдельных подразделений и Пользователей. При отключении данные в такие сервисы не передаются.

17.8. Пользователям не следует включать в запросы к интеллектуальным сервисам персональные данные, не относящиеся к обрабатываемому документу и задаче.

18. Заключительные положения

18.1. Компания вправе вносить изменения в Политику. Актуальная редакция размещается по адресу, указанному в п. 1.2, с указанием даты вступления в силу. О существенных изменениях Заказчики уведомляются не менее чем за 30 календарных дней до вступления изменений в силу.

18.2. Политика составлена на казахском и русском языках. В случае расхождений между версиями преимущественную силу имеет версия на казахском языке.

18.3. Отношения, не урегулированные Политикой, регулируются законодательством Республики Казахстан и договором между Компанией и Заказчиком.