Политика хранения и удалений

(редакция от «26» сентября 2025 г.)

1. Назначение и область действия

1.1. Политика устанавливает правила хранения, резервного копирования, ограничения по объёму и порядок удаления данных пользователей (далее — **Данные**) в Платформе DSLab.
1.2. Политика является неотъемлемой частью Договора-оферты и применяется ко всем пользователям (физическим и юридическим лицам).
1.3. Все системы хранения и резервного копирования находятся на территории Российской Федерации.

2. Термины

Проект — набор файлов, артефактов вычислений, кода и настроек.
Хранилище — суммарный дисковый объём аккаунта в DSLab.
Грейс-период — 7 дней после окончания платной подписки.
Резервные копии (бэкапы) — копии данных для аварийного восстановления.

3. Классы данных и SLA доступности

3.1. **Активные данные** (рабочие проекты, активные сессии): хранение на производительном уровне (NVMe/SSD или аналог).
3.2. **Архивные данные** (часто не используемые, «остановленные» окружения): могут переводиться в более «холодный» класс хранения.
3.3. **Временные данные** (кэш, промежуточные артефакты, логи задач): могут автоматически удаляться согласно регламенту.
3.4. Уровень доступности не является гарантированным SLA, если иное не указано в тарифе/допсоглашении; сервис предоставляется «как есть».

4. Лимиты хранилища и поведение при превышении

4.1. Лимиты определяются активным тарифом и суммируются на уровне аккаунта.
4.2. При превышении лимита:
– запись новых данных и запуск сессий могут быть ограничены;
– система выводит уведомления в интерфейсе и/или на e-mail.
4.3. Снижение объёма хранилища возможно удалением данных, сменой.

5. Грейс-период и порядок удаления при переполнении

5.1. По окончании оплаченного периода пользователю предоставляется 7 календарных дней на продление подписки или самостоятельную очистку памяти в хранилище.
5.2. Если к окончанию грейса объём превышает лимит бесплатного тарифа, DSLab вправе удалить данные сверх лимита без дополнительного согласования.
5.3. Очередность удаления проектов: от самых старых до самых новых. Удаление происходит пока память не будет в пределах нормы.

5.4. Удаление необратимо, если данные не присутствуют в актуальных бэкапах (см. п. 6–7).

6. Резервное копирование

6.1. Резервное копирование не совершается.

7. Восстановление

7.1. При аварии DSLab стремится восстановить работоспособность и данные из доступных бэкапов в разумные сроки.
7.2. DSLab не гарантирует восстановление каждого файла/версии/артефакта.
7.3. Пользователь самостоятельно обеспечивает локальные копии критичных артефактов (репозитории, датасеты, чекпоинты моделей и т.д.).

8. Удаление по инициативе пользователя

8.1. Удаление проекта — из активных систем немедленно/в короткий срок; из резервных копий — по завершении ротации.
8.2. Закрытие аккаунта — инициируется в Личном кабинете/через поддержку; удаление из активных систем — в разумный срок, из бэкапов — после ротации.
8.3. Удалённые данные, доступные в бэкапах до окончания ротации, не выдаются на экспорт.

9. Хранение журналов и метаданных

9.1. Служебные журналы (аудит, биллинг, телеметрия) хранятся в РФ определённые сроки для безопасности и бухгалтерского учёта.
9.2. Сроки хранения зависят от нормативных требований и внутренних регламентов.

10. Безопасность

10.1. Применяются организационные и технические меры (разграничение доступа, шифрование каналов, мониторинг, защита от МНН).
10.2. Пользователь обязан хранить секретные ключи/пароли, не допускать их раскрытия.

11. Ответственность и ограничения

11.1. Сервис предоставляется «как есть».
11.2. DSLab не несёт ответственности за потерю данных по причинам, зависящим от пользователя/третьих лиц, а также за последствия удаления по п. 5.
11.3. Совокупная ответственность ограничена офертой.

12. Изменения политики

12.1. Политика может изменяться с публикацией новой редакции на сайте. Продолжение использования сервиса означает согласие с изменившийся политикой.

NEP-политика обезличивания

(редакция от «26» сентября 2025 г.)

1. Назначение

1.1. Политика описывает методы и правила обезличивания входящих данных пользователей в NEP-сервисе, расположенном в РФ, до их возможной передачи зарубежным поставщикам LLM.
1.2. Цель — соблюдение требований законодательства РФ, в т.ч. ФЗ-152, и исключение трансграничной передачи персональных данных.

2. Роли и инфраструктура

2.1. DSLab выступает оператором ПДн в части аккаунтов/биллинга и обработчиком — когда действует по поручению клиента.
2.2. NEP-сервис и сопутствующие журналы размещены в РФ.
2.3. Передача данных за рубеж допускается только после обработки NEP и только в обезличенном виде.

3. Объём и источники данных

3.1. Источники: тексты запросов к API, вложения (файлы/изображения/метаданные), параметры вызовов, служебные сведения из SDK.
3.2. Пользователь обязан отправлять в API минимально необходимый объём и не включать ПДн, если это не нужно для личных целей.

4. Категории сведений, подлежащих защите

4.1. Персональные идентификаторы: ФИО, дата рождения, гражданство, документы, биометрия.
4.2. Контакты: e-mail, телефоны, мессенджеры, логины, почтовые/фактические адреса.
4.3. Косвенные идентификаторы: ID устройств/профилей, cookie, IP-адреса (в теле запроса), GPS-координаты, MAC/IMEI/серийные номера.
4.4. Финансовые/медицинские/профессиональные/образовательные данные, коммерческая тайна и иные охраняемые законом сведения.
4.5. Метаданные: EXIF, авторские теги файлов, URL с токенами, реферальные параметры, заголовки, в которых могут присутствовать ПДн.

5. Техники NEP-обработки

5.1. **Маскирование/удаление**: детектирование и замена сущностей (regex+NER+правила), вырезание секретных токенов/ключей/ID.
5.2. **Нормализация/обобщение**: приведение к менее детализированному виду (например, «г. Москва» вместо точного адреса; «возрастная группа» вместо даты рождения).
5.3. **Усечение контекста**: передача за рубеж только необходимых фрагментов.
5.4. **Фильтрация вложений**: очистка EXIF/метаданных, удаление встроенных превью/миниатюр с идентификаторами, запрет бинарей с неочищаемыми метаданными.
5.5. **Политики списков**: стоп-слова/черные списки для известных рисковых паттернов

(ключи, пароли, JWT, токены OAuth и т.п.).
5.6. **Блокировка**: если безопасная трансформация невозможна — запрос блокируется с ошибкой и рекомендациями по редактированию.

6. Журналы NEP и хранение

6.1. Журналы NEP содержат технические метаданные о трансформации (виды замен, категории сущностей, статусы) без исходных ПДн.
6.2. Хранятся в РФ ограниченный срок для безопасности, аудита и биллинга; доступ строго регламентирован.
6.3. Полные тексты пользовательских запросов не сохраняются в NEP-журналах после трансформации, за исключением минимальных фрагментов, необходимых для расследования инцидентов безопасности (и то — с дополнительным маскированием).

7. Гарантии и ограничения

7.1. NEP снижает риск утечки ПДн, но не гарантирует нулевой риск при некорректном использовании API (например, если пользователь намеренно встраивает ПДн в код/изображения после предупреждений).
7.2. Заказчик несёт ответственность за законность ввода данных и обязанность уведомления субъектов при необходимости.
7.3. Поставщики LLM не контролируются DSLab; поведение моделей и обработка на их стороне подчиняются их политикам.

8. Рекомендации пользователям

8.1. Минимизируйте ввод: удаляйте ПДн и чувствительные сведения до отправки.
8.2. Используйте placeholder-ы вместо реальных реквизитов (например, `<CLIENT_NAME>`).
8.3. Для изображений — отключайте геометки/EXIF на стороне клиента.
8.4. Не передавайте токены/пароли/ключи доступа в промптах.
8.5. Включайте внутренний ревью промптов перед продакшен-запусками.

9. Инциденты и уведомления

9.1. При выявлении потенциальной передачи ПДн за рубеж в обход NEP запускается процедура реагирования: локализация, анализ журналов, отчёт и корректирующие меры.
9.2. Пользователи уведомляются в разумные сроки, если инцидент затрагивает их интересы и это требуется законом.

10. Экспортный контроль и санкции

10.1. Запрещено использовать API в юрисдикциях/целях, подпадающих под ограничения.
10.2. При наступлении регуляторных запретов DSLab вправе ограничить доступ.

11. Безопасность

11.1. Каналы связи зашифрованы (TLS), доступ к NEP и логам — по принципу наименьших привилегий, ведётся аудит доступа.

11.2. Механизмы детектирования регулярных выражений, NER-модели и правила обновляются по мере развития угроз.

12. Изменения политики

12.1. NEP-политика может обновляться; новая версия публикуется на `/nep-policy`.
12.2. Продолжение использования API означает согласие с обновлениями.