Retencja, eksport i zakończenie usługi CarSpaIQ

CarSpaIQ · wersja 1.11.0 · obowiązuje od 19 listopada 2026 r.

1. Zakres i kanał dyspozycji

Dokument opisuje retencję, eksport, zwrot i usunięcie danych w CarSpaIQ. Dyspozycję może złożyć właściciel organizacji lub należycie umocowana osoba przez biuro@talitha.pl. Przed wykonaniem potwierdzamy tożsamość, uprawnienie, zakres i bezpieczny kanał odbioru; nie prosimy o hasło ani kod MFA.

2. Eksport podczas trwania umowy

Klient może korzystać z eksportów dostępnych w panelu, pobierać własne dokumenty i w zamkniętej alfie zażądać wspomaganego eksportu pozostałych danych. Eksport obejmuje dane przekazane przez klienta oraz dane wytworzone przez jego użycie usługi, w zakresie pozostającym pod jego kontrolą, z wyłączeniem danych innych tenantów, sekretów, wewnętrznych mechanizmów bezpieczeństwa i praw osób trzecich.

Format dobieramy do danych i uzgadniamy przed wykonaniem: w szczególności CSV lub JSON dla danych strukturalnych oraz oryginalne albo powszechnie czytelne formaty plików i PDF. Eksport jest przygotowywany w sposób tenantowy, szyfrowany lub udostępniany krótkotrwałym kanałem i ma termin pobrania. Klient powinien niezwłocznie potwierdzić kompletność i zabezpieczyć własną kopię.

3. Zmiana dostawcy i terminy

Po prawidłowym żądaniu rozpoczniemy współpracę przy zmianie dostawcy i usuniemy techniczne oraz umowne przeszkody pozostające pod naszą kontrolą. Standardowy okres przejściowy nie przekracza 30 dni, chyba że obiektywnie techniczna przeszkoda wymaga uzgodnionego, zgodnego z prawem przedłużenia. Po zakończeniu przejścia dane są dostępne do odbioru przez co najmniej 30 dni, chyba że klient poleci wcześniejsze bezpieczne usunięcie.

W zamkniętej alfie nie pobieramy opłaty za standardowy eksport lub zmianę dostawcy. Nietypowa, indywidualna transformacja może wymagać uprzedniego uzgodnienia zakresu i ceny tylko w zakresie dozwolonym prawem. Od 12 stycznia 2027 r. nie stosujemy opłat za zmianę dostawcy objętych zakazem z Data Act.

4. Zamknięcie i wybór klienta

Klient wybiera zwrot danych i późniejsze usunięcie albo usunięcie bez zwrotu. Po potwierdzeniu kompletności eksportu i zakończeniu wymaganych operacji blokujemy zwykły dostęp, kończymy aktywne procesy i usuwamy lub anonimizujemy aktywne dane, chyba że prawo wymaga zachowania konkretnego zakresu. Sam koniec planu nie powoduje niejawnego usunięcia bez okresu

odbioru.

5. Wyjątki retencyjne i backup

Dane konta i operacyjne są przechowywane przez czas umowy i kontrolowanego wyjścia. Dowody umowy, akceptacji, audytu, rozliczeń, incydentów lub roszczeń mogą pozostać dłużej w minimalnym zakresie wymaganym prawem albo uzasadnionym legal hold. Taki wyjątek nie pozwala ponownie używać danych do zwykłego świadczenia usługi lub marketingu.

Szyfrowane, odseparowane backupy wygasają w skonfigurowanym cyklu nie dłuższym niż 90 dni. Dane oczekujące na wygaśnięcie pozostają niedostępne dla zwykłego runtime; w razie awaryjnego odtworzenia ponownie stosujemy dyspozycję usunięcia. Po zakończeniu cyklu lub bezpiecznym zniszczeniu klucza nie odtwarzamy danych klienta z historycznej kopii.

6. Obowiązki klienta

Klient odpowiada za wskazanie potrzebnego zakresu, legalność dalszego wykorzystania, bezpieczne pobranie, kontrolę kompletności, ochronę własnej kopii i przekazanie danych nowemu dostawcy. Powinien zgłosić brak lub błąd eksportu przed poleceniem nieodwracalnego usunięcia. Po potwierdzonym usunięciu poza retencją ustawową i backupem odzyskanie danych może być niemożliwe.

Zasady w wersji 1.11.0 obowiązują od 19 listopada 2026 r..