RECURRENT · TÜRKIYE

KVKK Notice

Version 0.1 · November 5, 2026
https://recurrentaero.com/legal/en/TR/kvkk

Pre-launch version
Pre-launch version 0.1. These terms take effect for a training centre on the date it signs or accepts them, and for all other users on the date the service opens. No payments are taken under this version yet.

This notice explains, under Article 10 of the Turkish Personal Data Protection Law No. 6698 ("KVKK") and the Communiqué on the Procedures and Principles of the Obligation to Inform, how we process your personal data when you use the Recurrent Platform (Book, Manager and the mobile app). The Turkish text is the governing version.

1. Who is responsible for your data? (Data controller)

- **Name:** Nivorbit Teknoloji Limited Şirketi
- **Address:** Sarıcaeli Köyü, Sarıcaeli Küme Evleri No: 29 İç Kapı No: 109, Merkez / Çanakkale 17100, Türkiye
- **Central registry (MERSİS) no.:** 0631151313600001
- **Trade register:** Çanakkale Ticaret Sicili Müdürlüğü, no. 9575
- **E-mail for personal data requests:** contact@nivorbit.com
- **Web:** https://nivorbit.com

Training centres and corporate buyers (for example airlines) also process data about their customers and staff outside the Platform; their own notices apply to that. For a booking, the training centre processes the data it needs to deliver the training as a separate data controller.

2. Which personal data do we process?

- **Identity:** first and last name; passport and visa details (only if you add them).
- **Contact:** e-mail address, organization, preferred language.
- **Professional:** pilot licence, type ratings, English language proficiency level, proficiency checks (OPC/LPC), training records and logbook entries.
- **Health data (special category):** the class, validity and limitation codes of a medical certificate. **We never ask for a diagnosis or medical detail;** filling in these fields is optional.
- **Customer transactions:** bookings, cancellations, no-show records, disputes, credit balances, booking messages, invoices.
- **Financial:** payment status, card brand and last four digits (the full card number is held only by Stripe), and for training centres their bank account details (stored encrypted).
- **Transaction security:** session data, sign-in times, device notification tokens, IP address and technical logs, audit records.

- **Images and documents:** the documents and photos you upload.
- **AI assistant content:** what you write to the assistant and its answers.

3. Why do we process your data, and on what legal grounds?

- **Creating an account, signing in, organization membership:** establishing and performing a contract (KVKK Art. 5(2)(c)).
- **Search, booking, session-day check-in, cancellation, alternative offers, no-shows and disputes:** performing a contract (Art. 5(2)(c)).
- **Taking, holding in escrow, refunding and paying out payments; issuing invoices and statements:** performing a contract (Art. 5(2)(c)) and legal obligation (Art. 5(2)(ç); tax and commercial law).
- **Verifying training centres (KYB) and reviewing device qualification documents:** legal obligation and legitimate interest (Art. 5(2)(ç), Art. 5(2)(f)).
- **Keeping pilots' documents and checking eligibility at booking:** performing a contract (Art. 5(2)(c)). For medical certificate details, your **explicit consent** (Art. 6(2)) or, where the law provides, Art. 6(3).
- **Notifications (in-app, push, e-mail):** performing a contract (Art. 5(2)(c)). You can switch off notifications not tied to a transaction in settings.
- **Security, abuse prevention, audit records:** legitimate interest and legal obligation (Art. 5(2)(f), Art. 5(2)(ç); Law No. 5651).
- **Support given by the AI assistant:** performing a contract (Art. 5(2)(c)) and legitimate interest (Art. 5(2)(f)).
- **Establishing, exercising and defending legal claims:** Art. 5(2)(e).

We do not use your personal data to build marketing profiles and we do not sell it.

4. Who do we transfer your data to?

- **Training centres:** the centre you book sees what it needs to deliver the training and check you in (name, contact, required documents, booking details).
- **Your organization:** for bookings made for or by your organization, its authorised users see the related records.
- **Payment service provider:** Stripe Payments Europe Ltd. and its affiliates (payments, card storage, fraud prevention, payouts to training centres).
- **Hosting and infrastructure providers:** the providers of our application servers, database, file storage and sign-in server (Keycloak).
- **Notification service:** Google Firebase Cloud Messaging (mobile push notifications).
- **E-mail delivery provider.**
- **AI provider:** Anthropic PBC (to generate the assistant's answers; only the content you share with the assistant and the context it needs).
- **Identity providers:** Google, Apple or your organization's SSO (only if you sign in that way).

- **Competent public authorities:** where they lawfully request it.
- **Legal, accounting and audit advisers.**

5. Is your data transferred abroad?

Some of the providers above (for example Stripe, Google, Anthropic and hosting providers) process data outside Türkiye, in the European Union and the United States. We make these transfers under KVKK Art. 9 (as amended by Law No. 7499, in force since 1 June 2024): to countries with an adequacy decision, or with appropriate safeguards such as the **standard contracts** set by the Board, which are notified to the Personal Data Protection Authority within five business days of signature. In occasional cases without an appropriate safeguard, we rely on the exceptions in Art. 9(6) (for example explicit consent or the performance of a contract).

6. How do we collect your data?

We collect your personal data through the forms on the Platform, the mobile app, the documents you upload, the identity providers you sign in with, your organization's invitations and the training centres' records about your booking, electronically, by automated and partly automated means.

7. How long do we keep your data?

- **Account and profile:** while your account is open; after closure, for the statutory limitation periods.
- **Booking, payment and accounting records, invoices:** at least 10 years under the Tax Procedure Law and the Turkish Commercial Code.
- **Pilot documents:** until you delete them or close your account.
- **Notification tokens:** until you sign out or uninstall the app.
- **Security and access logs:** for the period the law requires (at least 2 years under Law No. 5651).
- **Assistant conversations:** as long as needed to provide the service.

When a period ends, we erase, destroy or anonymise the data under the Regulation on the Erasure, Destruction or Anonymisation of Personal Data.

8. What are your rights under KVKK Article 11?

By applying to the data controller you may:

- learn whether your personal data is processed,
- request information if it is,
- learn the purpose of processing and whether it is used accordingly,
- know the third parties in Türkiye or abroad it is transferred to,
- ask for it to be rectified if incomplete or inaccurate,
- ask for it to be erased or destroyed under the conditions of KVKK Art. 7,
- ask for rectification, erasure or destruction to be notified to the third parties it was transferred to,
- object to a result against you arising solely from automated analysis,

- claim compensation if you suffer damage from unlawful processing.

9. How do you apply?

Following the Communiqué on the Procedures and Principles of Applications to the Data Controller, and stating your identity and request clearly, you may apply:

- by e-mail to **contact@nivorbit.com** from the e-mail address registered on the Platform,
- or in writing to **Nivorbit Teknoloji Limited Şirketi, Sarıcaeli Köyü, Sarıcaeli Küme Evleri No: 29 İç Kapı No: 109, Merkez / Çanakkale 17100, Türkiye**.

We answer free of charge within **30 days**; if the request involves an additional cost, the fee in the Board's tariff may be charged. If your request is refused, you find our answer insufficient or it is not answered in time, you may complain to the Personal Data Protection Board within 30 days of learning the answer and in any case within 60 days of your application.