RECURRENT · EUROPEAN ECONOMIC AREA

Privacy Policy

Version 0.1 · November 5, 2026 · European Economic Area addendum version 0.3
https://recurrentaero.com/legal/en/EEA/privacy

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 policy explains how we collect, use, share and protect your personal data on the Recurrent Platform (Book, Manager and the mobile app). If you are in Türkiye, the KVKK Notice also applies. If you are in the European Economic Area (EEA), the General Data Protection Regulation (GDPR) also applies. We wrote this policy with both in mind. The addendum for your region is shown at the top of the page.

Summary of this Policy

- **We never see or store your card number.**
- **We do not profile you for advertising, we do not sell your data and we make no automated decisions about you.**
- **We process medical certificate details only with your explicit consent.**
- You can exercise your rights of access, rectification, erasure and others by writing to contact@nivorbit.com; we answer within 30 days.

1. Who is responsible for your data?

The data controller is **Nivorbit Teknoloji Limited Şirketi**, Sarıcaeli Köyü, Sarıcaeli Küme Evleri No: 29 İç Kapı No: 109, Merkez / Çanakkale 17100, Türkiye. For any privacy question or request: **contact@nivorbit.com**.

The training centre you book and the organization that books for you process your data as separate controllers, to deliver the training and keep their own records.

2. What data do we collect?

- **What you give us:** name, e-mail, language, organization; documents you choose to add, such as your licence, type ratings, medical certificate class and validity, English proficiency, passport and visa; booking messages; what you write to the assistant.
- **What comes from using the Platform:** bookings, cancellations, payment status, session check-ins, logbook entries, notification preferences.
- **Technical data:** session cookies, IP address, browser and device details, error logs, the mobile push token.
- **From others:** Google, Apple or your organization's SSO (name and e-mail); Stripe (the payment's outcome, the card's brand and last four digits); your organization's invitation and the rights it gives you.

We never see or store your card number; you enter card details directly into Stripe.

3. Why do we use your data? (legal bases under GDPR Art. 6)

- **To provide the service:** your account, search and booking, payment and refunds, cancellations and alternative offers, session day, documents and invoices (performance of a contract, Art. 6(1)(b)).
- **Our legal obligations:** accounting, tax, company verification and answering official requests (Art. 6(1)(c)).
- **Security and fraud prevention:** session security, audit records, detecting abuse (legitimate interests, Art. 6(1)(f)).
- **Improving the service:** debugging and aggregate, non-identifying usage measurements (legitimate interests, Art. 6(1)(f)).
- **Medical certificate details:** for the eligibility check at booking, **only with your explicit consent** (Art. 9(2)(a)). You can withdraw it at any time by deleting the document.

We do not profile you for advertising, we do not sell your data and we make no automated decisions about you. Eligibility checks are for information; the decision to confirm a booking is the training centre's.

4. How does the AI assistant use my data?

To answer you, the assistant (Wilco) sends what you write and the context it needs (for example the devices you are looking at or a summary of your booking) to our AI provider, Anthropic. Under the commercial terms that apply to API customers, Anthropic does not use this content to train its models. Please do not write unnecessary personal or health details to the assistant.

5. Who do we share your data with?

- **Training centres and your organization:** as far as the booking requires.
- **Our service providers (processors):** Stripe (payments), hosting and infrastructure providers, Google Firebase (push notifications), our e-mail delivery provider, Anthropic (assistant). Each processes data only on our instructions and under contract.
- **Authorities:** where the law requires it.
- **Corporate transactions:** if the business running the Platform is transferred to another company, subject to this policy.

6. Is my data transferred abroad?

Some providers process data outside the EEA (for example in the United States). These transfers rely on adequacy decisions (such as the EU–US Data Privacy Framework), the European Commission's Standard Contractual Clauses and, for transfers from Türkiye, the standard contracts under KVKK Art. 9.

7. How long do we keep your data?

We keep data as long as the purpose requires. We keep account data while your account is open; booking, payment and invoice records for the period accounting and tax law requires (at least 10 years); your documents until you delete them; security logs for the period the law requires. After that, we erase

the data or anonymise it.

8. How do we protect your data?

Connections are encrypted with TLS. Session cookies are encrypted and readable only by the server (HttpOnly). Bank account details are encrypted in the database with AES-256. Access is limited by groups and permissions inside each organization; platform administrators' actions are written to an audit log.

9. What are your rights?

You have the right to access, rectify and erase your data, to restrict processing, to object, to data portability and to withdraw consent (GDPR Art. 15–22; KVKK Art. 11). Send your request to **contact@nivorbit.com**; we answer within 30 days. In the EEA you may complain to the data protection authority of your country; in Türkiye, to the Personal Data Protection Board.

10. Children

The Platform is not meant for anyone under 18 and we do not knowingly collect their data.

11. What happens if this policy changes?

We may update this policy. We announce material changes on the Platform or by e-mail. The current version and date are at the top of this page.

Privacy Policy: Addendum AEA

This addendum completes the Privacy Policy for the data of people in the EEA. The GDPR applies to this processing.

AEA-1. Who is responsible for your data?

The controller of your data and the operator of the Platform is **Nivorbit Teknoloji Limited Şirketi**, Sarıcaeli Köyü, Sarıcaeli Küme Evleri No: 29 İç Kapı No: 109, Merkez / Çanakkale 17100, Türkiye. For every privacy question and request: **contact@nivorbit.com**.

AEA-2. Does your data leave the country?

Your data is transferred to Türkiye and to the countries where our service providers are located. The transfer is made to the extent necessary to perform the contract and relies on the applicable transfer tools.

AEA-3. Your medical certificate

The class, validity and restriction codes of a medical certificate are stored; the image is deleted after verification. Before your first medical certificate upload, we ask for your separate, express consent for this information.

AEA-4. AI provider

Our AI provider is Anthropic. No processing takes place without approval.