

Data Processing Agreement (DPA)

Annex to the OpTeamEr platform terms of use — version of 30 September 2026 — aligned with Article 28 of the GDPR and the Swiss Federal Act on Data Protection (FADP). Courtesy translation: the French version prevails.

1. Parties

Controller (the "Customer")	Company name: Address: Represented by:
Processor (the "Provider")	OpTeamEr, a sole proprietorship under Swiss law operated by Furkan Sertdemir, Chemin de Mochettaz 10B, 1030 Bussigny (Vaud), Switzerland — info@opteamer.com

2. Subject matter and duration

This agreement governs the processing of personal data carried out by the Provider on behalf of the Customer in the course of using the OpTeamEr platform (opteamer.com website and app.opteamer.com application): scheduling, working time, leave and HR document management. It applies for the whole duration of the terms of use and until the data is erased in accordance with Section 9.

3. Nature and purpose of the processing

Hosting, storage, display, computation (hours, leave balances, payroll variables), notification (emails, push notifications) and export of data, solely to provide the service to the Customer. The Provider processes data only on the Customer's documented instructions, evidenced by the use of the platform and this agreement.

4. Categories of data and data subjects

Data subjects	The Customer's employees, managers and administrators; people invited to the platform.
Categories of data	Identity and contact details (name, email, phone, date of birth); employment data (position, location, contract type, hours, hourly rate, schedules, clock-ins, leave, certifications, training); HR documents uploaded by the Customer; technical data (push subscription identifier, activity logs); GPS position at clock-in when the Customer enables that option.
Special categories	None is required by the service. Absence supporting documents uploaded by the Customer (for example medical certificates) remain under its sole responsibility.

5. Obligations of the Provider

- Process the data only for the purposes in Section 3 and on the Customer's instructions; inform the Customer if an instruction appears to infringe applicable law.
- Ensure that persons authorised to process the data are bound by confidentiality.
- Implement the security measures in Section 7.
- Assist the Customer, as far as possible, in responding to data subject requests (access, rectification, erasure, restriction, portability, objection).

- Assist the Customer in meeting its security, breach notification and impact assessment obligations, taking into account the information available to the Provider.
- Notify the Customer of any personal data breach without undue delay after becoming aware of it, with the information needed for the Customer's own notifications to the authority and to data subjects.
- Make available the information necessary to demonstrate compliance with this agreement and allow reasonable audits (Section 8).

6. Sub-processors and transfers

The Customer gives general authorisation for the following sub-processors: cloud hosting provider of the application (data hosted in the European Union), delivery network of the marketing website, Stripe (payments), email delivery provider. The current named list is available on request at info@opteamer.com. The Provider informs the Customer of any addition or replacement with 30 days' notice; the Customer may object on legitimate grounds by terminating the contract. The Provider imposes equivalent data protection obligations on its sub-processors. Any transfer outside the European Union or Switzerland relies on a recognised mechanism (adequacy decision or standard contractual clauses).

7. Security measures

- Encryption in transit (TLS) and at rest by the hosting provider.
- Per-company isolation enforced server-side on every request; role-based access control (administrator, manager, employee).
- Individual authentication with email and password; time-limited sessions; immediate account suspension by the administrator.
- Log of sensitive actions with author and date.
- Backups managed by the hosting provider; full data export available to the Customer at any time.
- Vulnerability reports handled within 3 business days.

8. Audit

At most once a year and with 30 days' notice, the Customer may request the information needed to demonstrate compliance with this agreement, or have an audit carried out by an independent third party bound by confidentiality, at its own expense, during business hours and without disrupting the service.

9. End of processing

At the end of the contract, the data remains exportable by the Customer for 30 days. After that period the Provider deletes the data, unless retention is required by law. The Customer may also delete its account in self-service from the application.

10. Governing law

This agreement is governed by Swiss law. Mandatory provisions of the law of the Customer's country of establishment, in particular the GDPR for a Customer established in the European Union, remain reserved. In case of conflict with the terms of use, this agreement prevails for all data protection matters.

For the Customer

Name, role, date, signature

For OpTeamEr

Furkan Sertdemir

Date, signature

