apron:pilot

Data Processing Agreement (DPA)

pursuant to Art. 28 General Data Protection Regulation (GDPR)
Version: December 2026, effective from: [Stichtag = Go-live 1.5.0]
This is a translation of the German version; in case of doubt, the German version prevails.

between

the **group** using the apron:pilot application (flying club, flight school, co-ownership or aircraft owner), represented by the administrator who accepts this agreement – hereinafter the **Controller** –

and

apron:pilot Aviation Software e.U., Rosenberggürtel 39, 8010 Graz, Austria, FN 557470i – hereinafter **apron:pilot** or the **Processor** –.

1 Subject Matter and Duration

1.1. apron:pilot provides the Controller with the apron:pilot application in accordance with the Terms of Use and, for paid modules, the Terms of Service (hereinafter the Main Agreement). In doing so, apron:pilot processes on the Controller's behalf personal data that the Controller records in the application about its members and other persons.

1.2. This agreement applies for the entire duration of the Controller's use of the application and ends with the deletion of the group.

1.3. The agreement is concluded when an administrator accepts it on behalf of the group: at registration or, for existing groups, at the next login of an administrator. The administrator thereby confirms that they are authorised to represent the group. The acceptance of one administrator applies to the whole group.

1.4. In the event of contradictions, the provisions of this agreement take precedence over those of the Main Agreement in matters of data protection.

2 Nature, Purpose and Scope of the Processing

2.1. **Purpose:** provision, operation, maintenance, backup and support of the application for organising the Controller's flight operations, members, aircraft, invoicing and training.

2.2. **Nature of the processing:** collecting, storing, organising, displaying and evaluating within the functions of the application, sending e-mails, transmitting to destinations specified by the Controller (e.g. exports to SFTP or WebDAV destinations), backing up, restoring and deleting.

2.3. **Categories of data subjects:** members of the group (administrators, users, instructors, examiners, student pilots), emergency contacts of the members, invoice recipients and other persons the Controller records in the application (e.g. speakers, course participants).

2.4. **Categories of personal data:** depending on use and subscribed modules, in particular

2.4.1. master and contact data of the members: name, e-mail address, address, telephone numbers, profile picture, role and functions, customer number, billing address, notification settings, last login to the group,

2.4.2. emergency contacts,

DRAFT

2.4.3. ratings, check flights and information on medical certificates (type and validity),

2.4.4. reservations including the waiting list and calendar subscription,

2.4.5. logbook and flight data: flights, times, aerodromes, pilot, supervising instructor,

2.4.6. data on aircraft, maintenance and defects including the reporting person,

2.4.7. information, messages and NOTAMs,

2.4.8. invoicing data: invoices, credit notes, bank details, payment runs (SEPA),

2.4.9. training data (TRAINING module): student files, training status, learning points, assessments, debriefings, feedback, courses, sessions, acceptances and declines, attendance, announcements, documents and files, exports,

2.4.10. e-mails of the application to the members, with recipients, subject, time and delivery status.

2.5. **Special categories:** Information on medical certificates may be health data within the meaning of Art. 9 GDPR. apron:pilot protects it with the measures described in Annex 2, in particular through encryption and role-based access. The Controller is responsible for the existence of a legal basis.

2.6. **Place of processing:** Processing takes place in the European Union. Processing in third countries only takes place through the sub-processors listed in Annex 1 and only under the conditions of Art. 44 et seq. GDPR.

3 Obligations of the Controller

3.1. The Controller is responsible for the lawfulness of the processing, in particular for recording the data of its members and other persons lawfully, informing them and, where necessary, obtaining consents, such as that of the parents or legal guardians of minor users.

3.2. Through its settings in the application, the Controller determines who within the group sees and edits which data, and assigns roles and functions with care.

3.3. The Controller informs apron:pilot without undue delay if it detects errors or irregularities in the processing.

4 Instructions

4.1. apron:pilot processes the data only on documented instructions from the Controller, unless apron:pilot is required to process it by Union or Member State law; in that case, apron:pilot informs the Controller of that legal requirement before processing, unless that law prohibits such information.

4.2. If an authority or a court demands that apron:pilot disclose data of the Controller, apron:pilot informs the Controller without undue delay, where legally permitted, and refers the authority to the Controller.

4.3. The Controller's instructions are conclusively laid down in this agreement and in the Main Agreement and are given by using the functions of the application (e.g. recording, changing, deleting, exporting data, settings). Further instructions are given by an administrator by e-mail to dataprivacy@apron-pilot.com. apron:pilot carries out instructions that go beyond the scope of services of the Main Agreement against payment for the effort, after sending a quote in advance and receiving the Controller's consent.

4.4. If apron:pilot considers that an instruction infringes data protection provisions, apron:pilot informs the Controller without undue delay and may suspend its implementation until it is confirmed or changed.

5 Obligations of apron:pilot

5.1. **Confidentiality:** apron:pilot ensures that all persons who have access to the data are committed to confidentiality in writing before taking up their activity or are under a statutory obligation of confidentiality. The commitment continues after the end of their activity.

DRAFT

Currently, only the owner of apron:pilot has access.

5.2. **Security:** apron:pilot takes the technical and organisational measures pursuant to Art. 32 GDPR described in Annex 2. apron:pilot may adapt these measures to the state of the art, provided the level of protection is not reduced.

5.3. **Access to data:** apron:pilot only accesses the Controller's data insofar as this is necessary for operation, troubleshooting, backup or a support request from the Controller.

5.4. **Record:** apron:pilot keeps a record of processing activities pursuant to Art. 30(2) GDPR.

5.5. **Use for own purposes:** apron:pilot does not use the data for its own purposes. An exception is the evaluation in anonymised and aggregated form pursuant to point 5.5 of the Terms of Use, which does not allow any conclusions about individual groups or persons.

6 Assistance to the Controller

6.1. Rights of data subjects: apron:pilot assists the Controller in fulfilling requests for access, rectification, erasure, restriction, data portability and objection primarily through the functions of the application (editing, deleting, exporting). apron:pilot designs the application so that the Controller can fulfil these requests within the statutory deadlines. If a data subject contacts apron:pilot directly, apron:pilot forwards the request to the Controller without undue delay and informs the data subject of this. apron:pilot provides assistance going beyond the functions of the application against payment for the effort and after sending a quote in advance.

6.2. Personal data breaches: apron:pilot informs the Controller without undue delay, at the latest within 72 hours after becoming aware of a personal data breach, by e-mail to the administrators and to the office e-mail address of the group. The information contains, as far as known, the nature and extent of the breach, the categories of data and persons concerned, the likely consequences and the measures taken. Information not yet available is provided subsequently.

6.3. Taking into account the nature of the processing and the information available to it, apron:pilot assists the Controller in complying with its obligations under Art. 32 to 36 GDPR: security of processing, notification of personal data breaches to the supervisory authority, communication to the data subjects, data protection impact assessment and prior consultation of the supervisory authority. apron:pilot provides assistance going beyond the information under point 6.2 and the functions of the application against payment for the effort and after sending a quote in advance.

7 Sub-processors

7.1. The Controller consents to the use of the sub-processors listed in Annex 1. apron:pilot contractually binds each sub-processor to data protection obligations corresponding to this agreement. If a sub-processor fails to fulfil its data protection obligations, apron:pilot remains liable to the Controller for the performance of these obligations (Art. 28(4) GDPR).

7.2. apron:pilot informs the administrators by e-mail at least 14 days in advance before a new sub-processor is engaged or an existing one is replaced. If the change has to be made at short notice due to an error, an outage or for security reasons, apron:pilot informs them without undue delay.

7.3. The Controller may object to the change for an important reason under data protection law within 14 days of the information by e-mail to dataprivacy@apron-pilot.com. In the event of an objection, the Controller may end the use of the application and this agreement free of charge; for ongoing subscriptions, the fee for the remaining term is refunded pro rata.

DRAFT

7.4. Service providers that have no access to personal data (e.g. for monitoring availability) are not sub-processors.

8 Evidence and Audits

8.1. On request, apron:pilot provides the Controller with all information necessary to demonstrate compliance with this agreement, in particular this description of the technical and organisational measures, the list of sub-processors and their certifications and evidence (e.g. the ISO/IEC 27001 certification of the data centre operator).

8.2. The data is processed exclusively in the data centres of the sub-processors; apron:pilot does not maintain any premises of its own in which data is processed or stored. Audits are therefore carried out by providing information and evidence pursuant to point 8.1. Further audits, for example by an auditor commissioned by the Controller and bound to confidentiality, must be agreed in writing; the costs are borne by the Controller.

9 End of Processing, Deletion

9.1. The Controller can retrieve its data at any time during use with the export functions of the application in common formats (e.g. CSV, Excel, PDF). After the end, it can choose whether its data is deleted or returned to it beforehand; the return takes place via these export functions and, for the TRAINING module, additionally in accordance with point 10.3 of the Terms of Service. apron:pilot provides any return going beyond this against payment for the effort and after sending a quote in advance.

9.2. After the end of use – through deletion of the group at the request of an administrator, through deletion due to inactivity (point 3.8 of the Terms of Use) or through termination of free use (point 3.6 of the Terms of Use) – apron:pilot deletes all personal data of the Controller, unless there is a legal obligation to retain it. For the end of paid modules, the Terms of Service additionally apply.

9.3. The data is removed from the backups when their retention period expires, at the latest after 12 months. Until then, it is only accessed to restore the entire system.

9.4. On request, apron:pilot confirms the deletion by e-mail.

10 Liability, Final Provisions

10.1. Liability is governed by point 6 of the Terms of Use, unless Art. 82 GDPR mandatorily provides otherwise.

10.2. apron:pilot notifies the administrators of changes to this agreement; they take effect when an administrator accepts them at their next login. Changes to the list of sub-processors are made in accordance with point 7.

10.3. **Controllers outside the EU:** If the Controller has its registered office in Switzerland, this agreement also constitutes an agreement on processing by a processor pursuant to Art. 9 of the Swiss Federal Act on Data Protection (FADP). References to the GDPR are to be read as references to the corresponding provisions of the FADP; the competent supervisory authority in this respect is the Federal Data Protection and Information Commissioner (FDPIC). For Controllers with their registered office in the United Kingdom, this applies accordingly to the UK GDPR.

10.4. Austrian law applies. In all other respects, the final provisions of the Terms of Use apply. Should a provision of this agreement be invalid, the remaining provisions remain valid.

Annex 1: Sub-processors

DRAFT

Sub-processor	Service	Place of processing	Basis for third country
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Germany	server, database, files, backups (Storage Box)	Germany, Falkenstein data centre	–
World4You Internet Services GmbH, Wolfgang-Pauli-Straße 2, BT3, 4020 Linz, Austria	mailboxes of apron:pilot (e.g. contact@, support@, dataprivacy@ etc.) receiving support requests with data of the group	Austria	–
Brevo SAS, 9–17 rue Salneuve, 75017 Paris, France (RCS Paris 498 019 298)	sending the e-mails of the application, delivery status	EU	–
Laravel Holdings Inc. (Laravel Forge), 60 Broad Street, 24th Floor #1559, New York, NY 10004, USA	management, updating and provisioning of the server (access to the server possible)	USA	EU-US Data Privacy Framework (also UK and Swiss-US DPF)
Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA	protection of registration against bots (Turnstile)	USA	EU-US Data Privacy Framework

Annex 2: Technical and Organisational Measures (Art. 32 GDPR)

Confidentiality

- **Physical access control:** The servers are located in data centres of Hetzner Online GmbH in Germany with access control, video surveillance and security staff; the data centre is certified to ISO/IEC 27001. apron:pilot does not operate any servers or storage systems of its own.
- **System access control:**
    - Access to the server only via SSH keys, no password login.
    - Two-factor authentication for all administrative accounts (hosting, server management, payment provider, e-mail sending, bot protection).
    - The database is only available locally on the server and cannot be reached from outside.
    - Firewall on the server; only the ports needed for operation are open.
    - apron:pilot's work devices are protected by an encrypted hard drive and an automatic screen lock; personal data from operation is only worked with locally in the context of a support request.
- **Data access control:**
    - Only the owner of apron:pilot has access to the server and the data.

DRAFT

    - In the application, the data of each group is separated from that of other groups; users only see the data of their group and only to the extent their role permits.
    - Passwords are stored exclusively as an irreversible hash value.

- **Separation control:** tenant separation in the application; separate systems for development, testing and production; no real data is used in testing.
- **Pseudonymisation and encryption:**
    - Transmission encrypted throughout (TLS/HTTPS).
    - Personal data is additionally stored in encrypted form in the database; this applies in particular to contact details, information on medical certificates and recipient details in the e-mail log.
    - Access credentials for SFTP and WebDAV destinations are stored in encrypted form.
    - Logs contain as little personal data as possible; e-mail addresses are made unrecognisable in them.

Integrity

- **Transfer control: t**ransfers only in encrypted form; exports to destinations of the group only via encrypted protocols (SFTP, WebDAV over HTTPS); protection against requests to internal addresses.
- **Input control:** In the TRAINING module, all changes to student files, courses and course sessions are recorded with the user, time and content of the change in an unalterable history. In the other areas, certain operations are logged (e.g. changes to invoiced logbook entries with a reason, cancellation and sending of invoices, offsetting of credits, sending of NOTAMs, deleted reservations with a reason); otherwise the creator and the last editor are stored.

Availability and Resilience

- Daily encrypted backup of the database and the uploaded files to a storage system separate from the server within the same data centre network (Hetzner Storage Box); retention up to 12 months (30 daily, 8 weekly, 12 monthly backups).
- Monitoring of the availability of the application and notification in the event of an outage.
- Data centre with uninterruptible power supply, fire protection and data-protection-compliant disposal of data carriers by the operator.
- Reporting procedure for personal data breaches pursuant to point 6.2.
- Regular security updates of the operating system, runtime environment and libraries used.
- Fonts, icons and scripts are loaded from our own server, not from third-party providers; the only exception is Cloudflare Turnstile on the registration page (see Annex 1).

Procedure for Regular Review

DRAFT

- Review of the measures in the event of significant changes to the application, at least annually.
- Automated tests and static code analysis before every release of a new version.
- Selection of sub-processors based on their security evidence (e.g. ISO/IEC 27001) and conclusion of a data processing agreement with each of them.
- Privacy-friendly default settings: users can decide themselves whether their contact details are visible to other members; automatic deletion of exports after 180 days, of activity entries after 13 months and of entries in the e-mail log after 3 years.

DRAFT