PRACTICLE

Standard data processing agreement (DPA)

for use of Practicle

Version	1.1
Effective from	16 September 2026
Language	English
Generated	31 October 2026

This standard data processing agreement (hereinafter referred to as “the Agreement”) governs the processing of personal data carried out in connection with the delivery and use of the Practicle software solution.

The parties:

The Customer (as defined in the Main Agreement, the licence order or the electronic account creation) (hereinafter referred to as “the Controller”)

Practicle

Snerlehaven 1, 2630 Tåstrup, Danmark

CVR no.: 27353606

Email: support@practicle.dk

(hereinafter referred to as “the Processor”)

Each referred to as a “Party” and collectively “the Parties”.

1. Purpose, subject matter and contractual basis

1.1. The Agreement sets out the rights and obligations of the Parties in the Processor’s processing of personal data on behalf of the Controller pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), in particular Article 28.

1.2. The Agreement also supports the Controller’s supply-chain security obligations under Directive (EU) 2022/2555 of the European Parliament and of the Council (the NIS2 Directive).

1.3. This Agreement constitutes an integral annex to the parties' contractual basis for the delivery and use of Practicle ("the Main Agreement"). In the event of conflict between the provisions of the Main Agreement and this Agreement regarding the processing and protection of personal data, this Agreement prevails.

2. Scope according to operating model (SaaS vs. On-Premises)

2.1. SaaS / Cloud delivery: For Practicle as a SaaS/cloud solution, the Processor is operationally responsible for the hosting infrastructure. In this model the Processor acts as data processor for all personal data that the Controller or its users load, create or generate in the application.

2.2. On-Premises special installation: In a paid special installation the platform is installed and operated in the Controller's own infrastructure. The Processor has no standard access to data and does not act as data processor in day-to-day operations. In this operating model this Agreement applies only if the Controller expressly requests technical assistance, support or troubleshooting that involves access to personal data.

3. Data ownership and instructions

3.1. Ownership: All data, including personal data, that the customer creates or uploads in Practicle belongs exclusively to the Controller.

3.2. Documented instructions: The Processor may process personal data only on documented instructions from the Controller, unless otherwise required by EU law or the national law of the Member States. The Main Agreement, this DPA, the system's configuration choices and the Controller's ongoing use of the platform constitute the complete instructions.

3.3. Conflicting instructions: The Processor shall immediately notify the Controller if an instruction, in the Processor's assessment, infringes the GDPR or other data protection law.

4. Confidentiality and access restriction

4.1. Confidentiality: The Processor ensures that all persons authorised to access personal data have committed themselves to confidentiality in writing or are under a statutory duty of confidentiality.

4.2. Need-to-know: The Processor's employees access customer data only when strictly necessary to provide technical support, troubleshooting or agreed assistance. All administrative access is logged.

5. Processing security and NIS2 supply-chain security

5.1. Technical and organisational measures: The Processor implements and maintains appropriate technical and organisational measures pursuant to GDPR Article 32 to ensure a level of security appropriate to the risks. The measures are specified in Annex B.

5.2. NIS2 compliance (Supply Chain Risk Management): To support the Controller's statutory management of cybersecurity risks in the supply chain, the Processor guarantees:

- Use of ISO 27001-certified hosting infrastructure within the EU (Germany).
- Ongoing system hardening, firewall protection, vulnerability management and validation of server-side API input against injection and web attacks.
- Robust access control with support for Keycloak SSO, LDAP, 2FA and protection against brute force and credential stuffing via rate limiting.
- System support in Practicle for managing frameworks, controls and periodic audits (using Practicle Compliance).

6. Use of sub-processors

6.1. General prior authorisation: The Controller gives general prior authorisation for the Processor to use sub-processors to fulfil the delivery. Approved sub-processors are listed in Annex C.

6.2. Notice of changes: The Processor shall give the Controller at least 30 days' written notice (by email or a notice in the platform) before adding or replacing a sub-processor. The Controller has the right to raise a reasoned, objective objection within the notice period.

6.3. Sub-processor obligations: The Processor shall impose the same data protection and security requirements on sub-processors as the Processor is subject to under this Agreement.

6.4. Third-country transfers: Processing and storage take place within the EU/EEA. Any transfer to third countries may only take place in compliance with GDPR Chapter V.

7. Security incidents and personal data breaches

7.1. Notification duty: The Processor shall notify the Controller without undue delay and no later than 24 hours after becoming aware of a confirmed or suspected personal data breach.

7.2. Content of the notification: The notification shall as a minimum describe the nature of the incident, the categories of data concerned, the approximate number of data subjects, likely consequences and measures taken/proposed to mitigate the incident.

7.3. Incident handling: The Parties shall cooperate in good faith to mitigate security incidents and to provide the documentation needed for supervisory authorities or affected parties.

8. Assistance to the Controller

8.1. Data subject rights: The platform provides functionality enabling the Controller independently to fulfil requests for access, rectification, restriction, objection, export and erasure.

8.2. Direct erasure requests: If data subjects contact the Processor directly, they are referred to the Controller's administrator, see Practicle's data deletion policy.

8.3. DPIA and supervision: The Processor shall assist the Controller to the necessary and reasonable extent with information for data protection impact assessments (DPIA) and any prior consultations with supervisory authorities, cf. GDPR Articles 35 and 36. Assistance is limited to providing information and technical documentation that the Processor already holds and that is necessary for the assessment. If the assistance requires separate time or adaptation by the Processor, it is billed on a time-spent basis at the Processor's then-current hourly rate, unless otherwise expressly agreed.

9. Audit, documentation and inspection

9.1. Documentation: The Processor shall make all necessary documentation of compliance with GDPR Article 28 and this Agreement available to the Controller.

9.2. Supervision and audit: The Controller or an independent auditor authorised by the Controller has the right to inspect processing security with at least 14 working days' prior notice during normal business hours. Inspections must not disrupt operations or provide access to other customers' data. The Controller bears all costs associated therewith, and assistance from the Processor that exceeds provision of existing standard documentation is billed on a time-spent basis.

10. Termination, export and erasure

10.1. Ongoing data export and snapshots: The Controller has at all times during the agreement period access via the administration module to extract a complete export or take a snapshot of its entire database.

10.2. Erasure upon termination: Upon termination of the Main Agreement for the SaaS delivery, the Processor shall delete all of the customer's personal data and existing data copies no later than 30 days after expiry of the agreement, unless EU or national law requires continued

storage. Technical backups are overwritten automatically according to the fixed rotation cycle (maximum 30 days).

Annex A: Instructions for processing personal data

A.1. Purpose and processing activities

The purpose of the processing is to make the ITSM and management platform Practicle available as SaaS, and by separate agreement as support for an On-Premises special installation. Processing includes storage, recording, structuring, retrieval, display, case management (service desk/support), configuration management (CMDB), task management, documentation archiving, password management and management of compliance requirements (e.g. NIS2 frameworks).

A.2. Categories of data subjects

- The Controller’s employees, administrators, consultants and IT users.
- The Controller’s end users, customers, suppliers or external partners who contact support or are registered in the system’s modules.

A.3. Categories of personal data

Ordinary personal data:

- Identification and master data: Name, username, company name, job title, department.
- Contact details: Email addresses, telephone numbers, address.
- System and network data: IP addresses, browser and device information, login history, user roles, action and audit logs.
- Case and process data: Content of support tickets, internal notes, project data, CMDB relations and user-uploaded documents.
- Encrypted access credentials: Passwords and API keys when using the password management module.

Special categories of personal data (sensitive data):

Practicle is not, as a starting point, intended for the processing or storage of special categories of personal data as referred to in GDPR Article 9. The Controller should therefore not use the platform for such data unless this has been separately agreed. This does not change the Processor’s statutory obligations under the GDPR, including Articles 28 and 32, and this Agreement. The Processor remains subject to those obligations for the processing the Processor actually carries out, including if the Controller enters such data into the platform.

A.4. Duration of processing

Processing continues for as long as the Main Agreement is in force.

Annex B: Technical and organisational security measures

Infrastructure and hosting (Hetzner, Nuremberg, Germany):

- The server infrastructure is located in ISO/IEC 27001-certified data centres in Nuremberg, Germany.
- Physical security includes 24/7 monitoring, access control systems, redundant power supply (UPS/diesel generators) and climate control.

Architecture and logical data separation:

- Multi-tenant architecture with PostgreSQL as the primary database.
- Logical data separation ensuring that each customer's data is isolated.
- Parameterised queries and server-side validation to prevent SQL injection and data leakage.
- Secure web headers implemented (including CSP – Content Security Policy and HSTS – HTTP Strict Transport Security).

Access control, identity management and authentication:

- Support for Keycloak SSO integration for Single Sign-On, multi-factor authentication and enterprise identity governance.
- Option for local two-factor authentication (2FA) and Active Directory / LDAP integration.
- Granular, role-based access control (RBAC) down to module and field level.
- Passwords are protected with strong hashing and salting.
- Automatic session timeout and CSRF protection.
- Rate limiting at network and application level (IP blocking, file-based burst protection and automatic account lockout after repeated failed login attempts).

Network security, hardening and monitoring:

- Network firewall that only allows traffic on required ports and filters scans and brute-force attempts.
- System hardening with only strictly necessary services exposed and ongoing rollout of OS and security updates.
- A custom monitoring engine that watches server load, latency, API errors and database health with automatic operational notification on deviations.

- Full audit logging of all key changes, administrative actions and login sequences with timestamps for traceability.

Encryption:

- In transit: All data in transit between client and server is encrypted via TLS/HTTPS.
- At rest: Databases, backups and passwords in the password management module are stored strongly encrypted.

Backup, recovery and customer-controlled operations:

- Automatic hourly backups with 3 days of history.
- Automatic daily backups with 30 days of history.
- Backups are actively monitored for completion and validated for integrity, with an alert to the operations team on failure.
- Customers can generate snapshots before changes/upgrades and restore via a guided restore flow.

Annex C: Approved sub-processors

Sub-processor	Hetzner Online GmbH
CVR / Reg. no.	DE 812873730
Service / Delivery	Hosting of server infrastructure, PostgreSQL database, firewalls and backup storage
Data centre location	Nuremberg, Germany
Legal basis / Transfer	Within the EU/EEA (ISO 27001-certified)

For On-Premises special installations where the customer operates the software itself, no sub-processors are used for hosting the customer's production data.

Annex D: System contacts and incident handling

- Customer service & technical support: support@practicle.dk
- Enquiries regarding data deletion & rights: support@practicle.dk (see Practicle's data deletion policy)
- Reporting of security breaches (GDPR Article 33 / NIS2 notification):
  - Email: security@practicle.dk / support@practicle.dk

- Notification deadline for a confirmed breach: Without undue delay and no later than 24 hours.