Privacy Policy (Apps)

2026-02-07 - Valid from 2026-02-07

Privacy Policy (Apps / SaaS)

1. Controller

Benjamin Wenzel SoluForge (sole proprietorship)

Owner: Benjamin Wenzel

Kolonnenstraße 8

10827 Berlin

Germany

Email (privacy): **privacy@craftifact.com**

2. Scope

This privacy policy applies to the processing of personal data when using the **Craftifact SaaS platform** (web app, APIs, identity service, and managed instance hosts), in particular at:

- app.soluforge.de (Craftifact application)
- iam.soluforge.de (identity and login service)
- managed Craftifact SaaS instance hostnames provided to Customers
- related technical endpoints (APIs) required to use the Service

It does not apply to:

- the marketing website craftifact.com (separate privacy policy)
- the online shop/checkout (separate privacy notices for the online shop)
- the website soluforge.de (separate privacy notices)

3. Roles under GDPR (Customer and SoluForge)

Craftifact is a B2B service. Depending on the data category, SoluForge may act in different roles:

1. **Processing on behalf (Art. 28 GDPR)**
   Where Craftifact processes personal data that the Customer processes as part of using the Service (e.g. user management within the Customer tenant, content/metadata, audit events), SoluForge typically acts as a **processor**. In this case, the respective Customer is the controller.

2. **SoluForge as controller**
   SoluForge processes certain data under its own responsibility, in particular:

- data for **contract performance** (e.g. contact persons, administrative contact, communication)
- data for **security, abuse prevention, and operational stability** (e.g. technical logs, monitoring and security events), to the extent such processing is not performed exclusively on the Customer's instructions

Where SoluForge acts as a processor, the Data Processing Agreement (DPA) additionally applies.

4. Categories of Data Processed

When using the SaaS platform, the following personal data may be processed in particular:

4.1 Identity and account data

- name (if provided by the Customer/IAM)
- business email address
- username / user ID
- tenant assignment
- if applicable, organization/team assignment

4.2 Authentication and authorization data

- roles, permissions, group memberships (RBAC)
- SSO/IdP references (e.g. realm/client information, claim references)
- session/token information (technically required identifiers)

4.3 Usage, security, and audit logs

- login timestamps, logout timestamps
- failed login attempts and blocking/protection events
- timestamps and details of administrative actions (e.g. role changes, user creation, policy changes), where technically provided
- API access (timestamp, endpoint, status code, and, where applicable, request metadata)
- access logs for app, IAM, and managed instance hosts, including timestamp, source IP address, host or service name, HTTP method, URL path, and response status code
- service and infrastructure metadata required for operations, such as instance or customer identifiers, container/service name, severity, and application log messages where applicable

- IP address and technical connection data (to the extent required for security/error analysis; may be truncated/anonymized depending on system configuration)

For central Caddy access logs, SoluForge does not intentionally store request query strings, request headers, cookies, or request bodies.

4.4 Customer data (data provided through usage)

- artifacts, metadata, configurations, permission assignments
- logs/audit events within the tenant
- other content that users store/transmit as part of using the Service

Note: Craftifact is generally not designed to process **special categories of personal data** (Art. 9 GDPR). The Customer is responsible for ensuring that such data are processed only where lawful and with appropriate additional safeguards.

5. Purposes of Processing

Processing is carried out in particular for the following purposes:

- providing the SaaS platform and its features (web app, APIs)
- authentication, authorization, and tenant separation (tenant operation, RBAC)
- operational security, protection against abuse/attacks, incident handling
- error analysis, performance monitoring, stability and capacity management
- support handling (intake, diagnosis, remediation)
- fulfilling contractual obligations towards Customers
- ensuring traceability of security-relevant events (audit and logging features)

6. Legal Bases

Depending on role and processing context, the following legal bases apply in particular:

6.1 Processing as processor (Art. 28 GDPR)

The Customer’s legal basis is typically Art. 6(1) GDPR (e.g. (b), (f)) or other applicable provisions. As a processor, SoluForge processes data on the Customer’s documented instructions in accordance with the DPA.

6.2 Processing under SoluForge’s own responsibility

- Art. 6(1)(b) GDPR (performance of a contract / pre-contractual measures), e.g. provision and administration of the Service towards the Customer
- Art. 6(1)(c) GDPR (legal obligations), where applicable
- Art. 6(1)(f) GDPR (legitimate interests), in particular in secure and stable operation, abuse prevention, attack detection, traceability, and error analysis

7. Recipients and Categories of Recipients

Recipients of personal data may include:

- SoluForge personnel bound by confidentiality (need-to-know)
- technical service providers (hosting/infrastructure) as processors (Art. 28 GDPR), where required
- in support cases: communication via support channels (e.g. email) to the extent necessary
- authorities/public bodies where SoluForge is legally obliged to do so

8. Sub-processors

Where SoluForge acts as a processor, sub-processors may be engaged. The current sub-processor list as set out in the DPA applies.

Currently (based on your materials): hosting/infrastructure in Germany.

9. International Data Transfers

Transfers of personal data to countries outside the EU/EEA take place only in compliance with the requirements of Art. 44 et seq. GDPR (e.g. adequacy decision or appropriate safeguards).

Currently, no regular international transfer is planned for operating the SaaS platform.

10. Cookies, Sessions, and Local Storage

For operating the SaaS platform, **technically necessary** mechanisms are used, in particular:

- session/authentication information (e.g. session cookie or token reference) required to recognize logged-in users and provide the Service
- security-relevant settings (e.g. CSRF protection, session security)
- where applicable, local storage to store technical UI settings (e.g. theme)

These technologies are used exclusively for operation, security, and providing features expressly requested by the user.

Legal bases:

- where applicable, technically necessary device access under applicable local law
- Art. 6(1)(b) GDPR (contract performance) and/or Art. 6(1)(f) GDPR (operation/security)

11. Retention and Deletion

11.1 Customer and tenant-related data (processing on behalf)

Retention depends on the main agreement and the DPA. Export and deletion timeframes follow the contractual provisions (in particular export/deletion after contract termination).

11.2 Logs and security data (operation/security)

Central operational and access logs used for platform operation and security are generally retained for **14 days** and are then deleted unless legal obligations or a concrete security incident require longer preservation. Security and operational logs are stored only as long as necessary for:

- attack detection and abuse prevention
- error analysis and evidence of stability
- forensic investigation of security incidents

and are then deleted or anonymized unless legal obligations require otherwise.

Note: specific retention periods may vary depending on data category and the security situation (e.g. shorter periods for pure performance logs, longer for security-relevant tenant audit events or incident evidence).

12. Data Subject Rights

12.1 Where SoluForge is a processor

Data subjects (e.g. users of a Customer tenant) should generally contact the **respective controller (Customer)** to exercise their rights (Art. 15–21 GDPR), as the Customer determines the purposes and means of processing.

SoluForge supports the Customer in fulfilling data subject rights in accordance with the DPA.

12.2 Where SoluForge is a controller

Where SoluForge processes data under its own responsibility (e.g. contract/contact data and certain security/operational data), data subject rights can be asserted with SoluForge at: **privacy@craftifact.com**.

13. Data Security

SoluForge implements appropriate **technical and organizational measures** to protect personal data against loss, manipulation, unauthorized access, or unauthorized disclosure. Details may follow from the TOMs described in the DPA and from security concepts.

14. Support and Administrative Access

In support cases, it may be necessary for SoluForge to access tenant-related information to analyze and remedy issues. Such access takes place:

- only to the extent necessary (need-to-know)
- with consideration of role/permission models and available logging
- within the contractual arrangements (in particular the DPA) where processing on behalf is involved

15. Automated Decision-Making / Profiling

As a rule, the SaaS platform does not carry out automated decision-making, including profiling, under Art. 22 GDPR.

16. Right to Lodge a Complaint

You have the right to lodge a complaint with a data protection supervisory authority. For Berlin:

Berlin Commissioner for Data Protection and Freedom of Information

Alt-Moabit 59–61

10555 Berlin

17. Changes to this Privacy Policy

We update this privacy policy as needed, in particular in case of changes to processing, security requirements, or legal obligations. The current published version applies.