Data Processing Agreement pursuant to Article 28 GDPR

between

Controller
the respective customer of ROESSOLYTICS
- hereinafter “Controller” -

and

Processor
ROESSOLUTIONS®
Benjamin Rößl
Ziegeleistr. 40c
84051 Essenbach
Germany
VAT ID No.: DE366480248
Email: support@roessolytics.de

- hereinafter “Processor” -

jointly hereinafter referred to as the “Parties”.

Version: May 16, 2026

1. Subject matter of the agreement

1. This agreement governs the processing of personal data by the Processor on behalf of the Controller in connection with the use of the **ROESSOLYTICS** SaaS web analytics platform.
2. The Controller is the controller within the meaning of the GDPR where it collects, processes, or has personal data evaluated through ROESSOLYTICS.
3. The Processor processes personal data exclusively as a processor in accordance with this agreement, the principal agreement, the booked services, and the documented instructions of the Controller.
4. This agreement does not cover processing activities where the Processor determines the purposes and means itself, in particular the processing of the Controller’s own contract, billing, payment, accounting, and communication data. Such processing is carried out by the Processor as an independent controller and is described in the Processor’s Privacy Policy.

2. Term of the agreement

1. This agreement begins upon conclusion of the principal agreement for the use of ROESSOLYTICS.
2. It ends automatically upon complete termination of the principal agreement, unless statutory retention, documentation, or backup obligations prevent this.
3. After the end of the agreement, personal data processed on behalf of the Controller will be deleted in accordance with Section 13 or, where technically available and requested by the Controller,

returned.

3. Nature and purpose of processing

The Processor processes personal data for the purpose of providing, operating, securing, maintaining, and further developing ROESSOLYTICS.

The processing includes in particular:

1. collection and evaluation of website and usage events,
2. provision of web analytics dashboards,
3. processing of page views, events, referrers, UTM parameters, and technical metadata,
4. creation of pseudonymous session and visit identifiers,
5. provision of tracking links and tracking pixels, where used by the Controller,
6. processing of custom properties, tags, event data, or identifiers transmitted by the Controller,
7. administration of websites, workspaces, roles, and user access,
8. abuse, error, and security analysis,
9. technical provision, monitoring, maintenance, support, and troubleshooting.

4. Types of personal data

Depending on the Controller’s use, the following data in particular may be processed:

1. technical access data:
   - IP address or information derived from the IP address,
   - user agent,
   - browser,
   - operating system,
   - device type,
   - screen size,
   - language setting,
   - date and time of access;
2. web analytics data:
   - visited URL,
   - path,
   - hostname,
   - page title,
   - referrer,
   - campaign parameters,
   - UTM parameters,
   - click IDs,

- events,
- tags,
- custom properties;

3. pseudonymous identifiers:
   - session ID,
   - visit ID,
   - website ID,
   - link ID,
   - pixel ID,
   - optional identifiers transmitted by the Controller, for example through an identify function;
4. account and usage data within the platform:
   - name,
   - email address,
   - role,
   - workspace assignment,
   - website assignment,
   - language,
   - theme,
   - time zone,
   - dashboard and display settings.

Where ROESSOLYTICS processes IP addresses, this is done according to the current technical concept in particular for geo derivation, security checks, and the creation of pseudonymous session identifiers. Permanent storage of IP addresses in plain text is not intended for regular analytics operation.

5. Categories of data subjects

The processing may in particular affect the following persons:

1. visitors to the Controller’s websites, apps, or digital offerings,
2. users, customers, prospects, or business partners of the Controller,
3. employees, administrators, and other authorized users of the Controller,
4. persons captured via the Controller’s tracking links or tracking pixels,
5. persons whose data the Controller transmits to ROESSOLYTICS via events, tags, custom properties, or identifiers.

6. Special categories of personal data

1. The processing of special categories of personal data within the meaning of Article 9 GDPR is not the purpose of using ROESSOLYTICS.

2. The Controller undertakes not to process special categories of personal data, health data, data concerning political opinions, religion, trade union membership, sexual orientation, biometric data, criminal offence data, or similarly sensitive data through ROESSOLYTICS unless this has been expressly agreed separately and an appropriate legal basis exists.
3. If the Controller nevertheless enters or transmits such data through custom properties, events, tags, tracking links, tracking pixels, or identify functions, the Controller is solely responsible for this.

7. Binding nature of instructions

1. The Processor processes personal data exclusively on documented instructions from the Controller.
2. Instructions arise in particular from:
   - this agreement,
   - the principal agreement,
   - the services booked by the Controller,
   - the settings in the dashboard,
   - the Controller’s technical integrations,
   - written instructions by email or support request.
3. The Processor may reject or suspend instructions if, in its assessment, they violate data protection law or other applicable law. In this case, the Processor will inform the Controller without undue delay unless legal reasons prevent this.
4. Oral instructions must be confirmed in text form without undue delay.

8. Obligations of the Controller

The Controller is in particular obliged to:

1. ensure an appropriate legal basis for the collection and processing of data through ROESSOLYTICS,
2. properly inform its own users, visitors, and data subjects about the data processing,
3. obtain required consents where legally required,
4. integrate ROESSOLYTICS in a technically correct and data protection compliant manner,
5. not transmit unlawful or excessive personal data,
6. not process special categories of personal data without a separate agreement,
7. appropriately manage access, roles, and permissions within its own area of responsibility,
8. ensure that only authorized persons receive access to the dashboard,
9. handle data subject requests, deletion requests, access requests, and objections on its own responsibility where they fall within the Controller’s area of responsibility.

9. Confidentiality

1. The Processor ensures that persons involved in processing personal data have been committed to confidentiality or are subject to an appropriate statutory duty of secrecy.

2. Access to personal data is limited to persons who require such access to perform their tasks.
3. The confidentiality obligation continues after termination of this agreement.

10. Technical and organizational measures

1. The Processor implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
2. The measures include in particular:
   - encrypted transmission via HTTPS/TLS,
   - role-based access control,
   - separation of customer and workspace areas,
   - restriction of administrative access,
   - protection of production systems through server, network, and application security measures,
   - authentication and authorization concepts,
   - pseudonymization of analytics identifiers where technically provided,
   - processing of analytics identifiers without permanent browser-side tracking cookies where the standard integration is used,
   - protection against unauthorized access,
   - regular updates and maintenance of the systems used,
   - logging of security-relevant events where technically configured,
   - backup and recovery measures according to the internal backup concept,
   - separation of production and test/staging environments where provided for the respective environment.
3. The technical and organizational measures may be adapted as part of technical development, provided that the security level is not materially reduced.
4. The Processor is entitled to use alternative appropriate measures if they ensure an equivalent or higher level of protection.

11. Assistance to the Controller

The Processor assists the Controller to the extent reasonable and necessary with:

1. responding to data subject requests,
2. access, rectification, deletion, and restriction requests,
3. data portability requests,
4. fulfilling notification obligations in the event of personal data breaches,
5. data protection impact assessments where ROESSOLYTICS is affected,
6. requests from supervisory authorities where they concern processing on behalf of the Controller.

Assistance is generally provided by email or support form. If a request causes significant additional effort for the Processor, this may be charged separately after prior coordination to the extent permitted by law.

12. Personal data breaches

1. The Processor informs the Controller without undue delay if it becomes aware of a personal data breach affecting personal data processed by the Processor on behalf of the Controller.
2. The information includes, where available:
   - the nature of the breach,
   - affected data categories,
   - affected groups of data subjects,
   - likely consequences,
   - measures already taken or proposed,
   - contact person for questions.
3. The Processor reasonably assists the Controller in assessing and fulfilling any notification and communication obligations.
4. Responsibility for notifying the competent supervisory authority or affected persons lies with the Controller where the Controller is the controller.

13. Deletion and return of data

1. After termination of the principal agreement, the Processor generally deletes personal data processed on behalf of the Controller within 90 days, unless statutory retention, documentation, or backup obligations prevent this.
2. Upon request by the Controller, the Processor provides the data processed on behalf of the Controller in an appropriate format before deletion, where this is technically available and reasonable.
3. Data transfer through the dashboard is currently available only to the extent that corresponding export functions are provided. Otherwise, data will be provided upon request.
4. Backup copies may still contain data for a limited period after termination of the agreement and will be deleted or overwritten according to the regular backup cycle.
5. Data that the Processor processes as an independent controller, in particular billing, contract, tax, or commercial law relevant data, is not covered by this deletion obligation.

14. Sub-processors

1. The Controller grants the Processor general authorization to engage sub-processors.
2. The Processor engages sub-processors only where this is necessary for the operation, security, provision, support, or further development of ROESSOLYTICS.
3. The Processor contractually binds sub-processors to data protection obligations that substantially correspond to the obligations under this agreement.
4. The Processor informs the Controller of material changes concerning sub-processors with reasonable prior notice, for example by email, website, dashboard, or another suitable notice.
5. The Controller may object to the use of a new sub-processor for an important data protection reason. In this case, the Parties will seek an appropriate solution. If no solution is possible, the

Processor may terminate the affected service or restrict its use to the extent that the sub-processor is necessary for providing the service.

6. The sub-processors used at the time of conclusion of the agreement are listed in Annex 3.

15. Third country transfers

1. Personal data is transferred to countries outside the European Union or the European Economic Area only where the requirements of the GDPR are met.
2. Where sub-processors in third countries are used or access from third countries cannot be excluded, the Processor ensures appropriate safeguards, for example through an adequacy decision, standard contractual clauses, or other mechanisms provided by law.
3. The Processor informs the Controller upon request about the safeguards used in each case.

16. Audit and documentation obligations

1. The Processor provides the Controller upon request with the information required to demonstrate compliance with the obligations under this agreement.
2. Audits generally take place through the provision of suitable evidence, documentation, security information, or self-assessments.
3. On-site audits are permissible only if they are necessary, appropriate, announced in advance, and coordinated with the Processor.
4. Audits must not disproportionately impair business operations, system security, or the rights of other customers.
5. The Controller bears its own audit costs. If the Processor incurs significant additional effort, this may be charged appropriately after prior coordination to the extent permitted by law.

17. Data processing in staging and test environments

1. Production personal data may be processed in staging, test, or development environments only where this is necessary for error analysis, maintenance, or further development and appropriate safeguards are in place.
2. The Processor endeavors to avoid or minimize production personal data in non-production environments.
3. The Controller must not introduce unnecessary personal data into test or support cases.

18. Support and remote maintenance

1. Support is provided exclusively by email, support form, or communication channels provided by the Processor.
2. In support cases, it may be necessary for the Processor to access technical information, account data, configurations, or analytics events.
3. The Processor limits support access to what is necessary.
4. The Controller should submit support requests without unnecessary personal data where possible.

19. Liability

1. The liability of the Parties is governed by the statutory provisions and the provisions of the principal agreement.
2. This agreement does not establish any further liability unless mandatory data protection law provides otherwise.
3. The Controller remains responsible for the lawfulness of the data processing, the selection of data, the legal basis, information obligations, and the data protection compliant integration of ROESSOLYTICS.

20. Order of precedence

1. In the event of contradictions between this agreement and the principal agreement, the provisions of this agreement prevail to the extent that they concern processing of personal data on behalf of the Controller.
2. In all other respects, the provisions of the principal agreement and the Terms and Conditions apply.

21. Final provisions

1. Amendments and additions to this agreement require at least text form unless a stricter form is prescribed by law.
2. If any provision of this agreement is or becomes invalid, the validity of the remaining provisions remains unaffected.
3. The law of the Federal Republic of Germany applies.
4. The place of jurisdiction is determined by the statutory provisions and the provisions of the principal agreement.

Annex 1 - Description of processing

1. Subject matter

Provision of the ROESSOLYTICS SaaS web analytics platform for privacy-friendly analysis of websites, digital offerings, tracking links, tracking pixels, and user-defined events.

2. Purpose

The purpose of processing is the technical collection, aggregation, evaluation, and presentation of usage and event data for the Controller.

3. Types of processing

- collecting,
- recording,
- organizing,
- structuring,
- storing,
- adapting,
- retrieving,
- consulting,
- using,
- transmitting,
- restricting,
- deleting,
- pseudonymizing,
- aggregating,
- evaluating.

4. Affected data categories

- technical access data,
- usage data,
- event data,
- referrer and campaign data,
- pseudonymous analytics identifiers,
- dashboard user data,
- role and permission data,
- custom properties transmitted by the Controller,
- identifiers transmitted by the Controller.

5. Affected groups of data subjects

- website visitors,
- users of the Controller’s digital offerings,
- customers and prospects of the Controller,
- employees and administrators of the Controller,
- recipients or users of tracking links or tracking pixels.

6. Duration

For the duration of the principal agreement. After termination of the agreement, deletion generally takes place within 90 days unless statutory or technical reasons prevent this.

Annex 2 - Technical and organizational measures

1. Physical access control

- operation in data center and hosting environments of professional providers,
- physical access protection by hosting providers,
- no general physical access by the Processor to data center infrastructure.

2. System access control

- access to systems only for authorized persons,
- authentication through user accounts,
- protection of administrative access,
- restriction of privileged access,
- regular review of required access.

3. Data access control

- role-based permissions within ROESSOLYTICS,
- separation of customer and workspace areas,
- role-based restriction of administrative functions,
- super admin access only for authorized internal administration purposes.

4. Transfer control

- encrypted data transmission via HTTPS/TLS,
- use of access restrictions for internal interfaces,
- transfer to sub-processors only to the extent necessary,
- no transfer to third parties without a legal basis or contractual permission.

5. Input control

- technical traceability of selected system and administration processes where configured,

- processing of account, role, and configuration data through defined user interfaces and APIs.

6. Processing control

- processing only on the basis of the principal agreement, this agreement, and documented instructions,
- contractual obligation of engaged sub-processors,
- control and selection of sub-processors according to data protection and security-related criteria.

7. Availability control

- operation on professional server infrastructure,
- backup and recovery measures according to the internal backup concept,
- technical monitoring of production services where configured,
- protection against accidental destruction or loss within the scope of appropriate technical measures.

8. Separation requirement

- logical separation of customer and workspace areas,
- separation of production and staging/test environments where provided,
- separate management of roles, websites, and workspaces.

9. Pseudonymization and data minimization

- pseudonymous session and visit identifiers,
- no standard permanent storage of IP addresses in plain text intended for regular analytics operation,
- processing only of data required for analytics, security, and operation,
- option for privacy-friendly integration without own tracking cookies.

Annex 3 - Sub-processors

At the time of conclusion of the agreement, the following sub-processors in particular may be used:

Sub-processor	Location	Purpose	Data categories
Hetzner Online GmbH	Germany	Hosting, server, network, and infrastructure services	all data required for operation
Cloudflare Inc.	USA / international	DNS, CDN, security functions, reverse proxy, DDoS protection	technical access data, IP address, request data
Email/SMTP service provider	specifically named in the respective production environment	sending technical and transactional emails	email address, name, technical sending data

Service providers used by the Processor for its own purposes as controller, in particular payment, invoicing, or accounting service providers for the contract and billing relationship between Processor and Controller, are not sub-processors within the meaning of this agreement.

Annex 4 - Instructions and contact persons

1. Instructions

Instructions may in particular be given through:

- settings in the ROESSOLYTICS dashboard,
- technical configuration of the tracking integration,
- support requests,
- email to support@roessolytics.de,
- contractual agreements.

2. Processor contact person

ROESSOLUTIONS®
Benjamin Rößl
Email: support@roessolytics.de

3. Controller contact person

Contact person named by the Controller at conclusion of the agreement or in the dashboard.