

Data Processing Agreement (DPA)

pursuant to Art. 28 GDPR · Version 1.1

1. Parties

Controller ("Customer"): the customer using a nootiz plan.

Processor ("nootiz"): hantha GmbH, Dick 48/B, 39058 Sarntal / Sarnthein, Südtirol – Italy, VAT ID IT03231400213, email info@nootiz.com, operator of the nootiz software (app.nootiz.com).

This agreement sets out the parties' data protection obligations under the main agreement (nootiz Terms of Service). It is concluded in electronic form pursuant to Art. 28(9) GDPR and is deemed agreed upon registration or purchase of a plan. No signature is required.

2. Subject matter, duration, nature and purpose

Subject matter is the provision of the nootiz SaaS solution for collecting, managing and processing visual website feedback. The duration equals the term of the main agreement.

Types of data: contact and account data (name, email, role), feedback content (comments, screenshots, attachments, URL, browser and device information), project and usage data, log data.

Data subjects: the Customer's users, their clients, project stakeholders and invited guests; where applicable, persons visible in screenshots.

Purpose: solely the provision of the contractually agreed services.

3. Instructions

nootiz processes personal data only on documented instructions from the Customer, including with regard to transfers to third countries, unless required to do so by Union or Member State law (Art. 28(3)(a) GDPR). Instructions are set out in this agreement, the main agreement and the settings in the software. nootiz informs the Customer without delay if it considers an instruction to infringe data protection law.

4. Confidentiality

All persons authorised to process the data have committed themselves to confidentiality or are under a statutory obligation of confidentiality (Art. 28(3)(b) GDPR).

5. Security of processing

nootiz implements the technical and organisational measures pursuant to Art. 32 GDPR described in Annex 1. It may adapt them to technical progress provided the level of protection is not reduced.

6. Sub-processors

The Customer grants general authorisation for the sub-processors listed in Annex 2. nootiz informs the Customer in advance by email or within the software of any intended changes. The Customer may object within 14 days on reasonable data protection grounds. If no agreement is reached, the Customer may terminate the main agreement for cause.

nootiz imposes the same data protection obligations on each sub-processor by contract (Art. 28(4) GDPR).

7. International transfers

Where processing takes place outside the EEA, nootiz ensures that the requirements of Art. 44 et seq. GDPR are met. This is done in particular through an adequacy decision (EU-US Data Privacy Framework for certified providers) or the EU Standard Contractual Clauses (Implementing Decision (EU) 2021/914), with supplementary measures where required.

8. Assistance

nootiz assists the Customer with appropriate measures in fulfilling data subject rights (Art. 12–23 GDPR) and the obligations under Art. 32–36 GDPR (security, breach notification, data protection impact assessment, prior consultation). Requests received directly from data subjects are forwarded without delay.

9. Personal data breaches

nootiz notifies the Customer of a personal data breach without undue delay and no later than 48 hours after becoming aware of it. The notification contains the information required by Art. 33(3) GDPR, as far as available.

10. Deletion and return

End of a project: the Customer can archive projects but not delete them. Archived projects remain stored until the end of the agreement. On request by email to info@nootiz.com, nootiz permanently deletes individual projects (feedback, screenshots, attachments, comments) within 30 days.

Termination or end of agreement: the Customer can export its data for 30 days after the end of the agreement. nootiz then permanently deletes all personal data of the account, unless statutory retention obligations apply (Art. 28(3)(g) GDPR). On request, the data is returned beforehand.

Backups: deleted data is automatically removed from backups no later than 30 days after deletion. Until then it is protected against access and not processed further.

Exception: invoicing and billing data is retained for the duration of statutory retention obligations (e.g. 10 years under tax law).

On request, nootiz confirms the deletion in writing by email.

11. Audits and evidence

nootiz makes available all information necessary to demonstrate compliance with these obligations. It allows for and contributes to audits and inspections with reasonable prior notice during normal business hours (Art. 28(3)(h) GDPR). Evidence is primarily provided through self-disclosure, documentation or certifications of sub-processors.

12. Liability and final provisions

Liability is governed by Art. 82 GDPR and otherwise by the main agreement. In the event of conflict, this agreement prevails over the main agreement on data protection matters. Should any provision be invalid, the remaining provisions remain unaffected. The law of the Processor's country of establishment applies, subject to the GDPR.

Annex 1 – Technical and organisational measures (Art. 32 GDPR)

Confidentiality: Encrypted transmission (TLS/HTTPS) for all connections. Encryption of stored data (at rest) at the hosting and database providers. Role- and permission-based access, restricted to authorised staff on a need-to-know basis. Passwords are stored hashed only. Tenant separation at project and account level.

Integrity: Logging of administrative access. Input validation. Code changes only through versioned, traceable deployments.

Availability and resilience: Operation in professional data centres with redundant infrastructure. Regular automated backups. Availability monitoring.

Recoverability: Restoration from backups is documented and tested.

Regular review: Regular review of the measures, security updates of dependencies, careful selection and monitoring of sub-processors.

Annex 2 – Sub-processors

Provider	Service	Location / safeguard
Vercel Inc., San Francisco, USA	Hosting of the application app.nootiz.com	EU region as configured; EU-US Data Privacy Framework, EU Standard Contractual Clauses
MongoDB, Inc. (Atlas), New York, USA	Database hosting	EU region as configured; EU-US Data Privacy Framework, EU Standard Contractual Clauses
Resend (Plus Five Five, Inc.), USA	Delivery of system emails	EU-US Data Privacy Framework, EU Standard Contractual Clauses

Note: Payments are processed by Stripe (Stripe Payments Europe, Ltd., Dublin, Ireland). Stripe processes payment data as an independent controller and is therefore not a sub-processor under this agreement.

Questions about this agreement: info@nootiz.com