

Data Processing Agreement (DPA)

pursuant to Art. 28 of the General Data Protection Regulation (GDPR)

Version 1.0 · October 2026

This English version is provided for information. The German version (Auftragsverarbeitungsvertrag) is legally binding.

Scope of application

This Data Processing Agreement ("DPA") applies between

nebty GmbH, c/o BASE Coworking, Blütenstraße 15, 80799 Munich, Germany, registered with the commercial register of the Local Court of Munich under HRB 293827 ("nebty"),

and the business that obtains services from nebty under nebty's General Terms and Conditions or an individually negotiated contract (the "Customer"; the respective contract for the services the "Main Agreement").

This DPA becomes part of the Main Agreement upon its conclusion – by completing the order process, activation of the customer account, or signature. No separate signature is required; the electronic form satisfies Art. 28(9) GDPR. nebty will provide a countersigned copy on request.

§ 1 Subject matter, scope and term

(1) nebty provides brand protection services to the Customer, in particular monitoring of online channels for brand abuse ("Monitoring"), enforcing the removal of infringing content ("Takedown"), provision of the nebty platform, and access via programming interfaces (together the "Services"). This DPA applies to the extent that nebty processes personal data on behalf of the Customer in doing so.

(2) The free website scanner and other offerings used without a customer account are not covered by this DPA.

(3) This DPA runs for the term of the Main Agreement. Obligations which by their nature survive termination, in particular under §§ 5(1) and 12, continue for as long as nebty processes personal data of the Customer.

§ 2 Nature and purpose of processing, types of data and data subjects

(1) The nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in **Annex 1**.

(2) The Customer is the controller within the meaning of Art. 4(7) GDPR. nebty is the processor.

(3) Where the Customer itself processes the data on behalf of a third party – for example as a managed service provider, agency or reseller for the brands of its end clients – nebty acts as a sub-processor. The Customer ensures that its instructions are covered by those of its controller and that this DPA meets the requirements of Art. 28(4) GDPR in its relationship with that controller. The Customer exercises the controller's rights vis-à-vis nebty.

§ 3 Processing under nebty's own responsibility

(1) This DPA does not cover processing for which nebty is itself the controller, in particular:

1. contract administration, invoicing and payment processing, and communication with the Customer about the contractual relationship,

2. ensuring the security and stability of nebty's own systems, including defence against abusive access,
3. retaining records that evidence proper performance of the Services or are necessary to establish, exercise or defend legal claims, and complying with statutory retention obligations.

(2) nebty may use technical threat indicators arising in the course of the Services – in particular domain names, URLs, IP addresses, hash values and information on hosting providers and registrars of fraudulent offerings – as well as anonymised or aggregated analyses, in order to improve its detection methods and to protect other customers from the same attacks. The Customer's identity, brands and case files are not disclosed in doing so. To the extent such indicators exceptionally relate to an identifiable person, nebty processes them under its own responsibility on the basis of Art. 6(1)(f) GDPR.

(3) Recipients of notices sent by nebty in the course of a Takedown – such as registrars, hosting providers, platform operators, search engines and operators of security blocklists – process the data transmitted to them under their own responsibility. They are not sub-processors under this DPA.

§ 4 Instructions

(1) nebty 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. In such a case, nebty informs the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(2) The Main Agreement, this DPA and the settings and requests made by the Customer in the platform or via the programming interfaces – such as setting up a brand, selecting the monitored channels or ordering a Takedown – constitute the Customer's instructions. The Customer issues further instructions in text form (email suffices).

(3) nebty informs the Customer without undue delay if, in its opinion, an instruction infringes the GDPR or other data protection provisions. nebty may suspend execution of the instruction until the Customer confirms or amends it.

(4) Instructions going beyond the agreed scope of Services are treated by the parties as a change request.

§ 5 Obligations of nebty

(1) **Confidentiality.** nebty ensures that persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and only have access to the data to the extent necessary to provide the Services.

(2) **Security of processing.** nebty implements the technical and organisational measures required under Art. 32 GDPR. The measures in place at the time of conclusion are described in **Annex 2**. nebty may adapt the measures to technical progress provided the level of protection is not reduced. nebty documents material changes.

(3) **Purpose limitation.** nebty processes the Customer's data only to provide the Services and, subject to § 3, for no other purpose. nebty does not sell the data and does not use it to train third-party AI models; nebty uses AI services only on terms that exclude use of the transmitted data for model training by the provider.

(4) **Place of processing.** The nebty platform, including the database and evidence storage, is operated in data centres in Germany. Certain sub-processors process data outside the European Economic Area; § 7 applies.

(5) **Records.** nebty maintains a record of all categories of processing activities carried out on behalf of its customers (Art. 30(2) GDPR).

(6) **Contact.** nebty's contact for data protection matters can be reached at info@nebty-id.com.

§ 6 Sub-processors

- (1) The Customer grants nebty general authorisation to engage sub-processors. The sub-processors engaged at the time of conclusion are listed in **Annex 3** and are deemed approved.
- (2) nebty informs the Customer at least **thirty (30) days** before adding or replacing a sub-processor, by updating the list in Annex 3 and by email to the address of the account owner stored in the customer account and to customers who have registered for change notifications.
- (3) The Customer may object to the change in text form on reasonable data protection grounds within fourteen (14) days of receipt of the notice. The parties will then seek an amicable solution. If none is reached within a reasonable period, either party may terminate the Services affected by the change with effect from the date the change takes effect. nebty refunds prepaid fees for the unused period on a pro-rata basis.
- (4) Where replacing a sub-processor is urgently required to ensure the security or availability of the Services, nebty may do so without observing the notice period in paragraph 2. nebty informs the Customer without undue delay in that case; the right to object under paragraph 3 remains unaffected.
- (5) nebty imposes on each sub-processor by contract substantially the same data protection obligations as set out in this DPA, in particular sufficient guarantees for appropriate technical and organisational measures. nebty remains liable to the Customer for the sub-processor's compliance with those obligations.
- (6) Ancillary services that nebty obtains from third parties without those third parties having intended access to the Customer's personal data – such as telecommunications services or software operated in nebty's own environment – do not constitute sub-processing.

§ 7 Transfers to third countries

- (1) Personal data is transferred to a country outside the European Economic Area only if the requirements of Art. 44 et seq. GDPR are met.
- (2) For transfers to sub-processors, nebty relies on an adequacy decision of the European Commission under Art. 45 GDPR – for recipients in the United States, on an active certification under the EU-U.S. Data Privacy Framework – or on the European Commission's Standard Contractual Clauses under Implementing Decision (EU) 2021/914 (Art. 46(2)(c) GDPR). The applicable mechanism is stated in Annex 3. If a mechanism ceases to apply, nebty switches the transfer to another lawful mechanism or suspends it.
- (3) Where personal data is transferred from the Customer to nebty from a third country, or the Customer accesses the platform from a third country, the Standard Contractual Clauses (Module 2, or Module 3 for customers under § 2(3)) are deemed agreed between the parties to the extent required. Clause 7 does not apply; Option 2 applies to Clause 9 with the notice period under § 6(2); the optional wording in Clause 11 does not apply; for Clauses 17 and 18, the law of the Federal Republic of Germany and the courts of Munich apply. The annexes to the Standard Contractual Clauses are completed by Annexes 1 to 3; the competent supervisory authority is the Bavarian Data Protection Authority (Bayerisches Landesamt für Datenschutzaufsicht). For transfers subject to the data protection law of the United Kingdom or Switzerland, the Standard Contractual Clauses apply with the adjustments provided for that purpose (UK International Data Transfer Addendum, or the adjustments specified by the Swiss Federal Data Protection and Information Commissioner).
- (4) **Notices in the course of a Takedown.** A Takedown requires nebty to send a notice including evidence to the provider responsible for the infringing content; such providers may be located anywhere in the world. By ordering a Takedown, the Customer instructs nebty to send these notices. Before each notice to a recipient outside the European Economic Area, nebty checks whether an adequacy decision or appropriate safeguards exist. Where this is not the case, the transfer is based on Art. 49(1)(e) GDPR to the extent it is necessary to assert the Customer's rights against the respective provider. nebty limits the content of each notice to what the respective recipient needs and redacts personal data not required for processing the notice.

§ 8 Assistance

(1) nebty assists the Customer by appropriate technical and organisational measures in responding to requests from data subjects exercising their rights under Chapter III GDPR. If a data subject addresses a request directly to nebty, nebty forwards it to the Customer without undue delay and does not respond without the Customer's instruction, provided the request can be attributed to the Customer.

(2) Taking into account the nature of processing and the information available to it, nebty assists the Customer in complying with its obligations under Art. 32 to 36 GDPR, in particular with data protection impact assessments and prior consultation of the supervisory authority.

(3) Assistance under this § 8 that goes beyond the functions provided in the platform and is not caused by a breach on nebty's part may be charged to the Customer at reasonable rates after prior notice.

§ 9 Personal data breaches

(1) nebty notifies the Customer of any personal data breach affecting the Customer's data without undue delay and no later than **forty-eight (48) hours** after becoming aware of it.

(2) To the extent known, the notification describes the nature of the breach, including the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact person. nebty provides information not yet available without undue delay as it becomes available.

(3) nebty takes the necessary measures to contain the breach and mitigate its consequences without undue delay and assists the Customer in meeting its notification obligations. nebty notifies supervisory authorities or data subjects on behalf of the Customer only on the Customer's instruction.

§ 10 Evidence and audits

(1) On request, nebty provides the Customer with all information necessary to demonstrate compliance with Art. 28 GDPR and this DPA, in particular the current description of the technical and organisational measures and the contractual basis of the sub-processors. Appropriate certifications or audit reports from independent bodies may serve as evidence.

(2) In addition, the Customer may conduct audits, including inspections, itself or through an auditor bound by confidentiality who is not a competitor of nebty. Audits take place on at least thirty (30) days' notice, as a rule no more than once per calendar year, during normal business hours and without disproportionate disruption of operations. Audits following a personal data breach and audits required by a supervisory authority are exempt from these limits.

(3) The Customer bears the costs of an audit. nebty may request reasonable compensation for its own effort, unless the audit reveals a material breach of this DPA by nebty.

(4) Audit rights do not extend to information constituting nebty's trade secrets or data of other customers, or to systems of sub-processors; in that respect, nebty provides the evidence it has received from them, to the extent it is permitted to share it.

§ 11 Obligations of the Customer

(1) The Customer is responsible for the lawfulness of the processing, in particular for having a legal basis and for complying with information obligations towards data subjects. This includes the selection of brands, marks and search terms to be monitored and the ordering of Takedowns.

(2) The Customer does not provide nebty with special categories of personal data within the meaning of Art. 9 GDPR or data within the meaning of Art. 10 GDPR, unless this is unavoidable for providing the Services and

agreed in advance. The fact that infringing third-party content may in individual cases contain such data remains unaffected.

(3) The Customer informs nebty without undue delay if it detects errors or irregularities in the processing.

(4) The Customer is responsible for managing its organisation's user accounts, in particular for granting and revoking access and protecting credentials. Where the Customer forwards notifications to its own systems or to third-party services – for example via webhook, to messaging channels or via programming interfaces to its own applications – the processing is the Customer's responsibility from the point of handover.

§ 12 Deletion and return

(1) The Customer can export its data during the term of the Main Agreement via the platform and the programming interfaces. On request, nebty provides the data within ten (10) business days after the end of the Main Agreement in a common, machine-readable format.

(2) After termination of the Main Agreement, nebty deletes the personal data processed on behalf of the Customer within thirty (30) days, unless the Customer has previously requested its return. Copies in backups are overwritten in the course of regular backup cycles, no later than after ninety (90) days. Until then, they remain subject to this DPA and are not actively processed.

(3) Paragraph 2 does not apply where Union or Member State law requires storage, or to data under § 3(1) no. 3. nebty confirms deletion in text form on request.

§ 13 Liability

(1) Liability towards data subjects is governed by Art. 82 GDPR.

(2) Between the parties, the liability provisions of the Main Agreement apply, unless mandatory law or the Standard Contractual Clauses provide otherwise.

§ 14 Regulated customers

If the Customer is a financial entity within the meaning of Regulation (EU) 2022/2554 (DORA) or is subject to comparable regulatory outsourcing requirements, the parties will agree a supplementary agreement on request, in particular regarding the requirements of Art. 30 DORA. nebty provides a template for this purpose.

§ 15 Final provisions

(1) **Order of precedence.** In case of conflict, the following apply in this order: (a) the Standard Contractual Clauses, to the extent applicable under § 7; (b) a data processing agreement individually signed between the parties; (c) this DPA; (d) the Main Agreement. This DPA takes precedence over the Main Agreement in all matters relating to the processing of personal data.

(2) **Amendments.** nebty may amend this DPA to the extent required to adapt it to changed legal requirements or changes to the Services, provided the level of protection for the Customer is not reduced. nebty announces amendments in text form at least six (6) weeks before they take effect. If the Customer does not object within this period, the amendment is deemed accepted; nebty will point out this consequence in the notice. If the Customer objects, the DPA continues to apply in its previous version; both parties' right to terminate the Main Agreement in the ordinary course remains unaffected. Changes to the list of sub-processors are governed exclusively by § 6.

(3) **Governing law and jurisdiction.** The law of the Federal Republic of Germany applies. Place of jurisdiction is Munich, to the extent the Customer is a merchant, a legal entity under public law or a special fund under public law.

(4) **Severability.** Should individual provisions of this DPA be or become invalid, the validity of the remaining provisions remains unaffected. The invalid provision is replaced by the statutory provision.

(5) **Language.** The German version of this DPA is binding. The English version is provided for information.

Annex 1 – Description of the processing

Subject matter and duration: Provision of the Services under the Main Agreement for its term and until deletion under § 12.

Frequency: continuous, to the extent necessary to provide the Services.

Service	Nature and purpose of processing	Types of personal data	Data subjects
Platform and customer account	Provision of the platform, management of user accounts and permissions, login, notifications by email and to channels set up by the Customer, support	Name, business email address, role and permissions, login and usage data, IP addresses, settings, support communications	Employees and representatives of the Customer; for customers under § 2(3), employees and representatives of their end clients
Monitoring	Automated search for offerings and content abusing the Customer's brands; collection, assessment (including AI-assisted) and documentation of findings	Domain and registration data (e.g. WHOIS, certificate data), content and screenshots of suspicious websites, publicly available profile data of suspicious social media and professional network profiles (e.g. name, profile picture, job title, profile URL), data on advertisements and advertisers, contact details on infringing pages	Owners, operators and contact persons of suspicious offerings; persons appearing in monitored content; employees of the Customer, to the extent their public profiles are used to distinguish genuine from fake profiles
Takedown	Preservation of evidence, identification of responsible providers, sending notices and complaints on behalf of the Customer, follow-up, verification of success, documentation	Case data (URLs, screenshots, page source, technical headers, timestamps), registration data, correspondence with providers including abuse contact addresses, information from the Customer on the case and its rights	As for Monitoring; additionally employees of the contacted providers and the reporting persons at the Customer
Programming interfaces	Customer access to the Services via API, webhooks and integrations	Access credentials, access log data, transmitted content as above	Employees of the Customer; persons as in the rows above

Special categories of personal data: not processed intentionally; see § 11(2).

Annex 2 – Technical and organisational measures

The measures are structured according to the protection goals of Art. 32 GDPR.

1. Confidentiality

Physical access control

- The platform, databases and object storage are operated exclusively in data centres of Hetzner Online GmbH in Germany, which are certified to ISO/IEC 27001 and have physical access control.

- nebtly does not operate its own server rooms. Workstations on which case data is handled are protected by full-disk encryption and screen lock.

System access control

- Personal user accounts for the platform, infrastructure and third-party services.
- Passwords are stored only as salted hashes.
- Two-factor authentication for administrative access to infrastructure and third-party services; available to platform users. Single sign-on available as an alternative login.
- Protection of login and registration against automated attacks.
- Access to programming interfaces only with access tokens; tokens can be revoked.

Data access control

- Role and permission concept based on the principle of least privilege.
- Logical separation of different customers' data; users see only their own organisation's data.
- Revocation of access when employees leave or change roles.

Separation control

- Data is processed only for the purpose for which it was collected; tenant separation within the platform.

2. Integrity

Transfer control

- Encryption of all connections to the platform and programming interfaces in line with the state of the art (TLS).
- Infringing domains are defanged in outgoing notices and never sent as clickable links.
- Notices to third parties are limited to the information the respective recipient needs.

Input control

- Logging of security-relevant events and of changes to case data.
- Evidence of success is documented with timestamp and source.

3. Availability and resilience

- Regular backups.
- Continuous monitoring of platform errors and incidents.
- Protection against automated and abusive access.
- Fallback reporting channel by email if the platform is unavailable.

4. Procedures for regular testing, assessment and evaluation

- Selection of sub-processors taking their security measures into account; conclusion of agreements under Art. 28 GDPR and, where required, Standard Contractual Clauses.
- Use of AI services only on the basis of business agreements with a data processing agreement and without use of the data for model training.
- Confidentiality undertakings from all employees and regular awareness training on data protection and information security.
- Regular updates of the software in use and its dependencies.
- Review of these measures at least annually and when required.
- Procedure for detecting, assessing and reporting personal data breaches under § 9.

Annex 3 – Sub-processors

The current list of sub-processors, including registered office, service, place of processing and transfer mechanism, is available at nebty-id.com/en/subprocessors/ and forms part of this DPA. Changes are made in accordance with § 6.

nebty GmbH · c/o BASE Coworking, Blütenstraße 15, 80799 Munich, Germany · info@nebty-id.com

Sub-processors

Annex 3 to the nebty GmbH Data Processing Agreement

As of: October 2026

nebty GmbH engages the following sub-processors to provide its services. The platform, the database and evidence storage are operated in Germany. The other service providers process data only for the purpose stated.

We announce planned changes at least 30 days in advance (§ 6 DPA). If you would like to be notified at an additional address, or do not have a customer account of your own, write to info@nebty-id.com.

For all services

Company	Registered office	Service	Place of processing	Transfer mechanism
Hetzner Online GmbH	Gunzenhausen, Germany	Platform operation, database, object storage for screenshots and evidence	Germany	– (no third-country transfer)
Functional Software, Inc. (Sentry)	San Francisco, USA	Error and performance monitoring of the platform	Storage in the EU; access from the USA possible	EU-U.S. Data Privacy Framework; Standard Contractual Clauses
Twilio Inc. (SendGrid)	San Francisco, USA	Email delivery: notifications, system messages and takedown notices	USA	EU-U.S. Data Privacy Framework; Standard Contractual Clauses
Google Cloud EMEA Limited	Dublin, Ireland	Google Workspace: business mailboxes including correspondence with providers during takedowns; sign-in with Google	EU; onward processing in the USA	For onward transfers to Google LLC: EU-U.S. Data Privacy Framework; Standard Contractual Clauses
Cloudflare, Inc.	San Francisco, USA	Protection against automated and abusive access; hosting of the website; operation of the nebty MCP server and other serverless functions (Cloudflare Pages and Workers)	Global network, USA	EU-U.S. Data Privacy Framework; Standard Contractual Clauses

Additionally for Takedown

Company	Registered office	Service	Place of processing	Transfer mechanism
Anthropic Ireland, Limited	Dublin, Ireland	AI-assisted handling of takedown cases	USA	Standard Contractual Clauses

Additionally for Monitoring

Company	Registered office	Service	Place of processing	Transfer mechanism
OpenAI Ireland Limited	Dublin, Ireland	AI-assisted assessment of findings	USA	Standard Contractual Clauses
OpenRouter, Inc.	USA	Access to AI models for assessing findings	USA	Standard Contractual Clauses

Company	Registered office	Service	Place of processing	Transfer mechanism
Bright Data Ltd.	Netanya, Israel	Retrieval of publicly available web content	Israel	Adequacy decision (Israel)
Oxylabs, UAB	Vilnius, Lithuania	Proxy infrastructure for retrieving publicly available web content	EU	– (no third-country transfer)
VostokInc SAS (ScrapingBee)	Paris, France	Retrieval and rendering of web pages, screenshots	France	– (no third-country transfer)

Not sub-processors

The following process data under their own responsibility and are therefore not listed:

- **Recipients of takedown notices** such as registrars, hosting providers, platform operators, search engines and operators of security blocklists (§ 3(3) and § 7(4) DPA).
- **Data sources** queried by nebty, such as public registries, certificate transparency logs and platforms' ad libraries.
- **Payment service providers** involved in invoicing; invoicing is processing under nebty's own responsibility (§ 3(1) DPA).
- **The Customer's own services** to which the Customer forwards notifications, for example via webhook or to messaging channels (§ 11(4) DPA).