Hanko Cloud Data Processing Agreement

Version: 1.0
Effective Date: August 11, 2026

This Data Processing Agreement ("DPA") forms part of the Hanko Cloud Terms of Service ("Terms") between:

Hanko GmbH
Ringstraße 19
24114 Kiel
Germany

("Hanko")

and the Customer identified through the Customer's Hanko Cloud account.

Hanko and the Customer are each a "Party" and together the "Parties".

1. Scope and Formation

1.1 Application

This DPA applies where Hanko processes Customer Personal Data on behalf of the Customer in connection with the Customer's use of Hanko Cloud.

1.2 Services

"Hanko Cloud" or the "Services" means the hosted versions of:

- Hanko Auth; and
- Hanko Passkey API,

including the associated APIs, infrastructure and project management functionality provided through `cloud.hanko.io`.

1.3 Business Customers only

The Services are offered exclusively to:

- legal entities and other organizations;
- public-sector entities;
- self-employed professionals; and
- natural persons acting in the course of a commercial, business, craft or independent professional activity.

Consumers within the meaning of Section 13 of the German Civil Code may not create or use a Hanko Cloud account.

1.4 Customer

The “Customer” is the legal entity, organization, public-sector entity or business or professional user for whose benefit a Hanko Cloud account is created or used.

If an individual creates or uses a Hanko Cloud account on behalf of an organization, that organization is the Customer. The individual represents that:

- they are authorized to act on behalf of the organization; and
- the organization accepts the Terms and this DPA.

Where an individual creates or uses a Hanko Cloud account in the course of their own commercial or independent professional activity, that individual is the Customer.

1.5 Free and paid plans

This DPA applies to free and paid Hanko Cloud plans.

1.6 Formation

This DPA becomes binding when the Customer:

- creates a Hanko Cloud account;
- accepts the Terms; or
- otherwise agrees to use the Services subject to the Terms.

No separate signature is required.

1.7 Identification of the Customer

The Customer is identified through:

- the Customer’s Hanko Cloud account;
- the email address associated with that account; and
- where applicable, the organization and billing details provided for a paid subscription.

The email address associated with the Hanko Cloud account is the Customer’s primary contact address for notices under this DPA.

1.8 Optional signatures

At the Customer’s request, the Parties may execute the Optional Execution Page included at the end of this DPA.

Unless the Parties expressly agree otherwise, signing the Optional Execution Page:

- documents the Parties' existing agreement to this DPA;
- does not amend this DPA or the Terms;
- does not replace the Customer's prior acceptance of the Terms; and
- does not change the date on which this DPA became binding.

This DPA remains valid and binding if the Optional Execution Page is not completed or signed.

1.9 Scope of processor role

This DPA applies only to processing for which Hanko acts as a processor or subprocessor.

It does not apply to personal data for which Hanko determines the purposes and means of processing as an independent controller.

1.10 Order of precedence

If there is a conflict between this DPA and the Terms concerning the processing of Customer Personal Data, this DPA prevails.

If the Parties enter into an individual agreement that expressly modifies this DPA, the individual agreement prevails to the extent of the modification.

2. Definitions

2.1 Applicable Data Protection Law

"Applicable Data Protection Law" means the data protection and privacy laws applicable to the processing of Customer Personal Data under this DPA, including, where applicable:

- Regulation (EU) 2016/679 ("GDPR");
- the GDPR as incorporated into the laws of the United Kingdom ("UK GDPR"); and
- applicable national laws implementing, supplementing or replacing those laws.

2.2 Customer Personal Data

"Customer Personal Data" means personal data that Hanko processes on behalf of the Customer through the Services.

2.3 Account Data

"Account Data" means personal data that Hanko processes as an independent controller in connection with its contractual and business relationship with the Customer, including:

- Hanko Cloud account information;
- contact details;
- billing and payment information;

- communications with the Customer;
- subscription and service administration information;
- Hanko Cloud Console activity information; and
- information processed to secure the Customer's Hanko Cloud account, prevent misuse or comply with legal obligations.

2.4 Personal Data Breach

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data.

2.5 Subprocessor

"Subprocessor" means a third party appointed by Hanko to process Customer Personal Data on behalf of the Customer.

2.6 Other terms

The terms "controller", "processor", "data subject", "personal data" and "processing" have the meanings given to them under Applicable Data Protection Law.

3. Roles of the Parties

3.1 Customer role

The Customer acts as:

- controller of Customer Personal Data; or
- processor of Customer Personal Data on behalf of another controller.

3.2 Hanko role

Hanko acts as processor of Customer Personal Data.

Where the Customer acts as a processor, Hanko acts as the Customer's subprocessor.

3.3 Customer acting as processor

Where the Customer acts as a processor, the Customer confirms that:

- the relevant controller has authorized the Customer to appoint Hanko as a subprocessor;
- the Customer is authorized to issue instructions to Hanko;
- the Customer's instructions are consistent with the instructions of the relevant controller; and
- the Customer will communicate all relevant controller instructions to Hanko.

3.4 Compliance

Each Party is responsible for complying with the obligations applicable to it under Applicable Data Protection Law.

3.5 Account Data

Hanko acts as an independent controller when processing Account Data.

Account Data is governed by Hanko's Privacy Policy and is not subject to this DPA.

4. Customer Instructions and Responsibilities

4.1 Processing on instructions

Hanko will process Customer Personal Data only:

- on documented instructions from the Customer;
- as necessary to provide, operate, secure and support the Services in accordance with those instructions; or
- where required by applicable law.

4.2 Documented instructions

The Customer's documented instructions include:

- this DPA and the Terms;
- the Customer's selection, configuration and use of the Services;
- instructions submitted through Hanko Cloud or its APIs;
- support requests made by authorized representatives of the Customer; and
- additional written instructions agreed between the Parties.

4.3 Legally required processing

If applicable law requires Hanko to process Customer Personal Data other than on the Customer's instructions, Hanko will inform the Customer before the processing unless the law prohibits such notification.

4.4 Unlawful instructions

Hanko will inform the Customer without undue delay if, in Hanko's opinion, an instruction infringes Applicable Data Protection Law.

Hanko may suspend the affected processing until the Parties have clarified or amended an instruction that Hanko reasonably considers unlawful.

4.5 Customer responsibilities

The Customer is responsible for:

- the lawfulness of the collection and processing of Customer Personal Data;
- establishing an appropriate legal basis for the processing;
- providing legally required information to data subjects;
- handling requests from data subjects;
- ensuring that its instructions to Hanko are lawful;
- configuring and using the Services in compliance with Applicable Data Protection Law;
- ensuring that it is authorized to provide Customer Personal Data and issue instructions to Hanko; and
- ensuring that any personal data submitted through configurable fields is appropriate for the Customer's use of the Services.

4.6 Special categories of data

The Services do not require the Customer to provide:

- special categories of personal data within the meaning of Article 9 GDPR; or
- personal data relating to criminal convictions and offences within the meaning of Article 10 GDPR.

The Customer must not intentionally provide such data through user metadata or other freely configurable fields unless:

- the processing is lawful and necessary;
- the Customer has established an appropriate legal basis; and
- the Customer has implemented appropriate safeguards.

5. Confidentiality

5.1 Authorized personnel

Hanko will ensure that persons authorized to process Customer Personal Data:

- process it only as necessary for their assigned duties;
- receive appropriate data protection and information security instructions; and
- are subject to contractual or statutory confidentiality obligations.

5.2 Access restrictions

Hanko will restrict access to Customer Personal Data according to the principles of least privilege and need to know.

6. Security of Processing

6.1 Security measures

Hanko will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data against:

- accidental or unlawful destruction;
- loss or alteration;
- unauthorized disclosure or access; and
- other unlawful processing.

6.2 Technical and organizational measures

The technical and organizational measures applicable to the Services are described in Schedule 2.

6.3 Changes to security measures

Hanko may update its technical and organizational measures to reflect:

- technical developments;
- changes to the Services;
- changes in the relevant risks; and
- improvements to Hanko's security controls,

provided that the overall level of protection is not materially reduced.

7. Assistance to the Customer

7.1 Scope of assistance

Taking into account the nature of the processing and the information available to Hanko, Hanko will reasonably assist the Customer with:

- responding to requests from data subjects exercising their rights;
- ensuring compliance with applicable security obligations;
- notifying supervisory authorities and affected data subjects of Personal Data Breaches;
- conducting data protection impact assessments; and
- prior consultations with competent supervisory authorities.

7.2 Data subject requests

If Hanko receives a request from a data subject concerning Customer Personal Data, Hanko will refer the data subject to the Customer unless:

- the Customer has authorized Hanko to respond directly; or
- Hanko is legally required to respond.

7.3 Verification

Hanko may require reasonable verification that a person requesting assistance is authorized to act on behalf of the Customer.

8. Personal Data Breaches

8.1 Notification

Hanko will notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data.

8.2 Information

To the extent available, the notification will include:

- a description of the nature of the Personal Data Breach;
- the categories and approximate number of data subjects affected;
- the categories and approximate number of data records affected;
- the likely consequences of the Personal Data Breach;
- the measures taken or proposed to address and mitigate the Personal Data Breach; and
- a contact point for further information.

8.3 Phased information

Where all relevant information is not immediately available, Hanko may provide the information in phases as it becomes available.

8.4 No admission

Notification of a Personal Data Breach does not constitute an acknowledgement of fault or liability.

9. Subprocessors

9.1 General authorization

The Customer grants Hanko general authorization to engage Subprocessors for the processing described in this DPA.

9.2 Current Subprocessors

The Subprocessors authorized by the Customer are listed in Schedule 3.

9.3 Providers listed before use

An authorized Subprocessor may be listed before it begins processing Customer Personal Data, including where Hanko is preparing:

- a migration between infrastructure providers;
- a replacement of an existing Subprocessor; or
- additional infrastructure capacity.

Listing a Subprocessor does not necessarily mean that the Subprocessor is already processing Customer Personal Data.

9.4 Contractual obligations

Hanko will enter into a written agreement with each Subprocessor that imposes data protection obligations providing a level of protection substantially equivalent to the obligations imposed on Hanko under this DPA.

9.5 Responsibility

Hanko remains responsible to the Customer for the performance of its Subprocessors' data protection obligations.

9.6 Notice of changes

Hanko will notify the Customer of an intended addition or replacement of a Subprocessor at least 14 days before the new Subprocessor begins processing Customer Personal Data.

Notification may be sent to the email address associated with the Customer's Hanko Cloud account.

9.7 Right to object

The Customer may object to a new Subprocessor during the notice period where the Customer has reasonable grounds relating to the protection of Customer Personal Data.

An objection must:

- be submitted in writing to `privacy@hanko.io`;
- identify the relevant Subprocessor; and
- explain the Customer's data protection concerns.

9.8 Resolution

Hanko and the Customer will work in good faith to resolve a valid objection.

Hanko may address an objection by:

- deciding not to use the Subprocessor for the Customer's processing;

- implementing additional safeguards;
- offering a commercially reasonable alternative; or
- allowing the Customer to terminate the affected Services before the Subprocessor begins processing Customer Personal Data.

9.9 No objection

If the Customer does not object within the notice period, the Customer is deemed to have authorized the new Subprocessor.

10. Data Location

10.1 Storage location

Customer Personal Data is stored exclusively in data centers located in Germany.

10.2 Processing and access

Hanko processes Customer Personal Data only within the European Economic Area and does not permit access to Customer Personal Data from outside the European Economic Area.

10.3 Customer-directed transmissions

Sections 10.1 and 10.2 do not restrict:

- access initiated by the Customer or its authorized users from locations selected by the Customer;
- access by data subjects using the Customer's applications or services;
- the transmission of authentication emails or other messages to recipients designated by the Customer;
- transmissions to external identity providers configured by the Customer;
- transmissions to systems integrated by the Customer; or
- other transmissions initiated or instructed by the Customer.

10.4 Changes to locations

Hanko will notify the Customer in advance of any intended change to the storage or processing locations.

10.5 Future international transfers

Any future transfer of Customer Personal Data outside the European Economic Area by Hanko or its Subprocessors will take place only:

- in accordance with Applicable Data Protection Law;
- on the basis of a legally recognized transfer mechanism; and

- subject to any supplementary safeguards required by Applicable Data Protection Law.

11. Return, Export and Deletion

11.1 Retention during the term

During the term of the Services, Hanko retains Customer Personal Data until:

- the Customer submits a documented deletion request to Hanko; or
- the Customer's Hanko Cloud account is terminated.

Hanko does not automatically delete Customer Personal Data from active production systems merely because particular data has not recently been accessed or used.

11.2 Export

The Customer may request a complete export of Customer Personal Data by contacting Hanko.

For security purposes, Hanko may require reasonable verification that the person requesting the export is authorized to act on behalf of the Customer.

Hanko will provide the export:

- in a commonly used, machine-readable format; and
- through an appropriately secure transfer method.

The export will include the Customer Personal Data and relevant project configuration required to migrate the Customer's projects from Hanko Cloud to a self-hosted Hanko deployment without loss of:

- stored user accounts;
- external identities;
- authentication credentials; or
- relevant project configuration.

Because the export may contain security-sensitive authentication data, including password hashes, TOTP secrets and authentication tokens, Hanko may apply additional:

- identity and authorization verification;
- encryption; and
- secure transfer requirements

before providing the export.

11.3 Deletion during the term

Following a documented deletion request, Hanko will delete the relevant Customer Personal Data from its active production systems within 30 days unless applicable law requires continued retention.

Customer Personal Data remaining in backups will:

- not be used for ordinary processing; and
- be deleted or overwritten within 14 days after deletion from the active production systems.

11.4 Return or deletion following termination

Following termination of the Customer's Hanko Cloud account, Hanko will retain Customer Personal Data for up to 30 days to allow the Customer to request an export.

The Customer may request earlier deletion during this period.

Unless the Customer requests an export or earlier deletion, the Customer instructs Hanko to delete Customer Personal Data from its active production systems no later than 30 days after termination of the account.

Customer Personal Data remaining in backups will be deleted or overwritten within 14 days after deletion from the active production systems.

11.5 Legally required retention

If applicable law requires Hanko to retain Customer Personal Data, Hanko will:

- inform the Customer where legally permitted;
- restrict the retained data from further processing except as required by law; and
- delete the retained data when the applicable retention requirement ends.

11.6 Account Data

This Section does not apply to Account Data processed by Hanko as an independent controller.

12. Information and Audits

12.1 Compliance information

Hanko will make available to the Customer the information reasonably necessary to demonstrate compliance with:

- this DPA; and
- the processor obligations under Applicable Data Protection Law.

12.2 Forms of evidence

Hanko may provide this information through:

- security and compliance documentation;
- audit reports or certifications;
- responses to reasonable questionnaires; or
- other appropriate evidence.

12.3 Customer audits

Where the information provided under Section 12.2 is not reasonably sufficient, or where the Customer has substantiated grounds to suspect material non-compliance, the Customer may conduct an audit subject to the following conditions:

- the audit must relate to processing under this DPA;
- the Customer must provide at least 30 days' prior written notice;
- audits may normally be conducted no more than once in any 12-month period;
- the audit must take place during normal business hours;
- the audit must not unreasonably disrupt Hanko's operations;
- the auditor must be independent, appropriately qualified and bound by confidentiality; and
- the Customer bears the costs of the audit, including Hanko's reasonable costs of supporting the audit.

12.4 Exceptions

The restrictions in Section 12.3 do not apply where an audit:

- is required by a competent supervisory authority;
- follows a confirmed material Personal Data Breach; or
- is reasonably necessary due to substantiated evidence of material non-compliance.

12.5 Auditor conflicts

Hanko may reject an auditor that:

- is a direct competitor of Hanko;
- lacks appropriate qualifications; or
- cannot provide adequate confidentiality assurances.

Hanko will not unreasonably withhold approval of an alternative qualified auditor.

13. Duration and Termination

13.1 Duration

This DPA applies for as long as Hanko processes Customer Personal Data on behalf of the Customer.

13.2 Downgrade to a free plan

Termination or expiry of a paid subscription does not terminate this DPA if the Customer continues to use a free Hanko Cloud plan.

13.3 End of the DPA

This DPA ends when:

- the Customer's Hanko Cloud account and all associated projects have been terminated; and
- Hanko has returned or deleted the Customer Personal Data in accordance with Section 11.

13.4 Survival

Provisions that by their nature are intended to survive termination continue to apply for as long as Hanko retains Customer Personal Data.

14. Changes to this DPA

14.1 Permitted updates

Hanko may update this DPA where reasonably necessary to:

- comply with applicable law;
- reflect changes to the Services or processing activities;
- update security measures or Subprocessors;
- correct errors; or
- improve clarity.

14.2 Level of protection

Updates must not materially reduce the protection of Customer Personal Data.

14.3 Notice

Hanko will notify the Customer of material changes by email or through Hanko Cloud.

Unless a shorter period is required by law, a material change will take effect no earlier than 30 days after notification.

14.4 Customer objection

If the Customer reasonably objects to a material change that adversely affects the protection of Customer Personal Data, the Customer may terminate the affected Services before the change takes effect.

14.5 Subprocessors

Changes to the list of Subprocessors are governed by Section 9.

15. General Provisions

15.1 Liability

The liability of the Parties under this DPA is governed by the limitations and exclusions of liability in the Terms, to the extent permitted by Applicable Data Protection Law.

15.2 Severability

If any provision of this DPA is invalid or unenforceable, the remaining provisions remain effective.

The Parties will replace an invalid or unenforceable provision with a valid provision that most closely reflects its intended commercial and legal purpose.

15.3 Governing law

This DPA is governed by the laws of the Federal Republic of Germany.

15.4 Jurisdiction

The courts having jurisdiction under applicable law will have jurisdiction over disputes arising from or relating to this DPA.

Where the Customer is:

- a merchant;
- a legal entity under public law; or
- a special fund under public law,

the courts at Hanko's registered office have exclusive jurisdiction to the extent legally permitted.

15.5 Notices

Notices and requests under this DPA must be sent:

To Hanko: `privacy@hanko.io`
To the Customer: the email address associated with the Customer's Hanko Cloud account.

Schedule 1

Details of the Processing

1. Subject Matter

The provision, operation, security and support of Hanko Auth and Hanko Passkey API through Hanko Cloud.

2. Duration

For the duration of the Customer's use of the Services and until Customer Personal Data has been returned or deleted in accordance with this DPA.

3. Nature and Purpose

Depending on the Services selected and configured by the Customer, Hanko may perform the following processing activities:

- receiving, recording, storing, structuring and retrieving user information;
- registering and managing users and identities;
- storing and verifying authentication credentials;
- authenticating users;
- managing passwords, passcodes, passkeys and multi-factor authentication methods;
- integrating external OAuth, OIDC and SAML identity providers;
- linking external identities to Hanko user accounts;
- issuing, managing and validating sessions and authentication tokens;
- managing passkey and WebAuthn credentials;
- preventing unauthorized access and detecting misuse;
- maintaining authentication, security and operational logs;
- transmitting transactional authentication emails;
- providing support and troubleshooting;
- backing up and restoring the Services; and
- exporting, migrating or deleting Customer Personal Data on the Customer's instructions.

4. Categories of Data Subjects

- users and prospective users of the Customer's applications and services;
- the Customer's employees, contractors and representatives where they use the Customer's applications or services;
- individuals whose identities are managed or authenticated through the Services; and
- other individuals whose personal data the Customer submits to the Services.

Hanko Cloud account holders and Hanko Cloud Console users are not included solely because they administer a Hanko Cloud account.

Their Account Data is processed by Hanko as an independent controller as described in Section 3.5.

5. Categories of Customer Personal Data

The categories depend on the Customer's configuration and use of the Services.

5.1 Identity and Profile Data

- internal user identifiers;
- email addresses;
- usernames;
- first and last names;
- profile information;
- profile images, where provided;
- freely configurable user metadata;
- identifiers received from external identity providers;
- external provider names and provider user identifiers;
- external identity claims and attributes; and
- relationships between external identities and Hanko user accounts.

5.2 Authentication and Credential Data

- password hashes;
- one-time passcode and authentication challenge information;
- TOTP secrets and related configuration;
- passkey and WebAuthn credential identifiers;
- public keys;
- user handles;
- authenticator names;
- authenticator metadata, including AAGUID and supported transports;

- information about authentication methods configured for a user;
- OAuth and OIDC tokens, identifiers and claims;
- SAML assertions and attributes; and
- other authentication information required to provide the Services as configured by the Customer.

Hanko does not store plaintext passwords.

Private passkey keys and biometric templates remain on the end user's device or authenticator and are not received or stored by Hanko.

5.3 Session, Device and Security Data

- IP addresses;
- timestamps;
- user-agent information;
- operating system, browser, platform and device information;
- session identifiers and session information;
- authentication attempts and results;
- security events;
- connection and request information;
- application diagnostics and error information; and
- technical and operational logs.

5.4 Passkey API Data

- Customer-provided user identifiers;
- relying party identifiers and origins;
- passkey registration and authentication challenges;
- credential identifiers and public keys;
- authenticator metadata;
- transaction and request information submitted for authentication or verification; and
- related technical and security logs.

6. Special Categories of Personal Data

The Services are not designed to require special categories of personal data or personal data relating to criminal convictions and offences.

Such data may be processed if the Customer intentionally submits it through freely configurable metadata or other fields.

The Customer is responsible for determining whether such processing is lawful and whether additional safeguards are required.

7. Frequency of Processing

Continuous for the duration of the Customer's use of the Services.

8. Processing Locations

- **Storage:** Germany
- **Other processing and authorized access:** European Economic Area

---

Schedule 2

Technical and Organizational Measures

Hanko maintains technical and organizational measures appropriate to the nature of the Services, the Customer Personal Data processed and the relevant risks.

1. Information Security Governance

- documented information security responsibilities and policies;
- risk-based assessment of technical and organizational controls;
- confidentiality obligations for personnel;
- security awareness and role-appropriate training;
- processes for onboarding, role changes and termination of personnel access; and
- assessment of relevant service providers and Subprocessors.

2. Access Control

- unique accounts for personnel with access to production systems;
- access granted according to least-privilege and need-to-know principles;
- multi-factor authentication for privileged or security-relevant access;
- role-based authorization;
- controlled management of administrative credentials and secrets;
- periodic review of access rights; and
- prompt revocation of access that is no longer required.

3. Encryption and Credential Protection

- encryption of data in transit using current transport encryption protocols;
- encryption mechanisms for production storage and backups;
- secure storage and management of cryptographic keys and secrets;

- storage of passwords only in hashed form using appropriate password-hashing methods;
- no storage of plaintext passwords;
- no receipt or storage of passkey private keys; and
- no receipt or storage of biometric templates used by an end user's device or authenticator.

4. Tenant Isolation

- a multi-tenant architecture using shared infrastructure and databases;
- logical association of data with the relevant Customer project or tenant;
- authorization controls designed to ensure that users and administrators can access only the projects and data they are permitted to access;
- controls designed to prevent unauthorized access across Customer projects or tenants; and
- separation of production, testing and development environments where appropriate.

5. Secure Development and Change Management

- source-code version control;
- peer review and automated testing appropriate to the relevant change;
- controlled deployment and change-management processes;
- dependency and vulnerability monitoring;
- security updates and patch management;
- protection of development and deployment credentials; and
- investigation and remediation of identified security vulnerabilities.

6. Logging and Monitoring

- logging of security-relevant system and administrative events;
- monitoring of service health and availability;
- detection and investigation of suspicious or unauthorized activity;
- protection of logs against unauthorized access and modification; and
- operational alerting and escalation procedures.

7. Availability and Recovery

- regular backups of relevant production data;
- protected and access-controlled backup storage;
- distributed data storage across multiple availability zones;
- documented recovery and continuity procedures;
- monitoring of service availability; and

- periodic review or testing of recovery processes.

8. Incident Management

- documented procedures for identifying, assessing and responding to security incidents;
- internal escalation and defined responsibilities;
- measures to contain, investigate and remediate incidents;
- procedures for assessing whether Customer Personal Data is affected; and
- processes for notifying affected Customers as required by this DPA.

9. Physical Security

Hanko uses professional cloud infrastructure providers responsible for the physical security of the data centers in which the Services are operated.

Relevant measures include:

- controlled physical access;
- monitoring and protection of data center facilities;
- environmental protection;
- power and network redundancy; and
- documented data center security controls.

10. Data Deletion

- documented processes for deleting Customer projects and user data following a Customer request;
- controlled deletion from active systems;
- deletion or overwriting of backup data according to the backup lifecycle;
- access restrictions preventing backup data from being used for ordinary processing; and
- secure disposal or deletion of storage resources where applicable.

Schedule 3

Authorized Subprocessors

The Customer authorizes Hanko to use the following Subprocessors.

Listing a Subprocessor in this Schedule authorizes Hanko to use that Subprocessor but does not necessarily mean that the Subprocessor is already processing Customer Personal Data.

1. Amazon Web Services

Legal entity: Amazon Web Services EMEA SARL
Address: 38 Avenue John F. Kennedy, L-1855 Luxembourg

Processing activities:

- cloud hosting;
- computing;
- databases;
- storage;
- networking;
- backups;
- transactional email delivery through Amazon Simple Email Service (SES); and
- related cloud infrastructure services.

Processing location: Germany

2. adesso as a service

Legal entity: adesso as a service GmbH
Address: Adessoplatz 1, 44269 Dortmund, Germany

Processing activities:

- managed cloud operations;
- infrastructure administration;
- monitoring;
- maintenance;
- technical administration; and
- technical support.

Processing location: Germany

3. Hetzner

Legal entity: Hetzner Online GmbH
Address: Industriestr. 25, 91710 Gunzenhausen, Germany

Processing activities:

- cloud hosting;
- computing;
- databases;
- storage;

- networking;
- backups; and
- related cloud infrastructure services.

Processing location: Germany

Optional Execution Page

This Optional Execution Page relates to the **Hanko Cloud Data Processing Agreement, Version 1.0**.

The DPA is valid and binding without completion or signature of this page.

Unless expressly stated otherwise below, the signatures:

- document the Parties' existing agreement to the DPA;
- do not amend the DPA;
- do not amend the Hanko Cloud Terms; and
- do not change the date on which the DPA became binding.

Customer

Legal name:
[_____]

Legal form:
[_____]

Registered address:
[_____]

[_____]

[_____]

Hanko Cloud email address:
[_____]

Name of signatory:
[_____]

Position or authority:
[_____]

Signature date:
[_____]

Signature:

[_____]

Hanko

Legal name: Hanko GmbH
Address: Ringstraße 19, 24114 Kiel, Germany

Name of signatory:
[_____]

Position:
[_____]

Signature date:
[_____]

Signature:

[_____]