BRANDDECK STANDARD TERMS

Data Processing Agreement

Pursuant to Article 28 GDPR (Auftragsverarbeitungsvertrag / verwerkersovereenkomst)

Document attribute	Value
Document code	BD-DPA-001
Version / issue date	1.0 / November 2026
Status	Standard version. Signature or documented electronic acceptance required
Owner	Snoepfabriek B.V., trading as BrandDeck
Classification	Public, standard terms

Contact Snoepfabriek B.V., trading as BrandDeck | Vondellaan 146, 3521 GH Utrecht, The Netherlands | hello@branddeck.co

How to use this document
This is BrandDeck's standard Data Processing Agreement. Fill in the customer details below, sign it and send it to hello@branddeck.co. We countersign and return a copy. Need a more extensive data protection and security review package (hosting, security, retention and assurance documents)? Ask us at hello@branddeck.co.

Parties

This Data Processing Agreement (DPA) is entered into between:

Party	Details
Controller (the Customer)	Name: _____ Address: _____ Data protection contact: _____
Processor	Snoepfabriek B.V., trading as BrandDeck Vondellaan 146, 3521 GH Utrecht, The Netherlands hello@branddeck.co

1. Scope and incorporation

1.1 This DPA forms part of the agreement under which Processor provides the BrandDeck platform and related services to Controller (the Main Agreement). It applies where Processor processes Personal Data on behalf of Controller.

1.2 If there is a conflict concerning the protection of Personal Data, the following order applies: (a) mandatory data protection law; (b) this DPA and its Annexes; (c) an expressly agreed customer-specific data protection clause in the Main Agreement; and (d) the remaining Main Agreement.

1.3 The Annexes form an integral part of this DPA. No undefined marketing statement reduces a protection or obligation set out in this DPA.

2. Definitions

Term	Meaning
Applicable Data Protection Law	The GDPR, applicable Union or Member State data protection law, and binding requirements of a competent supervisory authority.
Controller	The Customer named above, which determines the purposes and essential means of processing its Personal Data.
Customer Content	Brand guidelines, files, images, video, documents, comments, boards, metadata and other content submitted to or created in the service by or for Controller.
Customer Personal Data	Personal Data processed by Processor on behalf of Controller in connection with the service.
Personal Data Breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.
Processor	Snoepfabriek B.V., trading as BrandDeck.
Sub-processor	A third party engaged by Processor to process Customer Personal Data on behalf of Controller.

Terms such as Personal Data, processing, Data Subject, supervisory authority and special categories have the meanings given in the GDPR.

3. Controller instructions and legal compliance

3.1 Processor will process Customer Personal Data only on documented instructions from Controller, including the instructions in the Main Agreement, this DPA, authorised platform configurations and written directions from authorised Controller contacts.

3.2 Processor will not sell Customer Personal Data, use it for targeted advertising, or use it to train a general-purpose or shared artificial-intelligence model unless Controller gives an explicit, separate documented instruction and all legal, security and contractual conditions are satisfied.

3.3 If Union or Member State law requires processing beyond Controller’s instructions, Processor will inform Controller before processing unless the law prohibits that information for important grounds of public interest.

3.4 Processor will immediately inform Controller if, in its opinion, an instruction infringes Applicable Data Protection Law. Processor may suspend the affected operation while the parties resolve the issue, without using the suspension to avoid lawful instructions.

4. Confidentiality and personnel

4.1 Processor will ensure that persons authorised to process Customer Personal Data are subject to enforceable confidentiality obligations and receive access only where necessary for their tasks.

4.2 Processor will apply role-based access, least privilege, prompt revocation of access and periodic review of privileged and operational access. Personnel will receive appropriate security and privacy instructions.

5. Security of processing

5.1 Processor will implement and maintain the technical and organisational measures in Annex 2, taking account of the state of the art, implementation costs, the nature, scope, context and purposes of processing, and the risks to Data Subjects.

5.2 Processor may update a measure to reflect technical progress, provided the overall level of protection is not materially reduced. Material reductions require Controller's prior written approval.

5.3 Processor will regularly assess the effectiveness of its controls and remediate material deficiencies according to risk. Processor will not state or imply that BrandDeck holds a certification that it does not hold.

6. Data Subject requests

6.1 Processor will, taking into account the nature of processing, assist Controller through appropriate technical and organisational measures to respond to requests under Chapter III GDPR.

6.2 If Processor receives a request concerning Customer Personal Data directly from a Data Subject, it will forward the request to Controller without undue delay and will not respond substantively unless instructed by Controller or required by law.

6.3 Assistance may include search, access, export, correction, restriction, deletion and information needed for Controller to assess the request. Processor may verify that a person giving an instruction is authorised by Controller.

7. Assistance with Articles 32 to 36 GDPR

Processor will provide reasonable assistance, taking into account the nature of processing and the information available to it, concerning security of processing, Personal Data Breach assessment and notification, data protection impact assessments and prior consultation with a supervisory authority.

8. Records, information and regulatory cooperation

8.1 Processor will make available all information reasonably necessary to demonstrate compliance with Article 28 GDPR and this DPA, subject to proportionate protection of other customers, trade secrets and security-sensitive information.

8.2 Processor will cooperate with competent supervisory authorities in relation to processing under this DPA and will inform Controller of a binding authority request concerning Customer Personal Data unless legally prohibited.

9. Personal Data Breaches

9.1 Processor will notify Controller without undue delay after becoming aware of a Personal Data Breach. Processor's operational target for the first notification is no later than 24 hours after awareness, even if not all information is yet available.

9.2 Processor will provide the information listed in Annex 4 in phases without undue further delay, maintain an appropriate update cadence, take reasonable containment and remediation steps, preserve relevant evidence, and support Controller's risk assessment and notification obligations.

9.3 Processor will not notify a supervisory authority or Data Subjects on Controller's behalf unless Controller gives documented authority or Processor is independently required by law. A notification is not an admission of fault or liability.

10. Sub-processors

10.1 Controller grants Processor general written authorisation to engage the Sub-processors listed in Annex 3, solely for the services, data and locations stated there.

10.2 Processor will give at least 30 calendar days' written notice before appointing or replacing a Sub-processor that will process Customer Personal Data. The notice will identify the provider, service, location and relevant transfer safeguard.

10.3 Controller may object during the notice period on reasonable data protection or information-security grounds. The parties will seek a reasonable solution, such as an alternative configuration, provider or safeguard. If no reasonable solution is available and the change is material to the service, Controller may terminate the affected service without penalty before the new Sub-processor begins processing.

10.4 Processor will impose written obligations on each Sub-processor that provide at least the protection required by this DPA. Processor remains fully liable to Controller for the performance of the Sub-processor's data protection obligations.

10.5 No unnamed provider, optional integration or provider marked as not authorised may process Customer Personal Data unless it is added through the procedure above or Controller separately instructs the transfer to its own recipient.

11. International transfers

11.1 The standard configuration uses primary hosting in Germany and an EEA-first processing model. Processor will not intentionally transfer Customer Personal Data outside the EEA, including by remote access, unless the transfer is disclosed, authorised and protected under Chapter V GDPR.

11.2 Where a transfer is not covered by an adequacy decision, Processor will use an appropriate safeguard such as the applicable module of the European Commission Standard Contractual Clauses, assess the transfer context and apply supplementary measures where required.

11.3 Processor will document relevant processing locations and transfer mechanisms in Annex 3 and will notify Controller if the transfer position materially changes.

12. Audits and inspections

12.1 Processor will make available information reasonably necessary to demonstrate compliance and may first provide policies, questionnaires, certifications or independent reports where available.

12.2 Controller may conduct, or appoint an independent qualified auditor to conduct, a reasonable audit of relevant processing and controls. A routine audit requires at least 30 days' notice and is normally limited to once in any 12-month period, unless a breach, supervisory-authority request or material concern justifies an additional audit.

12.3 Audits must protect confidentiality, avoid unreasonable disruption and not expose another customer's data or security-sensitive information. Remote review will be used where it can reasonably meet the objective. Controller bears its own auditor costs. Processor may charge only objectively reasonable incremental costs for an unusually extensive, repetitive or out-of-scope audit, agreed in advance, unless the audit identifies a material breach by Processor.

13. Return and deletion

13.1 During the service and for up to 30 days after termination, Controller may export available Customer Content or request a reasonable return format. Controller remains responsible for completing required exports within this period.

13.2 At Controller's choice, Processor will return or delete Customer Personal Data and existing copies after the service ends, unless law requires retention. After the post-termination period, Processor will delete active production copies without undue delay, except where law requires retention.

13.3 Residual copies in encrypted backups will expire through the standard backup rotation, currently targeted at no more than 14 days after production deletion. Until overwritten, backup copies are isolated from ordinary use and may be restored only for continuity, security or legal purposes.

13.4 On request, Processor will confirm completion of deletion. Data retained under a legal obligation will be isolated, access-restricted and used only for that obligation.

14. Government and law-enforcement requests

Processor will review a request for access to Customer Personal Data, verify its legal basis and scope, challenge requests that are unlawful or disproportionate where reasonably possible, disclose only legally required data, and inform Controller before disclosure unless prohibited by law.

15. Controller responsibilities

Controller is responsible for the lawfulness of its instructions, the legal basis for Customer Personal Data, appropriate privacy information to Data Subjects, the accuracy and minimisation of submitted data, user administration, and secure configuration of sharing and optional integrations.

Controller will not intentionally submit special-category data, criminal-offence data or data about children unless this has been expressly agreed, is lawful and is covered by any additional safeguards reasonably required by Processor.

16. Term, governing law and changes

16.1 This DPA takes effect when signed or otherwise validly accepted and remains in force while Processor processes Customer Personal Data.

16.2 The governing law and competent courts stated in the Main Agreement apply, without limiting mandatory rights or powers under Applicable Data Protection Law. The parties will cooperate in good faith to amend this DPA if legal requirements materially change.

17. Signatures

Controller (the Customer)	Snoepfabriek B.V., trading as BrandDeck
Name: _____	Name: Danny Verroen
Title: _____	Title: Founder
Date: _____	Date: _____
Signature: _____	Signature: _____

Annex 1. Description of processing

Element	Description
Subject matter	Provision, hosting, support, security and administration of the BrandDeck cloud platform for brand guidelines, digital assets, files, boards and collaboration.
Duration	For the term of the Main Agreement plus the export, deletion and backup-expiry periods stated in Section 13.
Purpose	To allow authorised Controller users and invitees to create, organise, store, publish, share, view, download and collaborate on brand-related content.
Nature and operations	Collection, receipt, recording, organisation, structuring, storage, retrieval, consultation, display, sharing under Controller-selected access settings, download, transmission to authorised recipients, logging, backup, recovery, support, restriction and deletion.
Data Subjects	Controller's employees, officials, contractors, temporary staff, suppliers, collaboration partners, invited users and persons identifiable in files, images, video, audio, documents, comments or metadata uploaded by Controller.
Personal Data	Names, business contact details, account identifiers, roles, login and authentication data, IP address, device/browser data, access and audit logs, support communications, comments, approvals, project information, file metadata and personal data contained in Customer Content.
Special categories / criminal data	Not intended for the standard service. Such data may be processed only if expressly agreed in writing, lawfully instructed and protected by additional safeguards.
Processing locations	Primary hosting and storage in Germany. Other access or transfer locations are controlled by Section 11 and Annex 3.
Retention	During the service according to Controller instructions. Post-termination export period up to 30 days; encrypted residual backups currently targeted to expire no later than 14 days after production deletion.
Frequency and volume	Continuous while Controller uses the service. Volume depends on authorised users, workspaces, files, sharing settings and integrations.
Authorised instruction contacts	To be identified in the Main Agreement or implementation record.

Annex 2. Technical and organisational measures

The measures below are the contractual minimum. A control is implemented proportionately to the risk and service architecture. BrandDeck will not present a provider certificate as a certification of BrandDeck itself.

Control area	Minimum measure
1. Governance and accountability	Assigned security and privacy responsibilities; documented policies; risk-based review; remediation tracking; change review for material processing changes.
2. Confidentiality and personnel	Confidentiality obligations; need-to-know access; role-specific awareness; secure onboarding, role change and prompt offboarding.

Control area	Minimum measure
3. Identity and access management	Unique user identities; role-based access control; least privilege; separation of privileged administration from ordinary user access; periodic access review.
4. Authentication and sessions	Secure password handling and reset; session protection; monitoring of suspicious login activity; multi-factor authentication for privileged access where available; optional external identity-provider controls.
5. Encryption	TLS for data in transit; encryption at rest for stored platform data and backups; protected secrets and keys; restricted access to credentials and key material.
6. Tenant and workspace segregation	Logical separation of customer environments; authorisation checks at application and storage layers; controls intended to prevent cross-customer access.
7. Sharing controls	Admins and editors have defined permissions; Controller controls public, protected or email-invite sharing; viewers may be restricted to view/download; draft brands remain private until published.
8. Logging and monitoring	Security-relevant authentication, privileged and administrative events logged where proportionate; log access restricted; monitoring and alerting for material security events.
9. Secure development and change	Version-controlled source code; controlled deployments; review and testing; separation of development and production; protection of secrets; no routine use of production Customer Personal Data in development.
10. Vulnerability and patch management	Dependency and vulnerability monitoring; risk-based remediation; timely security updates; periodic technical testing proportionate to the service risk.
11. Backup and recovery	Regular automated encrypted backups stored separately from primary data. The current published operational baseline describes daily server, database and file backups with approximately 14 days of restore points.
12. Availability and continuity	Professional data-centre infrastructure; redundancy and capacity measures appropriate to the service; documented restoration and incident-recovery process; periodic recovery validation.
13. Incident response	Detection, triage, containment, evidence preservation, eradication, recovery, customer communication and lessons learned; escalation under Section 9.
14. Data lifecycle and deletion	Data minimisation; controlled retention schedule; customer export; production deletion; encrypted backup rotation; isolation of legal holds; deletion confirmation on request.
15. Supplier management	Due diligence, Article 28 terms where applicable, location and transfer assessment, breach notification duties, change control and periodic review.
16. Physical and environmental controls	Reliance on professional hosting-provider data-centre controls including restricted physical access, environmental monitoring, power/network resilience and secure media handling.
17. Audit and continuous improvement	Information to demonstrate compliance; customer audit cooperation; review after material incidents or changes; proportionate improvement of controls.

Annex 3. Sub-processor and recipient register

A provider is a Sub-processor only where it processes Customer Personal Data on BrandDeck's behalf. A customer-selected integration or independent controller is not automatically a Sub-processor. No provider not listed below may process Customer Personal Data unless added under Section 10.

Provider	Service and data	Location / transfer	Status
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen, Germany	Hosting infrastructure for the BrandDeck platform. May process Customer Content, account data, logs and technical metadata as hosted.	Germany / EEA. Article 28 terms apply. No standard third-country transfer is intended.	Authorised Sub-processor for the standard hosted service.
Supabase Pte. Ltd. 65 Chulia Street #38-01/03 OCBC Centre Singapore, 049513	Managed PostgreSQL database containing account data, workspace metadata and Customer Personal Data; provider-managed database backups. Includes Supabase Auth, Storage, Realtime, Edge Functions or Logs only if actually used.	Central EU (Frankfurt).	Authorised Sub-processor for the confirmed Supabase services. Contracting entity established in Singapore. Transfer covered by EU Standard Contractual Clauses under the Supabase Data Processing Addendum, accepted by Processor.

Related service	Classification and condition
Optional Google sign-in	External identity service selected by the user. It is not authorised to receive Customer Content. Controller may disable or prohibit this option in its account instructions.
Customer-selected design or AI integrations	Recipient chosen or enabled by Controller. No transfer of Customer Personal Data is permitted unless Controller gives a documented instruction and the legal, security, retention and transfer conditions are agreed.
Payment and invoicing services	Used for BrandDeck's own customer administration. They are not authorised to access Customer Content. Personal data processed for billing is covered by the Privacy Policy and applicable provider terms.
Marketing communication	Transactional email delivery. May process recipient name, email address, minimum template variables, message metadata, delivery status, bounce information and security/delivery logs. No Customer Content may be included beyond data necessary for the approved message.

BrandDeck will provide an updated list if another provider will process Customer Personal Data. The notification and objection procedure in Section 10 applies.

Annex 4. Minimum Personal Data Breach information

Information	Minimum content
Incident reference and contact	Unique identifier and the BrandDeck incident contact.
Awareness and timeline	Date/time of awareness, known occurrence period, detection method and current status.

Information	Minimum content
Nature of the breach	Confidentiality, integrity and/or availability impact; systems and functions affected.
Data and Data Subjects	Categories and approximate number of Data Subjects and records; affected Controller workspaces or accounts.
Likely consequences	Known or reasonably foreseeable effects and preliminary risk assessment.
Containment and remediation	Measures taken or proposed to contain, mitigate and prevent recurrence.
Evidence	Relevant logs, indicators and preserved evidence, subject to security and third-party confidentiality.
Sub-processor involvement	Provider involved, notification received and actions taken.
Transfer or disclosure	Known recipients, locations and whether unauthorised access or exfiltration is suspected.
Communication	Recommended Controller actions, update cadence and whether an authority or Data Subject has been contacted.

Notification route

Initial notices will be sent to the Controller contact designated in the Main Agreement. Urgent notices to BrandDeck should be sent to hello@branddeck.co with the subject “URGENT - DATA BREACH”.

References

- Regulation (EU) 2016/679, especially Articles 28, 32, 33, 35, 36 and Chapter V.
- BrandDeck Security: branddeck.co/security
- Hetzner Online GmbH legal and data protection information: hetzner.com/legal and docs.hetzner.com.