BIZZDESIGN DATA PROCESSING AGREEMENT

Part 1 – General Provisions

1. Purpose

This Data Processing Agreement (“DPA”) supplements the main agreement entered into between the Customer and Bizzdesign relating to the provision of software and associated services (the “Agreement”).

This DPA sets out the conditions under which Bizzdesign processes Personal Data on behalf of the Customer in connection with the provision of the Services.

In the event of any inconsistency between this DPA and the Agreement with regard to the protection of Personal Data, the provisions of this DPA shall prevail.

The DPA is binding in the original English language only. The English language version of the DPA shall control in the event of a conflict or inconsistency with any translated versions. Any versions of the DPA in any other language are for convenience only.

2. Definitions

In this DPA, the following terms shall have the meanings set out below:

"Affiliate" means, in relation to a party, any entity that directly or indirectly Controls, is Controlled by, or is under common Control with that party, where "Control" means the ownership of, or the ability to direct the exercise of voting rights attached to, more than ten per cent (10%) of the issued share capital or voting rights of an entity, or the ability to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting securities, by contract or otherwise.

"Agreement" means the underlying agreement entered into between Bizzdesign and the Customer for the provision of the Services, to which this DPA is appended and forms part, and pursuant to which this DPA is entered into.

“Applicable Data Protection Law” means any applicable legislation relating to the protection of personal data, including in particular the General Data Protection Regulation.

“Bizzdesign” means the company within the Bizzdesign Group with which the Customer has entered into the Agreement.

“Bizzdesign Group” means the group formed by Bizzdesign B.V., Capitool 15, (7521 PL) Enschede, The Netherlands – ID 08204584.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Customer” means the legal entity or entities that have entered into an agreement with an entity of the Bizzdesign Group for the use of the software, as identified in the applicable agreement, and that determine the purposes and means of the processing of personal data.

“Customer Authorized Affiliate” means any Customer Affiliate (as defined in the Agreement) that Customer has permitted to allow access to and use of the Services by the Affiliates’ employees, contractors, and agents, as described in the Agreement.

“Customer Personal Data” means Personal Data processed by Bizzdesign on behalf of Customer.”

“Data” means any data, including personal data, that is provided, uploaded, transmitted, generated, or otherwise made available by or on behalf of the Customer, or by Users authorized by the Customer, through or in connection with the use of the software.

"Data Subject" means an identified or identifiable natural person to whom Personal Data relates.

“Data Subject Request” means any request, complaint, or communication made by a Data Subject (or by a third party purporting to act on behalf of a Data Subject) to exercise any right available to that Data Subject under applicable data protection law, including any request for access, rectification, erasure, restriction of Processing, data portability, or objection to Processing, and any complaint or enquiry relating to the Processing of that Data Subject's Personal Data.

“Data Protection Laws and Regulations” means all laws and regulations applicable to the Services.

"Personal Data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person , for the avoidance of doubt, limited to such Personal Data processed by Bizzdesign on behalf of the Controller in connection with this Agreement.

“Processing” means any operation or set of operations performed on Personal Data.

"Services" means the services provided by Bizzdesign to the Customer pursuant to, and as more particularly described in, the Agreement.

"Sub-processor" means any third party engaged by the Processor to Process Personal Data on behalf of the Controller for the purposes of providing the Services, whether such third party is another member of the Processor's group of companies or an external third party.

3. Roles of the Parties

The Customer acts as Controller with respect to the Personal Data processed in connection with the Services.

Bizzdesign acts as Processor.

Bizzdesign processes Personal Data solely for the purposes of providing the Services.

Certain entities within the Bizzdesign Group may participate in the provision of the Services.

Such affiliated entities may act as sub-processors.

The list of sub-processors is set out in an annex to this DPA.

4. Data Protection Officer

Bizzdesign has appointed a data protection officer.

The appointed person may be reached at privacy@bizzdesign.com.

5. Customer Instructions

Bizzdesign shall process Personal Data only on documented instructions from the Customer.

The Customer's instructions shall be deemed to include the processing necessary for the performance of the Agreement.

Bizzdesign shall inform the Customer if, in its opinion, an instruction given by the Customer infringes Applicable Data Protection Law.

6. Customer-Controlled Data

The Customer determines the categories of Personal Data processed through the Services.

The Customer remains solely responsible for the content of the data that it chooses to input into the Services.

Bizzdesign exercises no control over the data entered into the Services by the Customer or by authorised users.

The Customer undertakes not to input into the Services any Personal Data whose processing would be contrary to Applicable Data Protection Law.

The Customer undertakes not to input into the Services any special categories of data within the meaning of the General Data Protection Regulation, unless such processing is necessary and lawful.

The Customer shall ensure that any use of the Services involving the processing of Personal Data is based on an appropriate legal basis.

7. Authorized Affiliates

7.1. Contractual Relationship.

The parties acknowledge and agree that, by agreeing to this DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Bizzdesign and each such Authorized Affiliate subject to the provisions of the Agreement and this DPA.

Each Authorized Affiliate agrees to be bound by the obligations set forth in this DPA and, to the extent applicable, the Agreement.
For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA.

All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

7.2. Communication.

The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Navan under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

7.3. Rights of Authorized Affiliates.

Where an Authorized Affiliate becomes a party to the DPA with Bizzdesign, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

- Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Bizzdesign directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together.

- The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Customer Personal Data, take all reasonable measures to limit any impact on Bizzdesign by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

8. Access to Data for Technical Support Purposes

In the course of providing the Services, Bizzdesign may provide technical support services to the Customer.

In order to diagnose or resolve certain technical incidents, it may be necessary for Bizzdesign to access Customer Data on a temporary basis.

Such access shall be limited to situations where it is strictly necessary in order to ensure the maintenance, security or proper functioning of the Services.

Access to Customer Data shall be restricted to duly authorized members of Bizzdesign personnel.

Persons authorized to access Customer Data shall be subject to appropriate confidentiality obligations.

Bizzdesign shall implement technical and organizational measures designed to control and record access to Customer Data.

Such measures may include in particular:
- identity and access management
- access logging
- strong authentication mechanisms
- internal authorization procedures.

Where possible, access to Customer Data shall be carried out under the supervision of the Customer or upon the Customer's instruction.

Where direct access to Customer Data is not necessary, Bizzdesign shall favour the use of test data or pseudonymized data.

Any intervention carried out as part of technical support shall be subject to appropriate traceability.

9. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement.

For the avoidance of doubt, Navan's total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and the DPA shall apply in the aggregate for all claims under both the Agreement and the DPA, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to this DPA.

Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices.

Part 2 – Data Protection

10. Confidentiality

Bizzdesign shall ensure that any person authorized to process Personal Data is subject to an obligation of confidentiality.

Such confidentiality obligation may arise from an employment contract or from a specific contractual undertaking.

Bizzdesign shall ensure that access to Personal Data is restricted to those persons who require such access for the performance of the Services.

11. Reliability

Bizzdesign shall take commercially reasonable steps to ensure the reliability of any Bizzdesign personnel engaged in the Processing of Customer Personal Data.

12. Security Measures

Bizzdesign shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Such measures are intended in particular to ensure the confidentiality, integrity and availability of Personal Data.

The security measures implemented by Bizzdesign are described in an annex to this DPA.

13. Sub-processing

The Customer provides a general authorisation for Bizzdesign to engage Sub-processors to Process Personal Data on its behalf.

Bizzdesign maintains an up-to-date list of its Sub-processors, made available to the Customer at Bizzdesign Products - List of Subprocessors.

Bizzdesign shall ensure that any Sub-processor it engages is bound by a written agreement imposing data protection obligations on that Sub-processor which are substantially equivalent to those imposed on Bizzdesign under this DPA.

Bizzdesign's liability for any act or omission of a Sub-processor shall be subject to the limitations and exclusions of liability set out in the Agreement (including any liability cap), in the same manner as if the relevant act or omission had been committed by Bizzdesign itself.

Bizzdesign may add or replace a Sub-processor at any time. Bizzdesign shall use reasonable efforts to notify the Customer of any material change, but the absence of such notification shall not affect the validity of the appointment.

If the Customer has reasonable, documented data protection grounds to object to a new Sub-processor, it may raise such objection in writing within ten [10] days of the change being published. Bizzdesign shall consider the objection in good faith but retains sole discretion to determine whether and how to address it, including by proposing alternative safeguards. No objection shall entitle the Customer to withhold payment, suspend the Agreement, or claim damages.

Absent a timely objection, the new Sub-processor shall be deemed accepted.

14. International Transfers

In the course of providing the Services, Personal Data may be processed in or accessed from countries located outside the European Economic Area.

Where Personal Data is transferred to a third country that does not benefit from an adequacy decision of the European Commission, Bizzdesign shall implement appropriate legal mechanisms to govern such transfers.

Such mechanisms may include, in particular, the Standard Contractual Clauses adopted by the European Commission pursuant to the General Data Protection Regulation.

Where necessary, Bizzdesign shall ensure that appropriate supplementary safeguards are implemented in order to ensure a level of protection of Personal Data that is essentially equivalent to that guaranteed within the European Union.

Where international transfers result from the involvement of sub-processors or cloud infrastructure providers used in connection with the Services, such transfers shall likewise be governed by appropriate legal mechanisms.

Bizzdesign shall provide the Customer, upon reasonable request, with information relating to the legal mechanisms used to govern such transfers.

Bizzdesign may update the transfer mechanisms used in order to take into account developments in applicable legislation or decisions of competent data protection authorities.

Part 3 – Cloud Infrastructure

15. Cloud Infrastructure

The provision of the Services relies on the use of cloud infrastructure operated by third-party infrastructure providers.

The primary infrastructure providers used for the hosting and operation of the Services are Amazon Web Services and Microsoft Azure.

These infrastructure providers supply essential services to the Processor, including in particular hosting services, computing capacity, storage services and network services required for the provision of the Services.

The Customer acknowledges that the provision of the Services depends on the proper functioning of the infrastructure operated by such infrastructure providers.

Bizzdesign shall remain responsible towards the Customer for the proper performance of its obligations under the Agreement and this DPA.

Bizzdesign shall ensure that the infrastructure providers it engages offer appropriate guarantees with respect to security and data protection.

Bizzdesign shall enter into contractual arrangements with such infrastructure providers including obligations relating to security and data protection in accordance with the requirements of Applicable Data Protection Law.

The use of such infrastructure providers shall be considered a normal and necessary component of the provision of cloud-based IT services.

16. Data Location and Cloud Infrastructure Transparency

Bizzdesign shall provide the Customer with information regarding the geographic regions in which Customer Data may be hosted or processed.

Bizzdesign shall endeavour to host Customer Data in data centres located within the European Economic Area where this is technically feasible and compatible with the architecture of the Services.

The Services may be provided through infrastructure operated by cloud infrastructure providers such as Amazon Web Services or Microsoft Azure.

Data may be replicated across multiple data centres in order to ensure the resilience and continuity of the Services.

Where Personal Data is transferred outside the European Economic Area, such transfers shall be governed by appropriate legal mechanisms.

Such mechanisms may include, in particular, the Standard Contractual Clauses adopted by the European Commission pursuant to the General Data Protection Regulation.

Bizzdesign shall inform the Customer of any material change relating to the geographic regions used for the processing or hosting of Customer Data.

17. Limitation of Cloud Infrastructure Audits

The Customer may verify Bizzdesign's compliance with the obligations set out in this DPA.

Such verification may be carried out through the review of documentation relating to the security of the Services.

Such verification may also be carried out through the review of independent audit reports or security certifications.

Depending on the software subject to the Agreement, the certifications that may be made available may include ISO 27001 and SOC 2 Type II certifications.

With respect to cloud infrastructure operated by third-party infrastructure providers such as Amazon Web Services or Microsoft Azure, physical audits of the data centres operated by such providers shall not be permitted.

Bizzdesign shall make available to the Customer the audit reports and security certifications made available by such infrastructure providers.

Any audit request submitted by the Customer shall be reasonable, proportionate and limited to systems directly operated by Bizzdesign in connection with the provision of the Services.

Such limitations are intended to preserve the security and integrity of the shared cloud infrastructure used to provide the Services.

Any audit shall be subject to additional charges.

The Customer acknowledges that Bizzdesign shall not be held responsible for any limitations affecting audit rights imposed by the third-party infrastructure provider.

Part 4 – Enhanced Regulatory Obligations

18. Personal Data Breach and ICT Incident Notification

Bizzdesign shall notify the Customer of any Personal Data Breach without undue delay after becoming aware of it.

Such notification shall include the information necessary to enable the Customer to comply with its legal obligations.

Bizzdesign shall also notify the Customer of any ICT incident likely to materially affect the availability, integrity or security of the Services.

Such notification is intended in particular to enable the Customer to comply with regulatory requirements applicable to financial institutions.

Such requirements may include those arising under the Digital Operational Resilience Act.

19. Regulatory Assistance

Bizzdesign shall provide reasonable assistance to the Customer in order to enable the Customer to respond to requests for the exercise of data subjects' rights.

Upon Customer's request, Bizzdesign shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligations under the EU GDPR to carry out a data privacy impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Bizzdesign.

Bizzdesign shall provide reasonable assistance to Customer in cooperation or prior to consultation with the Supervisory Authority in the performance of its tasks relating to this DPA, to the extent required under the applicable laws.

20. Requests for Access to Data by Public Authorities

If Bizzdesign receives a legally binding request from a public authority seeking access to Customer Data, Bizzdesign shall inform the Customer without undue delay, unless such notification is prohibited under applicable law.

Bizzdesign shall assess the legal validity of any access request received.

Bizzdesign shall endeavour to limit the disclosure of data to what is strictly necessary to comply with the request of the competent authority.

Where possible, Bizzdesign shall cooperate with the Customer in order to enable the Customer to challenge or limit the scope of the request.

21. Business Continuity

The Processor shall implement appropriate measures designed to ensure the continuity and resilience of the Services.

Such measures may include, in particular, infrastructure redundancy mechanisms, data backup procedures and disaster recovery plans.

Where business continuity arrangements applicable to the Services are described in the Agreement or in the Services documentation, such provisions shall prevail.

Where specific business continuity requirements are requested by the Customer, these may be addressed through a separate agreement between the Parties.

The Processor shall reasonably cooperate with the Customer in order to enable the Customer to comply with its regulatory obligations relating to business continuity and operational resilience.

Such cooperation may include the provision of information relating to the continuity and recovery mechanisms applicable to the Services.

Where the Services rely on cloud infrastructure operated by infrastructure providers such as Amazon Web Services or Microsoft Azure, certain business continuity measures may depend on the technical capabilities made available by such providers.

The Processor shall implement the Services taking into account the resilience features offered by such cloud infrastructure.

22. Cooperation with Competent Authorities

Bizzdesign acknowledges that certain Customers may be subject to specific regulatory obligations applicable to financial institutions.

Such obligations may include requirements relating to the outsourcing of critical or important functions.

Bizzdesign shall reasonably cooperate with the Customer in order to enable the Customer to comply with the regulatory obligations applicable to it.

Such cooperation may include the provision of information relating to security, service continuity and the management of risks associated with the Services.

Where required by Applicable Law, Bizzdesign may provide the Customer with the information necessary to enable competent supervisory authorities to exercise their oversight functions.

Such cooperation may include the provision of documentation relating to security measures, operational procedures and incident management mechanisms.

Any request for information originating from a supervisory authority shall be handled in accordance with the confidentiality and security obligations applicable to the Processor.

Bizzdesign shall not be required to grant direct access to its infrastructure or to the infrastructure of its cloud infrastructure providers where such access would be incompatible with the security requirements applicable to such infrastructure.

Where the Services rely on infrastructure operated by cloud infrastructure providers such as Amazon Web Services or Microsoft Azure, the information made available may include audit reports and security certifications provided by such providers.

Part 5 – Rights of Data Subjects

23. Data Subject Request.

Bizzdesign shall, to the extent legally permitted, promptly notify Customer if it receives a Data Subject Request.

Taking into account the nature of the Processing, shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Bizzdesign shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Customer is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations.

To the extent legally permitted, Customer shall be responsible for any non-negligible costs arising from Navan's provision of such assistance.

Part 6 – End of the Agreement

24. Return and Deletion of Data

Subject to the terms and conditions set out in the Agreement and associated service level agreement, Bizzdesign shall (i) return Customer Personal Data in its possession to Customer; or (ii) to the extent allowed by applicable law, delete Customer Personal Data and existing copies of Customer Personal Data in its possession.

25. Contractual Hierarchy

In the event of any inconsistency between this DPA and any other contractual provision relating to data protection, the provisions of this DPA shall prevail.

26. Annexes

Annex 1 — Description of Processing Activities
Annex 2 — Technical and Organizational Measures

Annex 1 — Description of Processing Activities

1. Subject Matter of the Processing

The processing concerns the provision of the software solution to the Customer on a software-as-a-service (SaaS) basis, including hosting, maintenance, support, monitoring, and related professional services.

2. Duration of the Processing

The Processing shall be carried out for the duration of the applicable agreement(s) between the Customer and Bizzdesign, and, where applicable, for any additional period necessary for data backup, archiving, or compliance with applicable legal obligations, as set out in the Agreement and this DPA.

3. Nature and Purpose of the Processing

3.1. Nature of the Processing

The Processing operations include, as applicable:
- collection, recording, organization, structuring;
- storage, hosting, and backup;
- consultation, use, and retrieval;
- restriction, erasure, or destruction.

3.2. Purpose of the Processing

The Processing is carried out solely for the purposes of:
- providing access to and use of the Software;
- operating, maintaining, securing, and improving the Software;
- providing customer support, incident management, and technical assistance;
- complying with documented instructions from the Customer.

4. Categories of Data Subjects

Depending on the Customer's use of the Software, the Data Subjects may include:
- Customer point of contacts;
- Customer users;
- any other individuals whose personal data is processed by the Customer through the Software.

5. Categories of Personal Data

The Personal Data processed may include:
- identification data (name, surname);
- contact details (business mail / email address and phone number);
- professional data (job title, department, role);
- usage data and technical data (IP address).

The software is not intended to process special categories of personal data, unless the Customer decides to upload such data under its sole responsibility and instructions.

6. Processing Operations

Processing operations include any operation necessary to provide the Software and related services, such as hosting, data storage, technical administration, customer support, incident resolution, and additional services as the case may be subject to a specific agreement between Bizzdesign and Customer.

Annex 2 — Technical and Organizational Measures

This document applies to all Bizzdesign SaaS products: Bizzdesign Horizzon, Bizzdesign HOPEX, Bizzdesign Alfabet, and Bizzdesign Unify. All products are delivered as Software as a Service (SaaS), are independently audited under SOC 2 standards, and are aligned with ISO/IEC 27001 principles.

Measures for user identification and authorisation
- Two-factor authentication (MFA) enabled for all Bizzdesign SaaS products across the entire information system.
- Strict user and access lifecycle processes implemented: access provisioned on onboarding, revoked upon role change or departure.
- Access Control Lists (ACLs) and user groups established in cloud IAM systems with incompatibility rules enforced.
- Individual user credentials issued per staff member — shared accounts prohibited; user IDs cannot be re-assigned.
- Regular review of all access rights: at minimum annual review for all products.
- Password policy enforced across all products: minimum length, complexity requirements, and periodic rotation.
- Workstation automatic timeout with mandatory re-authentication.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Security level of all cloud providers verified before engagement and re-assessed annually.
- Two-factor authentication enabled for the entire information system across all products.
- Strict user and access lifecycle processes implemented for all products.
- Regular security reviews conducted across all products: access reviews, backup integrity reviews, vulnerability reviews.
- Data classification and retention policies implemented to ensure data confidentiality.
- Network segregation implemented between customer traffic and management traffic.
- Intrusion Detection and Prevention Systems (IDPS) deployed across all products.

Restricted access to cryptographic secrets and credentials stored in cloud-native vaults.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Security incident management process implemented for all products.
- Personal data backup policy implemented: automated encrypted daily backups, Recovery Point Objective (RPO) of 24 hours for all products.
- Recovery Time Objective (RTO) defined in accordance with the applicable Service Level Agreement (SLA) for each product available at Terms and Conditions;
- Backups stored in geographically separate locations.
- Disaster Recovery plans maintained for all products; DR environments hosted in separate cloud regions.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
- Regular security reviews implemented across all products: access reviews, backup integrity reviews, vulnerability reviews.
- Security monitoring committees established: Risk, HR, IT, and Legal committees.
- Periodic third-party penetration testing performed for all products.
- Annual internal audits and quarterly control-effectiveness checks by the Global IT & Security Manager.
- All products independently audited under ISAE 3000 / AICPA SOC 2 standards.

Measures for the protection of data during transmission
- All data transmitted over public networks is encrypted using TLS.
- All administrative access sessions encrypted end-to-end across all products.
- Data transmissions logged and monitored for all products.

Measures for the protection of data during storage
- Personal data encrypted at rest across all products using industry-standard encryption (AES-256).
- Encryption keys managed exclusively through cloud-native key management services, with no plain-text access to keys or secrets.
- Strict access management policy implemented, limiting storage access to authorised personnel on a need-to-know basis.
- Customer data and backups never stored on external or removable devices.

Measures for ensuring physical security of locations at which personal data are processed
- Physical security policy implemented — all Bizzdesign SaaS infrastructure is cloud-hosted; no Bizzdesign-operated data centres.
- Cloud data centre physical controls: biometric access, card readers, 24/7 video monitoring, escorted visitor access, environmental controls (fire, temperature, humidity).
- Regular audits of physical entry privileges conducted by respective cloud providers.
- Bizzdesign reviews cloud provider SOC 2 reports annually to verify continued compliance.

Measures for ensuring events logging
- Log management policy implemented across all products with a minimum 365-day log retention.
- Logs centralised in dedicated log repositories for each product.
- Cloud platforms configured to log and collect security events per Bizzdesign policy.

Measures for ensuring system configuration, including default configuration
- Anti-malware agents deployed on all relevant systems across all products; signature definitions updated at least daily.
- Secure gateway implemented for all cloud applications.
- Security patches evaluated and applied on a bi-weekly cycle; critical vulnerabilities addressed with expedited timelines.
- Risk assessments conducted before upgrades or new releases are promoted to production for all products.

Measures for internal IT and IT security governance and management
- Information Systems Security Policy (ISSP) implemented.
- IT Charter implemented covering Security, Availability, and Confidentiality.
- Data Protection Officer (DPO) appointed.
- Development tools and practices aligned with ISO/IEC 27001 controls and described in Bizzdesign's SDLC document.
- Regular review of technical advancements conducted in accordance with Article 32 GDPR.

Measures for certification / assurance of processes and products
- SOC 2 Type 2 — Bizzdesign Horizzon, Bizzdesign Hopex and Bizzdesign Alfabet; infrastructure controls additionally aligned with ISO/IEC 27001.
- SOC 2 Type 1 — Bizzdesign Unify.
- All SOC 2 reports cover Trust Services Criteria for Security, Availability, and Confidentiality, audited under ISAE 3000 / AICPA standards.
- All products identified in this document are within the scope of Bizzdesign's ISO/IEC 27001:2022-certified ISMS.

Measures for ensuring data minimisation
- Categories of personal data collected and processed are enumerated and limited to what is necessary for the stated processing purpose.
- Users given the option to enter only information necessary for the processing purpose.

Measures for ensuring limited data retention
- Data retention policy implemented: customer SaaS tenant data deleted within 90 days after contract termination for all products.
- Audit/event logs retained for a minimum of 365 days across all products.
- Backup copies managed per Backup and Restore Policy.

Measures for allowing data portability and ensuring erasure
- Data reversibility process implemented in case of expiration or termination of contracts for all products.
- Customer data removed upon termination of subscription; removal procedures documented, tested, and verified by auditors.
- Secure erasure of storage media performed upon decommissioning.

Measures of encryption of personal data
Encryption of personal data at rest and in transit implemented across all products, as described under "Measures for the protection of data during transmission" and "Measures for the protection of data during storage" above.
Encryption keys managed via cloud-native key management services, with no plain-text access to keys or secrets.

Measures for ensuring data quality
Input and Output Validation: Systems automatically check data length, type, syntax, and business rules before storing or displaying information.
AI Quality Controls: AI features use human-in-the-loop review, real-time MLOps monitoring for model drift, and never train on customer data.
SDLC Code Quality: Software changes undergo mandatory peer review, automated unit and regression testing, SAST code scanning, and linting before release.

Measures for ensuring accountability
Data Protection Officer (DPO) appointed, as referenced under "Measures for internal IT and IT security governance and management" above.
Records of Processing Activities (RoPA) maintained for all products in accordance with Article 30 GDPR.
Data Protection Impact Assessments (DPIA) conducted for processing operations presenting high risk, in accordance with Article 35 GDPR.
Staff training on data protection and security provided at least annually to all Bizzdesign Group employee.
Security monitoring committees in place to oversee compliance, as referenced under "Processes for regularly testing, assessing and evaluating" above.
Third-party audits (SOC 2, ISO/IEC 27001 alignment) conducted annually and available to demonstrate compliance.