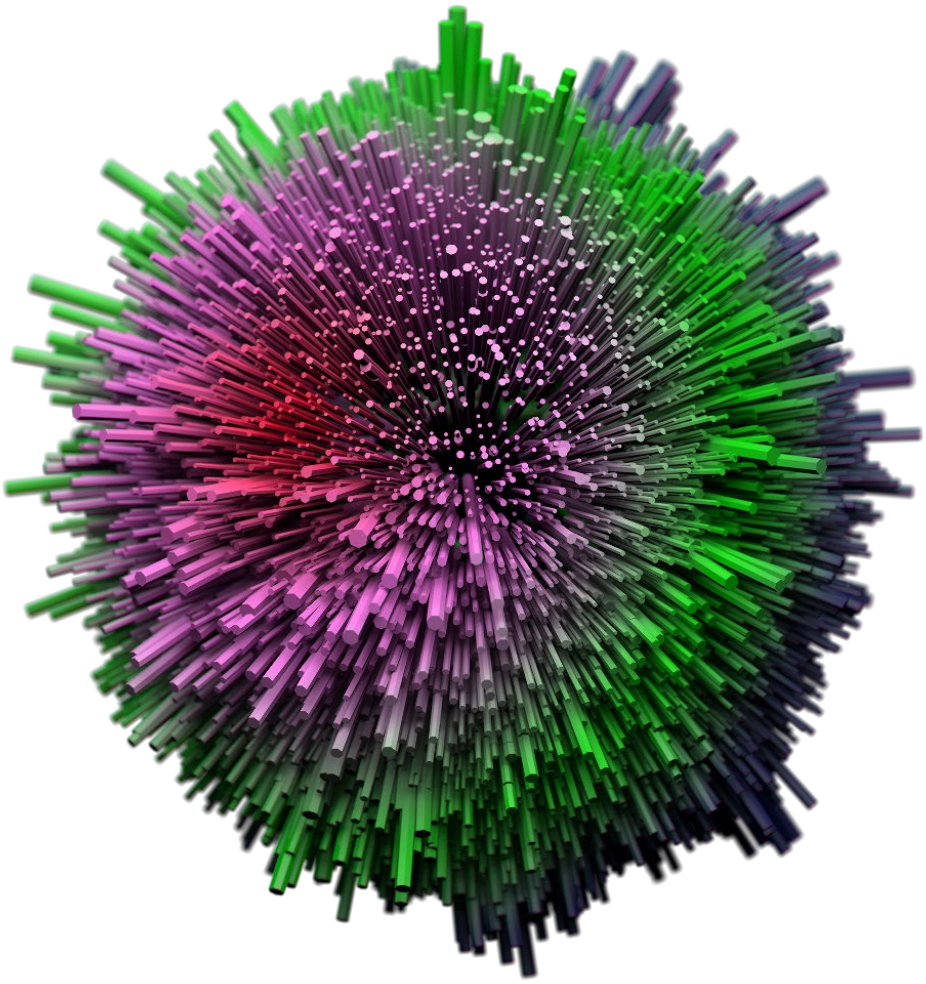
Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR no.: 33 96 35 56
Weidekampsgade 6
DK-2300 Copenhagen S

Phone: +45 36102030
www.deloitte.dk



Bizbrains A/S

Independent auditor's ISAE 3000 assurance report on information security and measures concerning data protection and processing of personal data pursuant to the data processing agreement with Bizbrains A/S's customers covering the period from 7 September 2023 to 7 September 2024.

Table of contents

1. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures concerning data protection and processing of personal data pursuant to the data processing agreement with Bizbrains A/S's customers

To: Bizbrains A/S and Bizbrains A/S's customers that have entered into a data processing agreement with Bizbrains

Scope

We have been engaged to provide assurance on Bizbrains A/S's (hereafter 'Bizbrains') description in section 3 of services in accordance with the data processing agreement with customers that have used Bizbrains's services throughout the period from 7 September 2023 to 7 September 2024 ("the Description") and about the design and operating effectiveness of controls related to the control objectives stated in the Description.

Bizbrains use the following sub-data processers:

- Microsoft Azure in Amsterdam for hosting (primary data centre) of the Link 3.x services
- Microsoft Azure in Dublin for recovery site for the Link 3.x services
- Mentor IT for hosting of the Link 2.x services
- Flowmailer BV for sending emails

Bizbrains's system description does not include control objectives and associated controls at the sub-data processers.

Some of the control objectives described in Bizbrains's description of its system can only be achieved if the complementary controls of customers are suitably designed and implemented together with the controls at Bizbrains. Our opinion does not include the suitability of the design, implementation and operating effectiveness of these complementary controls.

Bizbrains's responsibilities

Bizbrains is responsible for preparing the description and accompanying assertion in section 2, including the completeness, accuracy and the method of presentation of the description and the assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's independence and quality control

We have complied with the requirements for independence and other ethical requirements of IESBA's Code of Ethics for Professional Accountants issued, which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

Deloitte Statsautoriseret Revisionspartnerselskab applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on Bizbrains's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "*Assurance Engagements Other than Audits or Reviews of Historical Financial Information*", and additional requirements under Danish audit regulations to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of Bizbrains's platform, and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the design and operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in section 2.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a data processor

Bizbrains's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Bizbrains's services that the individual data controllers may consider important in their own particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in section 2, "*Management's assertion*". In our opinion, in all material respects:

(a) The description fairly presents Bizbrains's services as designed and implemented throughout the period from 7 September 2023 to 7 September 2024;

(b) The controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 7 September 2023 to 7 September 2024.

(c) The tested controls were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects and operated effectively throughout the period from 7 September 2023 to 7 September 2024.

Description of tests of controls

The specific controls tested, and the nature, timing and results of those tests are listed in section 4 of this report.

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for data controllers who have used Bizbrains's services and who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the General Data Protection Regulation have been complied with.

Copenhagen, 1 November 2024

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR no: 33 96 35 56

Thomas Kühn
Partner, state-authorised public accountant

Michael Bagger
Partner, CISA

2. Management's assertion

Bizbrains processes personal data for our clients in accordance with the data processing agreements.

The accompanying description has been prepared for the data controllers who have used Bizbrains's services and who have a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the General Data Protection Regulation (hereinafter referred to as the Regulation) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data have been complied with. Bizbrains confirms that:

a) The accompanying description in section 3 fairly presents Bizbrains's services which have processed personal data for data controllers subject to the Regulation throughout the period from 7 September 2023 to 7 September 2024. The criteria used in making this assertion were that the accompanying description:

   (i) Presents how Bizbrains's services were designed and implemented, including:

   - The types of services provided, including the type of personal data processed;
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict the processing of personal data;
   - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
   - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
   - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data is deleted or returned to the data controller unless retention of such personal data is required by law or regulations;
   - The procedures supporting, in the event of a breach of personal data security, that the data controller may report this to the supervisory authority and inform the data subjects;
   - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
   - Controls that we, in reference to the scope of Bizbrains's platform, assumed would be implemented by the data controllers and which, if necessary to achieve the control objectives stated in the description, are identified in the description;
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to the processing of personal data.

   (ii) Does not omit or distort information relevant to the scope of the service being described for the processing of personal data, while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Bizbrains's activities that each individual data controller may consider important in its own particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operating effectively throughout the period from 7 September 2023 to 7 September 2024. The criteria used in making this statement were that:

   (i) The risks that threatened the achievement of the control objectives stated in the description were identified;

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 7 September 2023 to 7 September 2024.

c) Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the Regulation.

Copenhagen, 1 November 2024

On behalf of Bizbrains

DocuSigned by:
Nicolai Krog
75C1BB248468423...

Nicolai Krog
CEO

3. System description

Description of processing

This statement pertains to Bizbrains's customers who use Bizbrains's iPaaS platform "Link 3.X." The purpose of Bizbrains's processing of personal data on behalf of the data controller is always based on the agreements "Agreement on Link," "Link Business / Link Enterprise General Terms and Conditions" and APPENDIX 5 - Data Processing Agreement. For Link Essentials, the online version of Data processing agreement is used. It is named Data Processing Agreement for Link Essentials and can be found here: Data Processing Agreement for Link Essentials (bizbrains.com)

3.1 Application / platform / service description

Bizbrains is an iPaaS company and consultancy firm specialising in assisting customers in exchanging EDI data between B2B relationships and applications. Bizbrains handles personal data in the Link 3.x application on behalf of its customers. The Link 3 application is used for exchanging EDI documents and conducting B2B integration.

Document transfers can occur through various protocols and document formats. Bizbrains recommends conducting document transfers through secure protocols such as SFTP, AS2, AS4, etc. Since customers can set up connections for document transfer themselves, it is the customer's responsibility to choose and use encrypted connections.

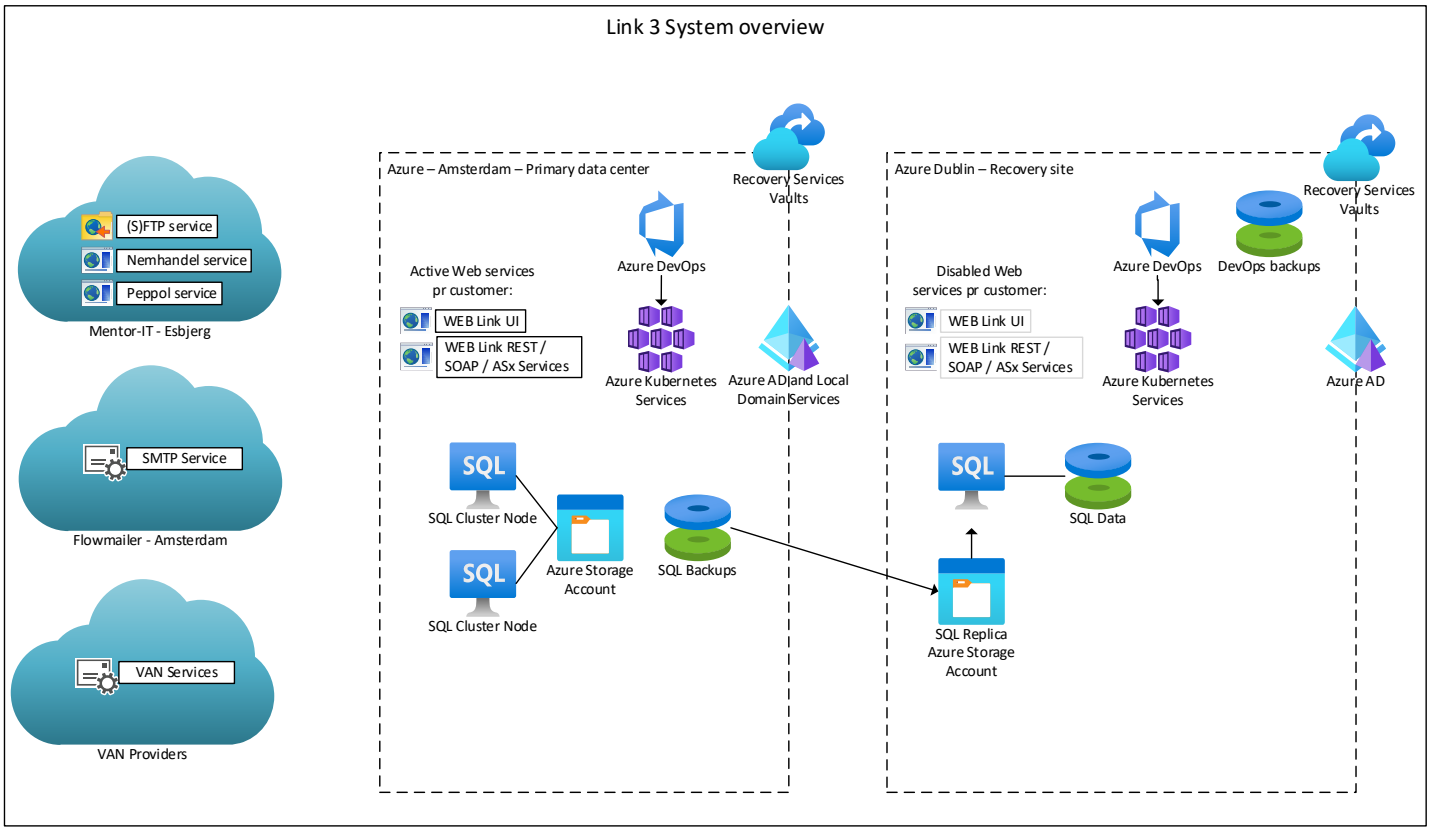
The data controller can be granted rights to manage parts of or the entire single tenant iPaaS solution, Link 3.x, operated by Bizbrains. Access rights can be customised to the individual user's needs via RBAC. Access to the system is typically provided through the data controller's Azure AD authentication.
A data processing agreement is signed with all data controllers. Bizbrains is responsible for developing the software application Link and operating the solution, primarily hosted on the Microsoft Azure platform. The data controller is responsible for the data they choose to process through Link 3. Bizbrains cannot know what data is being sent through the system, as documents can contain anything. If data needs to be searchable, the data controller must ensure that tracking fields are associated with the data. These transport services are hosted on the Mentor-IT platform: (S)FTP, Nemhandel and Peppol. These transport services are hosted on the Flowmailer platform: Outgoing Email (SMTP).

Technical description

Azure Amsterdam - Primary data centre.
Overall description: The engine of Link 3 runs on container technology, orchestrated by Azure Kubernetes services. Each data controller operates within a set of containers under their own namespace. Communication between namespaces is restricted. Each container can scale out, meaning that when there is high load, a new container is started to run in parallel. When consumption is low, the extra containers are turned off. If there are not enough resources available on existing nodes (servers) for the container, additional nodes are automatically started, and resources are allocated to the new container. For example, one container may have the role of creating the user interface, Web Link UI, which the data controller can use to log into the system. Other containers may expose SOAP, AS2, AS4 or REST interfaces for document delivery. This design makes the Link engine highly scalable and automated.
The code for Link 3 is developed and stored in Azure DevOps. Each container communicates with a SQL backend in a clustered setup. Each data controller has their own set of databases, which are encrypted using TDE (Transparent Data Encryption). SQL backups are also encrypted using TDE. Permissions and RBAC (Role-Based Access Control) are managed through Azure AD (Active Directory) / Local Domain services. VM (Virtual Machine) and SQL backups are handled through Azure Recovery Services Vault, protected by Multi-User Authentication / Resource Guard.

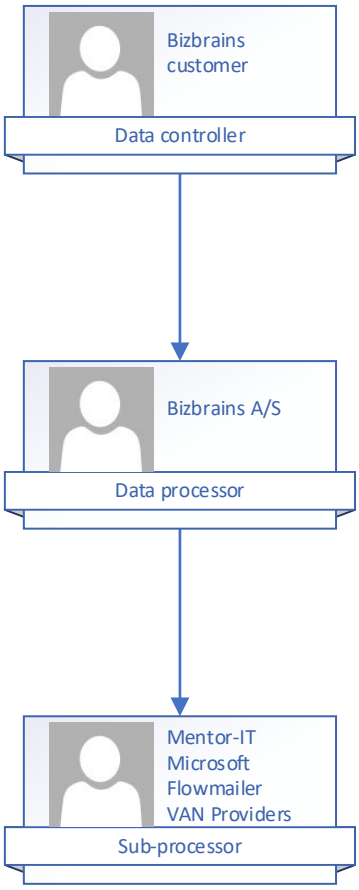
Azure Dublin - Recovery site
The idea behind the recovery site, located in a separate tenant and subscription with its own Azure AD, is for Bizbrains to quickly be able to operate on an emergency system. The Recovery Time Objective (RTO) for this can be as low as 4 hours depending on the agreement. Database backup logs from the

primary site are continuously replicated to an Azure Storage Account in Dublin. Nightly automated restore of the databases means that the heavy part of a recovery scenario is completed, so only transaction log backups need to be loaded. The remaining tasks are to scale up, deploy customer namespaces and update customer DNS pointers.



3.2 Sub-processors

Illustration of the relationship between the data controller, data processor and third-party data processor.



A data processing agreement has been established with the below sub-processors:

Microsoft – Amsterdam and Dublin
The primary datacentre is in Amsterdam. The Disaster Recovery centre is in Dublin. Several services such as virtual machines, storage and Kubernetes services are hosted by Microsoft.

Mentor-IT – Esbjerg
If a customer chooses to use services such as (S)FTP, Nemhandel or Peppol, these are hosted by Mentor-IT.

Flowmailer – Amsterdam
If a customer wishes to use SMTP, i.e., sending documents by email, this service is hosted in Amsterdam by the company Flowmailer.

VAN provider
If a customer chooses to use a VAN provider, the full list of these providers can be found here: https://support.bizbrains.com/subprocessor

3.3 Nature of processing

Bizbrains's processing of personal data on behalf of the data controller is documented through the signed data processing agreements. Bizbrains primarily processes data within three main categories:

1. EDI Documents in Link may contain personal information. It is the data controller who defines what information should be in an EDI document.

2. Technical contact persons can be defined in Link. These individuals are contacted, e.g., in case of failed documents.
3. Users who can log into the system to access documents and technical settings.

3.4 Personal data

The following types of personal data can be processed in Link 3.x:

- General personal data, including identification information such as name, contact details, position, work area and work phone. Usernames, system permissions and system usage logging
- Other personal data may appear in EDI documents, but it is the data controller who defines what personal data is contained in the EDI documents.

Categories of registered individuals covered by the data processing agreement:

- Employees of the data controller
- Customers of the data controller
- Partners of the data controller.

3.5 Risk assessment

Bizbrains conducts an annual risk assessment concerning the system/platform and the utilised sub-contractors to ensure that the necessary precautions are taken so that customer data is not exposed to unnecessary risks.

3.6 Control measures

Bizbrains has implemented controls for the processing of personal data in the following areas:

- Data processing agreements and instructions (control objective A)
- Technical security measures (control objective B)
- Organisational measures (control objective C)
- Deletion and return of personal data (control objective D)
- Retention of personal data (control objective E)
- Use of sub-data processors (control objective F)
- Transfer of personal data to third countries or international organisations (control objective G)
- Assistance to the data controller (control objective H)
- Security breach management (control objective I).

In section 4, the control measures that Bizbrains considers relevant to the processing of personal data are described. Below is a detailed description of a selection of relevant control measures.

3.6.1 General procedures for the processing of personal data (control objective A)

Scope
Procedures and controls are complied with to ensure that instructions relating to the processing of personal data are adhered to in accordance with the data processing agreement.

Procedures and controls used
Bizbrains has implemented a number of policies and procedures that describe how personal data should be processed, thus allowing adequate processing that secures data in relation to confidentiality, integrity and availability and ensuring that personal data is processed only under the instructions of the data controller. All Bizbrains employees are regularly informed of this through training and awareness campaigns.

Procedures are reviewed at least once a year. The timing of the periodic checks and reviews of organisational and technical measures is defined in a GDPR compliance annual wheel and carried out by the operations team.

3.6.2 Technical security measures (control objective B)

Scope
Procedures and controls are complied with to ensure that Bizbrains has implemented technical measures to ensure relevant security of processing.

Procedures and controls used
Based on a risk assessment, Bizbrains has implemented appropriate technical security measures under the data processing agreements concluded. Security measures include anti-malware, firewalls, network segmentation, access management regarding data, monitoring and alerting, logging, patching and physical access security.

Bizbrains continuously monitors security through vulnerability assessments to assess whether an appropriate level of technical security measures has been implemented. These technical security measures cover, e.g., MFA, anti-malware protection, encryption, backup and disaster recovery setup.

3.6.3 Organisational measures (control objective C)

Scope
Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant security of processing.

Procedures and controls used
Bizbrains has implemented and established organisational measures based on risk assessments. This includes processes and procedures to ensure that IT security policies and personal data processing policies are updated continuously and communicated to employees.

3.6.4 Deletion and return of personal data (control objective D)

Scope
Procedures and controls are complied with to ensure that personal data can be deleted or returned if an agreement to this effect is reached with the data controller.

Procedures and controls used
Bizbrains has policies and procedures in place describing how personal data should be processed. These procedures describe how, under the instructions of the customer, Bizbrains should return and delete data.

3.6.5 Data retention (control objective E)

Scope
Procedures and controls are complied with to ensure that the data processor only stores personal data in accordance with the agreement with the data controller.

Procedures and controls used
Bizbrains has prepared a guide on how personal data should be processed and stored. This guide and the underlying policies are communicated to Bizbrains employees and are updated on an ongoing basis.

3.6.6 Use of sub-data processors (control objective F)

Scope
Procedures and controls shall be carried out to ensure that only approved sub-data processors are used and that the data processor follows up on the sub-data processors' technical and organisational measures to protect the data subjects' rights and to ensure that the processing security of personal data is adequate.

Procedures and controls used
Bizbrains continuously maintains an overview of sub-data processors used. Bizbrains shall ensure that sub-data processor agreements have been concluded with sub-data processors and that sub-data processors are subject to the same technical security measures as Bizbrains. The review of data processing agreements and sub-data processors is carried out annually.

3.6.7 Transfer of personal data to third countries or international organisations (control objective G)

Scope
Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

Procedure and controls used
Bizbrains is using Microsoft Azure for hosting the Link 3 platform. Bizbrains has established procedures to ensure that there is a valid basis of transfer when using Microsoft Azures cloud service. Microsoft is listed as a sub-data processor in the Data processing agreements. Furthermore, Bizbrains is verifying that Microsoft is actively signed up on the Data Privacy Framework list to ensure that it has reliable mechanisms for personal data transfers consistent with EU law.

3.6.8 Assistance to data controllers (control objective H)

Scope
Procedures and controls are complied with to ensure that the data processor can assist the data controller in correcting and deleting data relating to the processing of personal data and assist with the provision of such data to the data subject or the limitation of the processing of personal data.

Procedures and controls used
Bizbrains has established procedures for assisting data controllers with disclosure, correction and deletion to the extent that such action is requested.

3.6.9 Security breach (control objective I)

Scope
Procedures and controls shall be complied with to ensure that any security breaches can be dealt with in accordance with the data processing agreement concluded.

Procedures and controls used
Bizbrains has established procedures describing the process to be followed in connection with a possible security breach.

3.7 Complementary controls at the data controllers

The following is a description of the controls that are expected to be implemented by the data controllers and are essential to achieve the control objectives outlined in the description.

The data controller has the following obligations:

- Ensuring that the personal data is up to date.
- Ensuring that the instruction is lawful in relation to the current data protection regulations
- Ensuring that the instruction is appropriate in relation to this data processing agreement and the main service
- Ensuring that the data controller's users are up to date in Link 3
- If deciding to use unencrypted protocols for transmission of personal data, ensuring that appropriate controls are in place to protect the personal data when in transfer.
- Ensuring that controls are in place to ensure they are updated with the list of sub-processors in section 3.2. New or changed VAN providers can be added to or removed from the list without notice.

4 Bizbrains’s control objectives, control activity and test results

4.1 Introduction

This report is designed to provide Bizbrains's customers with information about Bizbrains's services and controls that may affect the processing of personal data and to provide data controllers for whom Bizbrains processes personal data with information about the operating effectiveness of the controls that were tested.

This report, when combined with an understanding and assessment of the controls of data controllers, is intended to assist data controllers in assessing the risks associated with the outsourced processing of personal data that may be affected by the controls at Bizbrains.

Our testing of Bizbrains's controls was restricted to the control objectives and related controls listed in the control matrix below in this section of the report and was not extended to all the controls described in the system description or controls that are expected to be implemented by the data controllers to meet the control objectives.

It is the data controller's responsibility to evaluate this information in relation to the controls in place at the data controller. If certain complementary controls are not in place at the data controller, Bizbrains's controls may not compensate for such weaknesses.

4.2 Test of controls

The test of controls performed to determine the operating effectiveness of controls consist of one or more of the following methods:

Method	Description
Inquiry	Interview, i.e., inquiry with selected personnel at Bizbrains
Observation	Observation of the execution of the control
Inspection	Review and evaluation of documents and reports concerning the performance of controls. This includes reading and evaluating reports and other documentation to assess whether specific controls are designed and implemented. Furthermore, it is assessed whether controls are monitored and supervised adequately and at appropriate intervals.
Re-performance of control	Repetition of the relevant control to verify that the control functions as intended.

4.3 Control objectives, control activity and test results

In the table below, the tested control objectives and controls are listed. Furthermore, we have described the audit procedures performed and the results of those procedures. To the extent that we have identified material control weaknesses, we have indicated this.

4.4 Control objectives, control activity and test results

Control objective A Procedures and controls are complied with to ensure that instructions for the processing of personal data are adhered to consistently in accordance with the data processing agreement entered into.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures exist to ensure that personal data is only processed according to instructions. Checked by way of inspection that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in data processing. Checked by way of inspection that procedures are up to date.	No exceptions noted
A.2	The data processor only processes personal data stated in the instructions received from the data controller.	Checked by way of inspection that management ensures that personal data is only processed according to instructions. Checked by way of inspection on a selection of samples of data processing agreements that processing is conducted consistently with instructions.	No exceptions noted
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or Member State data protection provisions.	Checked by way of inspection that formalised procedures exist ensuring verification that personal data is not processed against the Regulation or other legislation.	No exceptions noted

Control objective A Procedures and controls are complied with to ensure that instructions for the processing of personal data are adhered to consistently in accordance with the data processing agreement entered into.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
		Checked by way of inspection that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated against legislation. Inquired that the data controller was informed in cases where the processing of personal data was considered to be in breach of the legislation.	

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
B.1	Written procedures exist which include a requirement that agreed safeguards are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures exist to ensure establishment of the agreed safeguards. Checked by way of inspection that procedures are up to date. Checked by way of inspection of 5 data processing agreements that the safeguards agreed have been established.	No exceptions noted
B.2	The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.	Checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data. Checked by way of inspection that the data processor has implemented technical measures ensuring an appropriate level of security consistent with the risk assessment. Checked by way of inspection that the data processor has implemented the safeguards agreed with the data controller.	No exceptions noted
B.3	For the systems and databases used in the processing of personal data, anti-virus software has been installed that is updated on a regular basis.	Checked by way of inspection that, for the systems and endpoints used in the processing of personal data, anti-virus software has been installed. Checked by way of inspection that the anti-virus software is up to date.	No exceptions noted

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	Checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall.	No exceptions noted
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. Inspected network documentation to ensure appropriate segmentation.	No exceptions noted
B.6	Access to personal data is restricted to users with a work-related need for such access.	Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data. Checked by way of inspection that formalised procedures are in place for following up on whether users' access to personal data is consistent with their work-related needs. Checked by way of inspection that the agreed technical measures support retaining the restriction on users' work-related access to personal data. Checked by way of inspection of samples of users' access to systems and databases that such access is restricted to the employees'	No exceptions noted

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
		work-related needs.	
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. Such monitoring comprises: • System monitoring (certificates, CPU, RAM, discs, services) • Link monitoring • Audit logs (Event logs)	Checked by way of inspection, for systems and databases used in the processing of personal data, that system monitoring, link (application) monitoring and event logging have been established. Checked by way of inspection that an SMS alarm feature has been established.	No exceptions noted
B.9	Logging of the following matters has been established in systems, databases and networks: • Changes in users' system rights; • Failed attempts to log on to systems, databases or networks.	Checked by way of inspection that formalised procedures exist for setting up logging of user activities in systems, databases and networks used for processing and transmitting personal data. Checked by way of inspection that logging of user activities in systems, databases and networks used for processing or transmitting personal data has been configured and activated.	No exceptions noted
B.11	The technical measures established are tested on a regular basis by way of vulnerability scans.	Checked by way of inspection that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans. Checked by way of inspection of a selection of samples that documentation exists for regular testing of the technical measures taken. Checked by way of inspection that any deviation or weakness in the technical measures has been responded to in a timely and satisfactory manner and communicated to the data controllers, as appropriate.	No exceptions noted

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
B.12	Changes to systems, databases or networks are made consistently with the procedures in place that ensure maintenance through relevant updates and patches, including security patches.	Checked by way of inspection that formalised procedures exist for handling changes to systems, databases and networks, including handling of relevant updates, patches and security patches. Checked by way of inspection of a selection of changes to systems, databases and networks that changes have been carried out according to the procedure.	No exceptions noted
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including continued justification of rights by a work-related need.	Checked by way of inspection that formalised procedures exist for granting and removing users' access to systems and databases used for processing personal data. Checked by way of inspection that access to systems and databases granted to employees has been authorised, and that a work-related need exists. Checked by way of inspection of 2 samples of resigned or dismissed employees that their access to systems and databases was deactivated or removed on a timely basis. Checked by way of inspection that documentation exists that user access granted is evaluated and authorised on a regular basis.	No exceptions noted

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed by using two-factor authentication at a minimum.	Checked by way of inspection that formalised procedures exist for ensuring that two-factor authentication is applied to the processing of personal data involving a high risk for the data subjects. Checked by way of inspection that users can only process personal data that involves a high risk for the data subjects by using two-factor authentication.	No exceptions noted
B.15	Physical access safeguards have been established to only permit physical access by authorised persons to premises and data centres at which personal data is stored and processed.	Checked by way of inspection that Bizbrains obtains and reviews appropriate auditor's reports covering the physical access safeguards around Microsoft Azure.	No exceptions noted

Control objective C Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
C.1	The management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	Checked by way of inspection that an information security policy exists which was considered and approved by management within the past year. Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No exceptions noted
C.2	The management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	Inspected documentation of management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into. Checked by way of inspection of 5 samples of data processing agreements that the requirements stated in the agreement are covered by the requirements of the information security policy for safeguards and security of processing.	No exceptions noted
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant: • References from former employers; • Certificate of criminal record.	Checked by way of inspection that formalised procedures are in place for ensuring screening of the data processor's employees as part of the employment process. Checked by way of inspection of 5 samples of new employees that screening has been carried out. Such screening comprises: • References from former employers; • Certificate of criminal record.	No exceptions noted

Control objective C Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and the data processing procedures, as well as any other relevant information about the employees' processing of personal data.	Checked by way of inspection of one new employee that the relevant employee has signed a confidentiality agreement. Checked by way of inspection of 5 new employees that the relevant employees have been introduced to: • The information security policy; • The procedures for processing personal data and other relevant information.	No exceptions noted
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal, and that assets, such as access cards, computers, mobile phones, etc., are returned. Checked by way of inspection of 2 employees resigned or dismissed that their rights have been deactivated or terminated and that assets have been returned.	No exceptions noted
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid, and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	Checked by way of inspection that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. Checked by way of inspection of 2 employees resigned or dismissed that documentation exists for the continued validity of the confidentiality agreement and the general duty of confidentiality.	No exceptions noted

Control objective C Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Checked by way of inspection that the data processor provides awareness training to the employees in general IT security and security of processing related to personal data. Inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	No exceptions noted

Control objective D Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. Checked by way of inspection that the procedures are up to date.	No exceptions noted
D.2	The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines: • Personal data is stored with the data processor until the controller requests that the data be deleted or returned. It is therefore the controller's responsibility to delete any personal data in accordance with applicable laws, practices and other guidelines.	Checked by way of inspection that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. Checked by way of inspection of the system that the client has the opportunity to configure data retention.	No exceptions noted
D.3	Upon termination of the processing of personal data for the data controller and in accordance with the agreement with the data controller, data has been: • Returned to the data controller; and/or • Deleted, if this is not in conflict with other legislation.	Checked by way of inspection that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. Checked by way of inspection of 2 samples of terminated data processing sessions during the assurance period that documentation exists that the agreed deletion or return of data has taken place.	No exceptions noted

Control objective E Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. Checked by way of inspection that the procedures are up to date.	No exceptions noted
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	Checked by way of inspection that the data processor has a complete and up-to-date list of processing activities stating localities, countries or regions.	No exceptions noted

Control objective F Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
F.1	Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. Checked by way of inspection that procedures are up to date.	No exceptions noted
F.2	The data processor only uses sub-data processors to process personal data specifically or generally approved by the data controller.	Checked by way of inspection that the data processor has a complete and up-to-date list of sub-data processors used. Checked by way of inspection of 2 samples of sub-data processors from the data processor's list of sub-data processors that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements – or otherwise as approved by the data controller.	No exceptions noted
F.3	When changing the generally approved sub-data processors used, the data controller is informed in a timely manner to enable such controller to raise any objections and/or withdraw personal data from the data processor. When changing the specifically approved sub-data processors used, this has been approved by the data controller.	Checked by way of inspection that formalised procedures are in place for informing the data controller when changes are made to the sub-data processors used. Inquired if changes have been occurred regarding the use of sub-data processors within the last year.	No exceptions noted

Control objective F Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
F.4	The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or a similar agreement with the data controller.	Checked by way of inspection the existence of signed sub-data processing agreements with sub-data processors used as stated on the data processor's list. Checked by way of inspection of 2 samples of sub-data processing agreements that they include the same requirements and obligations as those stated in the data processing agreements between the data controllers and the data processor.	No exceptions noted
F.5	The data processor has a list of approved sub-data processors disclosing: • Name • Location • Description of processing (purpose).	Checked by way of inspection that the data processor has a complete and up-to-date list of sub-data processors used and approved. Checked by way of inspection that the list at least includes the required details about each sub-data processor.	No exceptions noted
F.6	Based on an up-to-date risk assessment of each sub-data processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or a similar activity. The data controller is informed of the follow-up performed at the sub-data processor.	Checked by way of inspection that formalised procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements. Checked by way of inspection of documentation that each sub-data processor and the current processing activity at such processor are subjected to a risk assessment.	No exceptions noted

Control objective F Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
		Checked by way of inspection of documentation that technical and organisational measures, security of processing at the sub-data processors used, third countries' bases of transfer and similar matters are appropriately followed up on.	

Control objective G Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures exist to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Checked by way of inspection that procedures are up to date.	No exceptions noted
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	Checked by way of inspection on a sample basis that the use of data processors in third countries or international organisations is in accordance with the data processing agreement. Inquired whether any data transfers have been carried out during the period.	No exceptions noted
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer. Checked by way of inspection that relevant sub-processors are actively signed up on the Data Privacy Framework list.	No exceptions noted

Control objective H Procedures and controls are complied with to ensure that the data processor can assist the data controller in correcting and deleting personal data, restricting the processing of personal data or providing information about the processing of personal data to the data subject.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
H.1	Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place governing the data processor's assistance to the data controller in relation to the rights of data subjects. Checked by way of inspection that procedures are up to date.	No exceptions noted
H.2	The data processor has established procedures, in so far as this was agreed, that enable timely assistance to the data controller in correcting and deleting personal data, restricting the processing of personal data or providing or handing out information about the processing of personal data to data subjects.	Checked by way of inspection that the procedures in place for assisting the data controller include detailed procedures for: • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects.	No exceptions noted

Control objective I Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.			
No.	**Bizbrains's control activity**	**Test performed by Deloitte**	**Result of test**
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. Checked by way of inspection that procedures are up to date.	No exceptions noted
I.2	The data processor has established the following controls to identify any personal data breaches: • Awareness among employees.	Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches.	No exceptions noted
I.3	If a personal data breach has occurred, the data processor has informed the data controller without undue delay and no later than 72 hours after having become aware of such personal data breach at the data processor or a sub-data processor.	Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach. Made inquiry as to whether they have identified any personal data breaches or been informed thereof by sub-data processors.	No exceptions noted
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency which should describe: • The nature of the personal data breach • The probable consequences of the personal data breach • The measures taken, or proposed to be taken, to respond to the personal data breach.	Checked by way of inspection that the data processor has established procedures for assisting the data controller in filing reports with the Data Protection Authorities describing: • The nature of the personal data breach • The probable consequences of the personal data breach • The measures taken, or proposed to be taken, to respond to the personal data breach.	No exceptions noted