This Data Processing Agreement ("Agreement") is entered into between the parties identified below, governing the processing of personal data under the General Data Protection Regulation (GDPR).

It is acknowledged that Visma IMS A/S ("Visma IMS") acts as a data processor on behalf of its customers ("Controllers"), while Impossible Cloud GmbH ("Impossible Cloud") is engaged as a sub-processor for the processing of personal data. This Agreement is designed to address the roles and responsibilities of each party within this processing structure, ensuring GDPR compliance and adequate data protection measures.

Data Processing Agreement Article 28 GDPR

Status: February 2025

Data Processing Agreement between

Impossible Cloud GmbH
Jürgen-Töpfer-Str. 48
22763 Hamburg, Germany
- Processor, hereinafter referred as **"the Agent"-**

and

Visma IMS A/S
Axel Kiers Vej 5 A, 8270 Højbjerg
25862015
- Controller, hereinafter referred as **"the Principal"**-

Principal and Agent individually designated as "Party" and collectively as "Parties".

1. Subject-Matter

In the framework of the delivery and performance relationship between the parties (hereinafter referred to as the "Main Agreement") it is necessary that the Agent handles personal data as a processor in the sense of Article 4 no. 8 GDPR, for which the Principal is responsible as controller or processor of the controller in the sense of Article 4 no. 7 GDPR (hereinafter referred to as "Principal-Data"). This Agreement concretizes the data privacy rights and duties of the parties in the context of handling the Principal-Data for the performance of the Main Agreement by the Agent.

2. Nature and Purpose of the Processing, Nature of the Personal Data, Categories of Data Subjects, Duration of the Processing

The Agent shall process the Principal-Data for the duration of the contract on behalf of and in compliance with the instructions of the Principal. The Principal remains the controller according to Article 5 (2) GDPR ("Master of the Data "). Nature and purpose of the processing as well as the nature

of the personal data and the categories of data subjects are specified in Annex 1. The Agent shall not process any personal data deviating from or going beyond this, in particular if its for the Agents' own purposes.

3. Principal's Rights to Give Instructions

3.1. Instructions from the Principal shall be given in writing or text form (e-mail being sufficient). Deviating from this, (telephone) verbal instructions may be given, if they are subsequently confirmed in writing or text form.

3.2. The Agent shall carry out the instructions of the Principal without undue delay or, where applicable, in compliance with a reasonable deadline set by the Principal. The agent shall, in particular, rectify, delete and block personal data as instructed by the Principal without undue delay and confirm this in writing upon request.

3.3. If the Agent considers that an admissible individual instruction violates applicable provisions of the General Data Protection Regulation or other data privacy provisions of EU law or the law of the Member States, he shall point this out to the Principal without undue delay. The Agent is entitled to suspend the execution of the instruction until the instruction is confirmed by the Principal.

4. Duties of the Principal

4.1. The Principal shall be externally, i. e. vis-à-vis third parties and data subjects, responsible for the lawfulness of the processing of the Principal-Data and for safeguarding the rights of data subjects.

4.2. The Principal shall keep all business secrets of the Agent (in particular those with regard to technical and organisational measures) acquired in the context of the contractual relationship confidential. This obligation shall remain in force even after termination of this contract.

4.3. Insofar as the Agent defends himself with legal means against a claim for damages according to Article 82 GDPR, against an imminent or already imposed administrative fine according to Article 83 GDPR or other sanctions in the sense of Article 84 GDPR, the Principal shall allow the Agent to disclose details of the processing for the purpose of legal defense, including instructions issued from the Principal.

5. Duties of the Agent

5.1. If a data subject addresses the Agent directly in the exercise of his rights under Chapter 3 GDPR (Art. 12-23 GDPR), taking into account Part 2, Chapter 2 BDSG (Sections 32-37 BDSG), the Agent shall immediately forward this request to the Principal and support the Principal in a reasonable manner with appropriate technical and organisational measures to comply with his obligation to respond to such requests for the exercise of the rights of the data subject specified in Chapter 3 DSGVO.

5.2. The Agent shall support the Principal in complying with the duties arising out of Art. 32-36 GDPR taking into account the nature of the processor and the information available to the Agent.

5.3. If the Agent becomes aware of a personal data breach within the meaning of Art. 4 No. 12 GDPR it shall immediately notify the Principal thereof. Within this notification pursuant to Art. 33 para. 2 DSGVO, the Agent shall inform the Principal as comprehensive as possible about the nature and extent of the

incident and the time it occurred, the IT system and data subjects affected, the time of discovery, all conceivable adverse consequences of the personal data breach and the measures taken as a result.

5.4. The Agent informs the Principal without undue delay if the rights of the Principal concerning the personal data held by the Agent are significantly affected by measures taken by third parties or other events.

5.5. The Agent shall return all Principal-Data at the request of the Principal. Data carriers received from the Principal shall be marked separately and administered on an ongoing basis. Copies and duplicates of the personal data may only be made with the prior consent of the Principal, unless they are used for the proper execution of this agreement or the respective project assignment or to comply with legal storage obligations.

5.6. If the Agent is legally required, it shall assign a data protection officer (Art. 37-39 GDPR). His or her contact details and where applicable information about his or her replacement shall be given to the Principal for the purpose of direct contact at least in text form (e-mail being sufficient).

6. Security in the Processing

6.1. The Agent shall take all measures necessary pursuant to Art. 32 GDPR to grant a level of data security commensurate with the risk of processing. In particular, these measures include the ability to restore the confidentiality, the integrity, the availability and the resilience of the systems permanently and to restore the availability of and access to personal data quickly after a physical or technical incident. The Agent shall regularly review, assess and evaluate the effectiveness of the technical and organisational measures taken to grant the security of the processing and documents the results. The Agent will conduct regular, at least quarterly, comprehensive reviews, assessments, and evaluations of the effectiveness of the technical and organisational measures to ensure the security of processing and document the results. This includes a clearly defined process for the regular evaluation and adjustment of the TOMs to ensure their adequacy and effectiveness.

6.2. The Agent shall implement the technical and organisational measures listed in **Appendix 2** prior to commencing the processing of Principal-Data, to maintain them for the duration of the processing and to adapt them commensurate with the state of the art and the risk of the processing. The Agent ensures that the TOMs are updated as part of the regular evaluations, especially with regard to new risks and technological developments.

6.3. The Agent shall ensure that all persons authorized to process personal data are obliged to confidentiality or are subject to an adequate statutory confidentiality obligation.

7. Supervision Authority of the Principal

7.1. The Agent shall grant the Principal the right to evaluate the data processing and the compliance with this contract or the respective project assignment. In particular, the Agent shall provide the Principal with all information required to prove compliance with the obligations laid down in this Agreement and shall enable the execution of evaluations, including inspections. These actions may also be carried out by a third party obliged to confidentiality, provided that the third party is not a competitor of the Agent.

7.2. The parties agree that the Principal shall conduct an evaluation in accordance with Clause 7.1 by instructing the Agent, at the Agents' option, to submit an appropriate audit report, a report or extracts

of reports from independent bodies (e.g. accountants, auditors, data protection officers, data protection officers, data protection auditors or quality auditors) or an appropriate certification by an IT security or data protection audit - e.g. in accordance with ISO/IEC 27001 or "BSI-Grundschutz" (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) - ("Audit Report"). Notwithstanding, the Principal may conduct an independent evaluation when reasonably justified.

7.3. The Agent shall support the Principal in its evaluation. This includes granting the Principal all access, information and inspections rights. The same applies to evaluations conducted by the competent supervisory authority in accordance with the applicable data protection regulations.

7.4 The Principal shall inform the Agent about all circumstances relating to the conduct of the evaluation in due time (generally at least four weeks prior to the evaluation). Generally, the Principal may conduct an evaluation once per calendar year. Notwithstanding the foregoing, the Principal shall have the right to conduct further evaluations in the event of special occurrences.

8. Subprocessors

8.1. The Agent may subcontract with further processors (subprocessors). For the time being, the Agent commissions the subcontractors listed in **Appendix 3**. The Principal agrees to their commissioning. The Agent shall always inform the Principal of any intended change in relation to the use or replacement of subcontractors, which shall give the Principal the opportunity to object to such changes within two weeks, although this may not be done without good cause in terms of data protection law. Unless the Principal raises justified objections within two weeks of notification of the change, the change shall be deemed to have been approved by the Principal. The Agent shall inform the Principal of this significance of his conduct at the beginning of the period. In the event of an objection, the Agent may, at his own discretion, either provide the service without the intended change or - if the provision of the service without the intended change is not reasonable for the Agent - discontinue the service to the Principal within two weeks of receipt of the objection and terminate the main contract without notice and with immediate effect.

8.2. Should the commissioning of a subprocessor lead to a transfer of Principal-Data to a country outside of the European Union (EU) or the European Economic Area (EEA) ('third country'), clause 9 of this agreement applies.

8.3. The Agent shall ensure that the data protection obligations stipulated in this Agreement also apply vis-à-vis the subcontractor. The Agent shall oblige the subprocessor respectively pursuant to Art. 28 (4) GDPR by way of a contract or another legal instrument in accordance with EU law or the law of the respective member state prior to the commencement of the processing, whereby, in particular, sufficient guarantees must be provided that the appropriate technical and organisational measures are conducted in such a way that the processing complies with the regulations of the GDPR.

9. Transfer of Principal-Data to Third Countries

9.1. Generally, the data processing contractually agreed upon shall be conducted in a member state of the European union (EU) in a signatory state of the Agreement on the European Economic Area (EEA). Any transfer of Principal-Data to a country outside the EU/EEA ("third country") shall only take place if the special requirements of Art. 44 et seq. GDPR are met.

10. Return and Deletion

10.1. The Agent shall return all Principal-Data after having finished the processing agreed on and, in particular after the end of the contractual performance (in particular in the event of termination or other end of the Main Agreement) and subsequently delete this data in accordance with the applicable regulations (including existing copies). Data carriers obtained by the Principal shall be returned or destroyed in compliance with an appropriate level of protection. The same applies to test and rejection material. This shall not apply provided Union or Member State law requires storage of the personal data.

10.2. Documentations which serve the purpose of proving the orderly and due data processing or legal requirements of record-keeping shall be kept by the Agent according to the respective record-keeping periods beyond the duration of the contract.

11. Duration and Termination

The term and termination of this Agreement shall be governed by the provisions concerning the term and termination of the Main Agreement. A termination of the Main Agreement automatically results in the termination of this Agreement. An isolated termination of this Agreement is excluded.

12. Priority clause

Unless special provisions are contained in this Agreement, the provisions of the Main Agreement shall apply. In the case of any conflicts between provisions of this Agreement and provisions of other agreements, in particular with the Main Agreement, the provisions of this Agreement shall prevail.

In the event of conflicts between different language versions of this Agreement, the German version shall prevail.

Hamburg, 10.4.2025	Højbjerg, 25th of March 2025
Place / Date	Place / Date
Agent: Impossible Cloud GmbH	**Principal**

Appendix:

- Appendix 1: Nature and purpose of the processing, Type of personal data, Categories of data subjects
- Appendix 2: Technical and organisational matters
- Appendix 3: Subcontractors
- Appendix 4: Teleworking Guideline

Appendix 1:

Nature and Purpose of the Processing, Type of Personal Data, Categories of Data Subjects

***Nature and Purpose of the Processing*:**

The contractor provides hosting services for the client or customers of the client. The client or its customers determines which content is stored on the provided servers. The contractor has access to this content in order to perform support and maintenance tasks. Additionally, the contractor has access to the log data of the systems. Furthermore, the contractor has access to the data created by the client or customers of the client in the Partner Portal of Impossible Cloud.

***Type of Personal Data*:**

The processed personal data is determined by the client or customers of the client. The client or its customers can independently utilize the provided storage spaces and upload all information themselves.

Typically, the scope of the contract includes the processing of the following personal data:

- Identification data (e.g., IP address)
- Contact details (e.g., name, email address

***Categories of Data Subjects*:**

The categories of affected individuals are determined by the information uploaded by the client or its customers. Typically, the following groups of individuals are affected:

- Customers of the client
- Employees of the client or its customers
- Service providers and other business partners of the client or its customers

Appendix 2:

Technical and Organisational Measures

1. Confidentiality (Article 32 (1) Pt. b GDPR) and Encryption (Article 32 (1) Pt. a GDPR)

Physical Access Control

Measures to prevent third parties from accessing Data Processing Facilities used to process personal data:

- Avoidance of the use of local storage media such as hard drives.
- Entrance doors are always kept locked.
- Individual access authorization with documentation of access rights.
- Electronic door openers that can only be activated by chip card or similar mechanism.
- Visitors/external individuals are accompanied or collected and supervised at all times.
- Certain IT systems are operated in external data centers (hosting) and through external services (Software-as-a-Service). Access control at these locations is ensured by the respective provider.
- Additional securing of physical documents, such as physical archives, and minimising access for employees.

Electronic Access Control/Encryption

Measures to prevent unauthorized use of the Data Processing Facilities and -Methods:

- Access to externally hosted/operated IT systems is highly secured (encryption, VPN).
- Metadata is stored in Tier 3 or higher data centers with corresponding security measures.
- Two-factor authentication.
- Network isolation to prevent unauthorized external access (firewall).
- Access to IT systems is only possible with a user ID and individual password.
- Access permissions are documented.
- Functional assignment of individual end devices and logging of system usage.
- Avoidance of the use of mobile storage devices.
- Screen lock on workstations, automatic locking after extended periods of absence.
- Careful selection of cleaning personnel.
- Dedicated Teleworking Policy for All Employees for the Implementation of Mobile Work

Internal Access Control

Measures to guarantee the usage of Data Processing Methods by authorized personnel is restricted exclusively to access the personal data their access rights are based on:

- Individual access rights for each user (documented in a written authorization concept), centrally managed and controlled by system administrators).
- Dedicated permissions per user role for IT systems for reading, editing, and deleting.
- Regular review of access permissions. Unnecessary permissions are revoked promptly.
- Recording of accesses to the IT system.
- Definition of user roles and corresponding assignment of stakeholders.
- Logging of access, editing, and deletion of files.

Separation Control/Purpose Limitation Control

Measures to guarantee that data collected for separate purposes can be processed separately:

- Separation of production and test systems (in separate databases).
- Access permissions are task-based and limited to a minimum. This also applies to the number of administrators.

2. Integrity (Art. 32 (1) Pt. b GDPR)

Data Transfer Control

Measures that prevent the unauthorized reading, copying, change or deletion of personal data during the electronic transfer or transport or saving on the data carrier, and also ensure the possibility to examine and determine to which destinations a transfer of personal data through data processing facilities is to be taken:

- Data storage and processing take place on IT systems in the data center. The connection between clients and servers is highly secure (encryption, VPN).
- Use of physical storage media is prohibited.
- When hardware is circulated or exchanged, hard drives are wiped and reinstalled.
- Visitors do not have access to the operational LAN/WLAN.
- Employee training on phishing attempts and general dangers related to email usage.

Data Entry Control

Measures to ensure the possibility of a review of whether and by whom personal data is entered into-, or changed or deleted in Data Processing Systems:

- Logging of activities of the system administrator and all users.
- Logging of all activities on the server.
- Protection of log data against loss or alteration.
- Four-eyes principle for changes to the system landscape (requiring approval or review by at least two individuals)

3. Availability and Resilience (Art. 32 (1) Pt. b GDPR), Rapid Recovery (Art. 32 (1) Pt. c GDPR)

Availability Control

Measures to ensure the protection of personal data against destruction or loss by chance (this information refers to the clients own IT-Systems):

- Dedicated data security concept ("Information Security Policy").
- Versioned data and system backups according to a backup plan (multiple times daily).
- Disk mirroring (RAID).
- Protection against malicious software (malware).
- Security-related updates and patches are applied regularly and promptly.
- Received and outgoing data storage media undergo malware checks.
- Dedicated reporting procedure and dedicated incident response plan ("Incident Response Plan").

4. Procedures for Regular Testing, Assessment and Evaluation (Art. 32 (1) Pt. d GDPR; Art. 25 (1) GDPR)

Order of Contract Control

Measures to ensure that personal data, processed by order of a third party, are processed only in compliance with the instructions of the client:

- Contractors are selected carefully.
- Written instructions to the contractor (e.g., through a data processing agreement).
- Obligation of the contractor's employees to maintain confidentiality.
- Oversight of the contractor by management or the data protection officer.

Data Protection Management

Measures to allow for control over the data protection measures and compliance with data protection regulations in a verifiable manner:

- A knowledgeable person has been appointed as the data protection officer.
- There is a documented data protection management system.
- Employees receive training and awareness in data protection and are informed about the confidentiality of data.

5. Pseudonymisation (Art. 32 (1) Pt. a GDPR, Art. 25 (1) GDPR

Measures to ensure that personal data is processed in such a way that the data cannot be associated to a specific concerned person without the assistance of additional information, provided the additional information is stored separately and is subject to appropriate technical and organisational measures:

- Personal data is modified or aggregated in such a way that it can no longer be directly attributed to a specific individual.
- Personal data is separated from other data and stored separately to facilitate pseudonymization.
- Personal data is restricted to a regional level, ensuring, for example, that access to personal data from the EU or authorised third countries is not possible.

Appendix 3: Subcontractors

Name	Address/Country	Content of the Order
Auth0	Okta Inc., Salvatorplatz 3, 80333 Munich, Germany	Provision of user authentication (login, signup)

Appendix 4: Teleworking Guideline

Impossible Cloud GmbH and the employee have concluded an employment contract which does not contain any provisions for working from home or remotely (hereinafter referred to as 'teleworking').

§ 1 Subject matter, General terms

(1) This guideline regulates issues of data protection and data security if teleworking is permitted to the employee.

(2) In order to ensure the proper processing of personal data, the employer may issue complementary instructions in addition to the provisions of this guideline.

(3) For the purposes of this guideline

- 'company data' means all data and information relating to the employer's business operations, in particular personal data, business and trade secrets as well as other confidential information;
- 'company IT systems' means all work equipment provided by and/or systems operated by the employer for processing company data, including terminals and access points (e.g. laptops, tablets, smartphones, internet access, access media, email accounts, software services, cloud storage, servers and storage media);
- 'third party' means all persons not employed by the employer, e.g. family members, other roommates, guests of the employee.

§ 2 Handling of company data

(1) While teleworking the employee remains part of the employer's organization. This means that all contractual rights to issue instructions remain effective and, in particular, all company data to which the employee has remote access remain exclusively within the employer's organizational sphere. The employee is therefore prohibited from disseminating company data, information or documents - in particular personal and otherwise confidential data - to third parties, enabling third parties to gain knowledge of them (for example by viewing them on screen or printing them out), saving company data on his or her personal storage media, copying them without authorization or using them for any purposes other than work purposes.

(2) In particular,

- it is prohibited to disseminate or make available to third parties passwords or other ways to access company IT systems, e.g. by writing down passwords or storing chip cards, codes or similar on the device;
- it is prohibited to grant third parties access to company IT systems and/or company documents;
- it is prohibited to save company data on storage media other than the storage media provided by the employer. In particular, storage on personal cloud services, smartphones, hard drives, USB sticks or forwarding to personal email accounts is prohibited;
- it is prohibited to process company data with personal devices. Access to remote servers, cloud services and webmail accounts from a personal device is only permitted if access is browser-based and no synchronization with the personal device takes place. Should processing with personal devices be necessary in addition to this, an agreement on the use of personal devices must be concluded in addition to this agreement;
- it is prohibited to deactivate or circumvent security measures or to make other technical changes to the company IT systems or to install software unassisted;

- any printouts containing company data must be securely destroyed when they are no longer needed (document shredder).

(3) All disruptions or anomalies in the use of the company IT systems must be reported immediately to the IT manager or the management.

(4) The employer is entitled to demand the employee at any time to surrender all company data and documents, including all copies. If passwords or other keys are required to access company data, they shall also be surrendered. The employee may not assert a right of retention against this.

§ 3 Security measures for teleworking

(1) Only a room that can be locked may be used as a workplace in the employee's home. It should be locked when not in use by the employee. If the employee has visitors (including craftsmen) in his or her home, the room must be locked. If visitors are at the workplace, the employee must watch them at all times.

(2) If the employee leaves his or her workplace (even if only briefly, for example to go to the bathroom), it must be ensured that no third party can access company data or documents. This means, in particular, that:

- the computer used must be locked so that at least the password must be entered to unlock it when returning;
- windows must be locked, except in cases of short-term absence during which intrusion can realistically be excluded (e.g. 10th floor and no possibility to climb over from the adjacent apartment);
- if documents are used, they must be locked in a cupboard or the workplace must be locked; this does not apply if the employee is alone at home and only leaves his workplace for a short time;
- when leaving home, any access medium used (e.g. chip card, transponder) must be removed from the computer and when using documents, they must be locked in a cabinet.

§ 4 Additional security measures for remote teleworking

When working from outside the employee's home, in addition to the provisions of § 3 the following shall apply:

(1) The employee may not leave the remote workplace unattended - even briefly - unless it is ensured that employee of the employer watches the workplace. As an exception, leaving for a short time shall be permitted if the mobile device is connected to stationary or sufficiently large objects, sufficient social control is ensured, the absence is short and no particularly confidential data is processed.

(2) Before the employee turns his or her direct attention away from the remote workplace, the computer must be locked and all access media (e.g. chip card, transponder) must be removed and stored securely.

(3) Remote use of documents requires prior consent of the supervisor.

(4) Carrying along company IT systems abroad requires the consent of the supervisor. Consent must be given for destination and transit countries.

§ 5 Security measures for transport and transfer of company data

(1) The removal of printed documents or mobile data storage devices (e.g., USB sticks) is generally prohibited and may only occur if absolutely necessary.

(2) If the employee takes along documents containing company data, they may only be transported in a locked container (e.g. sealed briefcase). The employee may not leave the documents unattended

at any time during transport. This also applies if the locked container is transported in the trunk of a car (e.g. it is not permitted to leave the vehicle to go shopping on the way home).

(3) Access and attempted access while teleworking may be recorded and regularly evaluated by the employer. This data shall only be used to detect, combat and prosecute misuse and not to monitor performance or behavior.

§ 6 Discontinuation of teleworking

(1) If the employee's permission for teleworking or the employment relationship ends or if the employee is irrevocably released from the obligation to perform work, the employee must return all work equipment provided by the employer as well as the company documents and data carriers to the company without undue delay and regardless of whether the employer expressly requests this or not. If passwords or other keys are required to access company data or company IT systems, they shall also be handed over.

(2) In addition, the employee shall accept the collection of work equipment provided by the employer as well as of company documents and data carriers by persons appointed by the employer after a reasonable period of notice.

§ 7 Information about legal consequences in case of violations

The employer points out that violations of this agreement may not only have consequences under labor law (admonition, warning, termination with or without notice), but may also result in a fine and/or be punishable by law (e.g. Art. 83 GDPR, § 42 BDSG, § 23 GeschGehG and, if applicable, § 203 StGB). In addition, violations of this agreement may result in claims for injunctive relief and damages.