Data Processing Agreement

Clause 1

Purpose and subject matter of this Data Processing Agreement

a) Details regarding the subject matter of processing shall be determined in each case by the attached Annex II and the Service Contract, concluded between the Parties and underlying this Data Processing Agreement (hereinafter referred to as "DPA").

b) The controllers and processors listed in Annex I have agreed to this Data Protection Agreement in order to ensure compliance with Article 28(3) and (4) of the UK General Data Protection Regulation (hereinafter referred as the "UK GDPR"). UK GDPR (being EU General Data Protection Regulation 2016/679 ("UK GDPR") as retained into English law pursuant to the Data Protection, Privacy And Electronic Communications (Amendments Etc) (EU Exit) Regulations 2019 made on 28 February 2019 (as amended by the Data Protection, Privacy And Electronic Communications (Amendments Etc) (Eu Exit) Regulations 2020 laid on 14 October 2020), the Data Protection Act 2018.

Clause 2

Interpretation and Definitions

Where this DPA uses the terms defined in the UK GDPR respectively, those terms shall have the same meaning as in that Regulation.

Clause 3

Docking clause

a) Any entity that is not a Party to this DPA may, with the agreement of all the Parties, accede to this DPA at any time as a controller or a processor by completing all the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to this DPA and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

c) The acceding entity shall have no rights or obligations resulting from this DPA from the period prior to becoming a Party.

Clause 4

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 5

Obligations of the Parties

5.1. Instructions

The processor shall process personal data only on written documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented in writing. The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe the UK GDPR or any other applicable Union or Member State data protection provision.

5.2. Purpose limitation and duration

Purpose and duration of the processing of personal data are set out in Annex II.

5.3. Security of processing

5.3.1. The processor has implemented the technical and organizational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data (personal data breach).

5.3.2. The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor ensures that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.4. Sensitive data

Any processing of such data is as outlined in Annex II.

5.5. Documentation and compliance

5.5.1. The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from the UK GDPR. At the controller's request, the processor shall also permit and contribute to audits to verify compliance with the provisions of this DPA by the processor in its business operations through spot checks, which are generally to be announced at least 30 days in advance. The controller may conduct one audit per calendar year. Additional audits will be conducted at the expense of the controller and with prior agreement. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

5.5.2. The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with a 30 days notice.

5.5.3. The Parties shall make the information referred to in this DPA, including the results of any audits, available to the competent supervisory authority/ies on request.

5.6. Use of sub-processors

5.6.1. The processor has the controller's general written authorization for the engagement of sub-processors from an agreed list, which is attached an Annex IV of this DPA. The processor shall inform the controller of any intended changes of that list through the addition or replacement of sub-processors in advance, thereby giving the controller an opportunity to object to such changes prior to the engagement of the relevant sub-processor(s).

5.6.2. Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with this DPA. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to this DPA and the UK GDPR.

5.6.3. At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

5.6.4. The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

5.6.5. The processor shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

5.7. International transfers

5.7.1. Any transfer of data to a third country or an international organization by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement of UK law to which the processor is subject and shall take place in compliance with Chapter V of the UK GDPR.

5.7.2. The controller agrees that where the processor engages a sub-processor in accordance with Clause 5.6. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of the UK GDPR, the processor and the sub-processor can ensure compliance with Chapter V of the UK GDPR by using the EU Addendum to standard contractual clauses as outlined by Article 46 (3) UK GDPR, provided the conditions for the use of those standard contractual clauses are met or an Internation Data Transfer Agreement (IDTA).

Clause 6

Assistance to the controller

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorized to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

c) In addition to the processor's obligation to assist the controller pursuant to Clause 6(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

    1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

    2. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

    3. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

    4. the obligations in Article 32 of the UK GDPR

d) The Processor sets out in Annex III the appropriate technical and organisational measures.

Clause 7

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of the UK GDPR.

7.1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

7.1.1. in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it

7.1.2. in obtaining the following information pursuant to Article 33(3) of the UK GDPR, shall be stated in the controller's notification, which includes the nature of the personal data, categories and approximate number of data subjects and/or personal data records, likely consequences and the measures taken or proposed to be taken.

7.1.3. in complying, pursuant to Article 34 of the UK GDPR, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

7.2. Data breach concerning data processed by the processor

7.2.1. In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall be provided without undue delay and contain a description of the nature of the breach, the details of a contact point where more information concerning the personal data breach ca be obtained, its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects..

7.2.2. The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of the UK GDPR.

Clause 8

Erasure and return

Duration of processing is as outlined in Annex II of this DPA.

Following termination of the Service Contract, the processor shall, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with this DPA.

Final Provisions

Clause 9

Non-compliance with the Clauses and termination

a) Without prejudice to any provisions under UK GDPR, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the Service Contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

1. the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

2. the processor is in substantial or persistent breach of the obligations of this DPA;

3. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or UK GDPR.

c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 5.1, the controller insists on compliance with the instructions.

d) In the event of a contradiction between this DPA and the provisions of related agreements between the Parties existing at the time when this DPA is agreed or entered into thereafter, this DPA shall prevail.

Annex I

List of Parties

Controller(s): The Customer, as specified in the Commissioning of DataGuard-Services.

Processor(s): DataCo International UK Limited, as specified in Annex I

Contact details of the Data Protection Officer (DPO): dpo@dataguard.co.uk

Annex II

Description of the processing

Categories of data subjects whose personal data is processed
Business customers, employees, suppliers, agents and service providers, platform users

Categories of personal data processed
Business partner data, customer data, personal data in customer documents

These are, among others, the following categories of personal data:
- First name
- Surname
- Salutation
- Gender
- E-mail address
- Position / function in the company
- Business address
- Business name
- Business phone number

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Special categories of data as defined under Article 9 UK GDPR are not processed in the scope of the Data Processing Agreement.

Nature of the processing

Customers can upload documents and store them on the DataCo Platform, DataCo International UK Limited acts as a processor within the meaning of Art. 4 (8) UK GDPR by providing the storage medium of the cloud. If DataCo International UK Limited needs to access these documents, it does so on its own responsibility in order to fulfil contractual obligations.

Likewise, DataCo International UK Limited acts as a processor within the meaning of Art. 4 (8) UK GDPR when it links customers to partners via the platform without becoming actively involved itself, for example by forwarding them via a link.

The scope of this data processing agreement therefore is limited to the specific upload area of the platform, i.e. the upload, storage and deletion of documents as well as the provision of corresponding services to external partners; other sub-areas remain unaffected by this agreement.

Purpose(s) for which the personal data is processed on behalf of the controller:

Based on the Service selected by the Customer, DataCo provides support to the Customer to meet their obligations in the field of security and compliance.

Duration of the processing:

The duration of the processing begins with execution of the Service Contract and ends with the termination of the Service Contract. The data is deleted after termination of the service, unless there are legal retention obligations..

Annex III

Technical and organizational measures to ensure the security of the data on the DataCo Platform

I. Physical Access Controls

Unauthorised persons must be denied physical access to data processing equipment with which personal data are processed or used.

Access Control System:
A centrally managed access control system is used for the company.

Access Control System - Administration:
The access control system is managed in the following way:

- Electronic

Access Control System - Technical means:
The access control system is based on the following technical means:
Token / Transponder
Chip card

Access Control System - Visitor Registration
The presence of visitors is registered in the following way:

- Digital visitor book

Access Control Systems - Lockable rooms:
All rooms in which access to personal data is possible are lockable.

Securing the premises / buildings of the company:
The company premises / building is secured from public ground by:

- Office in a larger building complex
- Gate
- Lockable door

Security at the Company Premises - Alarm System:
The company premises or parts of it are safeguaded by an alarm system.

Server
One or more servers are used on the company premises.

Server - Access Authorisation:
Access to the server rooms is restricted to the necessary group of persons in the company.

Server - Access Control
Access to the server room in the company is controlled.

Server - External Use:
External servers were rented in the company.

Server – Room:
The company's servers are operated in an intended room.

II. Logical Access Control

Unauthorised persons shall be denied access to data processing equipment with which personal data are processed or used.

Access to Personal Data in Visitor Areas:
It is ensured that personal data in the company is not freely accessible in visitor areas.

Passwort Manager:
A password manager is used in the company.

Password Manager - Access Control:
The used password manager offers sufficient access control and encrypted storage.

Portable Terminal Devices - Access Control:
Terminal devices in the company have access controls (password, PIN, pattern, etc.).

Remote Maintenance - Access Options:
Remote maintenance accesses are released individually.

Remote Maintenance - Control Regulations for Maintenance:
Regulations and controls regarding remote maintenance in the company have been defined.

Remote Maintenance – Logging:
The execution of remote maintenance in the company is logged.

Remote Maintenance - Security Measures:
Remote maintenance in the company shall be performed under appropriate security measures.

Remote Maintenance – Tools:
The following tools are used for remote maintenance in the company:

- Digital Mountain Remote Maintenance

Mobile Device Management (MDM)
An MDM is implemented to regularly check all endpoints, delete data if necessary and only allow approved applications.

Single Sign-On Procedure:
A single sign-on procedure is used in the company.

III. Data Access Control

It must be ensured that persons authorised to use a data processing system can only access the data according to designated access permissions.
Departing Persons - Withdrawal of Authorisations:
All access authorisations and access rights of a departing person are blocked/deleted promptly.

Documentation – Authorsations:
The allocation and withdrawal of access authorisation for IT-systems in the company is logged.

Documentation – Backup:
The logging of the permitted users, user groups and rights profiles is included in the data backup procedure.

Documentation - Digital Administration:
The logs on access authorisations to IT systems in the company are digitally recorded.

IT Security - Firewall Name
The following firewalls are used in the company:

- Fortinet

IT Security - Firewall
One or more firewalls are used against unwanted network access in the company.

Identity & Access Management
Authorizations are controlled centrally via the Active Directory according to the need-to-know principle.

IV. Storage Device Control

Storage devices should not be read, copied, changed or removed without authorisation.

Portable Terminal Devices - Anti-theft Protection:
In the company, portable terminals are secured against theft outside use hours.

Portable Terminal Devices - Approval Procedure for Applications:
There is a test and approval procedure for applications on terminal devices in the company.

Portable Terminal Devices - Remote Deletion:
Remote deletion of data on terminal devices in the company is possible.

Storage Device Management - Inventory List:
Inventories for the following storage devices are kept in the company:

- Laptops
- Mobile phones
- Tablets

Storage Device Management - Secure Deletion:
Electronic storage devices are securely deleted in the company.

Workplace - Sealable Containers:
There are lockable containers available at every workplace to securely store documents and storage devices in the company.

V. Communication Control

It must be possible to determine and establish where personal data can be transmitted by data transmission equipment.

Connection to the Telecommunications Provider:
The following method is used to connect to the telecommunications provider:

- Regular DSL/fibre optic connection

VI. Transmission Control

It is necessary to prevent unauthorised reading, copying, modification or deletion of data during the transfer of personal data or during the transport of data carriers.

Data Transmission - Concealed Transport:
Containers used by the company to transport storage devices containing personal data are not sent in sealed labelled containers.

Encryption of Transmission:
Data is encrypted during transmission using the following procedures/protocols:

- SSL/TLS

VII. User Control

It must be prevented that data processing systems can be used by unauthorised persons using data transmission devices.

Administrators:
Administrators and their deputies have been appointed for all IT systems and networks in the company.

Administrators - Consistent Accounts:
Administrator accounts are used at the following level in the company.

- Database
- Operating system
- Application
- Network

Administrators - Special Accounts
Special administrator accounts are used in the company. Admins use multifactor authentication.

Data Protection for Teleworkers
Teleworkers were made aware of compliance with relevant data protection regulations.

Departing Persons - Reclaiming Company Owned Property:
All company-owned property containing personal data are reclaimed of a departing person.

Employee Training:
The following measures are taken to make employees aware of the importance of data protection and to oblige with them in accordance with the requirements.

- Training of all employees with access rights

Employee Training – Regularity:
Regular training sessions are held on the subject of data protection in the company.

IT Security - Qualification of the IT Administration:

The company ensures that he IT administrative staff has sufficient qualifications to perform the task.

VIII. Service Provider Control

It must be ensured that personal data processed under contract can only be processed according to the instructions of the client.

External Service Providers:
The company works with external service providers.

External Service Providers - Contact with Personal Data:
Outside personnel who may come into contact with personal data in the company are constantly monitored at work.

External Service Providers - Processing Instructions to Order Processors:
Instructions on the processing of personal data in the company are only given in writing to the data processors.

Service Provider for Disposal of Storage Devices:
An external service provider is used for the disposal of storage devices.

IX. Storage Control

Unauthorised entry into storage systems as well as unauthorised access to, modification or deletion of stored personal data shall be prevented.

Measures for Data Locking and Data Deletion:
Data locking/deletion measures are in place, meaning data can easily be locked/deleted in all systems upon request.

Password Protection - Password List
No unencrypted password list is kept.

Professional Disposal of Personal Data:
Employees in the company are required to dispose personal data properly.

X. Availability control

It must be ensured that personal data are available at all times and are protected against accidental destruction or loss.

Archiving Concept:
An archiving concept is defined that regulates how and for how long documents are archived.

Archiving Concept - Legal Retention Obligation:

There is a legal storage obligation for the archived documents.

IT Security - Malware
Encrypted data in the company is checked for malware as well as unencrypted.

IT Security - SSL/TLS Scanner:
An SSL/TLS scanner is used to check encrypted data packets for malware as well.

IT Security - SSL/TLS Scanner Examination
The checking and classification of the scanned data packet in the company takes place automatically.

IT Security - SSL/TLS Scanner Name:
The following TLS/SSL scanner is used:

- Fortinet

Server - Protection against Hazards:
The server rooms are secured against the following hazards:

- Overheating

XI. Reliability

It must be ensured that personal data is secured against accidental loss or destruction.

Critical Systems – Redundancy:
Critical systems and the infrastructure are designed redundantly.

IT Security - Network Monitoring:
A software is used to check the network or the applications in the company.

IT Security - Network Monitoring Software:
The following software is used:

- WatchGuard with extended security and logging functionalities

XII. Data Recovery

It is necessary to ensure that personal data can be quickly restored in the event of a physical or technical incident.

Backups:
Backups in the company are performed by:

- Independent backups (e.g. Microsoft SharePoint)
- Service providers
- Cloud provider

Backups are stored redundantly in separate fire compartments and are tested regularly.

XIII. Separability

IT Security - Particularly Sensitive Personal data:
A dedicated and separated network is used for particularly sensitive categories of personal data.

Segregation of Workplaces:
Workplaces where particularly sensitive personal data is processed are physically separated from other workplaces.

Client capability
All major systems are multi-client capable.

XIV. Operating system

Unauthorised individuals must be prevented from gaining access to operating systems.
Operating system - Authorisation Concept for Test and Development Environments:
An authorisation concept in test and development environments has been implemented in the company.

Password Protection - Examining the Password Guidelines:
Compliance with the password specifications in the company is technically checked.

Password Protection - Initial Passwords:
Initial passwords must be changed at the first login in the company.

Password Protection - Password Complexity:
There is a default for password complexity in the company.

Password Protection - Password Components:
The passwords in the company consist of at least the following components:

- Numbers
- Special characters
- Letters

Password Protection - Password Composition
Es There is a default for the password composition in the company.

Password Protection - Password Length:
There is a default for the password length in the company.
The password has a length of at least 8 characters.

Password Protection - User Account:
Each user account of the operating system in the company is protected by a password.

Protocol - Logging of Incorrect Entries:
Incorrect password entries of users in the company are logged.

XV. Software and additional information about the Data

Unauthorized individuals must be prevented from gaining access to any applications.

Software - Separation between Environments:
Productive, test and development environments including the data bases are separated from each other in the company.

DataCo Platform
In addition to the measures described, further measures are implemented to protect personal data that is processed via the DataGuard platform. The platform is hosted in ISO/IEC27001 certified data centers. Maintenance of the platform and access via SSH is only permitted to dedicated developer and the CTO of DataCo GmbH. Authentication provisions are strong and state of the art. Dedicated backups are created, there is an authorization concept according to the need-to-know principle and a data transfer is always TLS encrypted.
Due to the advanced security measures, DataGuard is of the opinion that personal data in the platform is sufficiently protected in terms of integrity, confidentiality and availability.

Annex IV

List of sub-processors

Name of the subcontractor	Address	Description of scope & services	Location of the processing activity
Open Telekom Cloud	Deutsche Telekom AG Friedrich-Ebert-Allee 140 53113 Bonn Germany	Hosting Provision of web servers and the necessary infrastructure to provide Data-Guard's web services	Germany
Hetzner	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Germany	Hosting Backup storage	Germany
Okta Inc. (Auth0)	100 First Street, San Francisco, California 94105, USA	Authentication - Access to customers' credentials is via Auth0. The service provider does not have any information about the persons associated with the organization. Type of data: Customer's login details: name and e-mail address	USA
Google Cloud EMEA Limited (Google Cloud Platform (GCP)	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Infrastructure Cloud provider for the operation of all our virtual machines. All data is encrypted at rest. No PaaS services are used Type of data: Platform data	Ireland

Mailjet	4, rue Jules Lefebvre 75009 Paris	Email delivery system used within the DataCo Platform	France
Salesforce.com Germany GmbH	Erika-Mann-Str 31 80636 München	Management of Customer Data provided as part of the Service Contract	Germany