Technical and organizational measures (TOMs)
Maddox AI GmbH

Version: 3.2

As of: April 24, 2026

I. General Information

1. Legal Background

The EU General Data Protection Regulation (**GDPR) stipulates** that every controller and processor must take appropriate technical and organizational measures to ensure a level of protection appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as risks of varying degree and severity with regard to the rights and freedoms of natural persons.

To comply with our accountability obligations under Art. 5 (2) GDPR, this document contains the technical and organizational measures we have implemented in accordance with Art. 25 and 32 GDPR.

2. Content and Status of the Document

This document was last updated on March 25, 2024.

Section II lists the technical and organizational measures that Maddox AI GmbH (hereinafter **"Maddox AI**") directly implements by itself in its own area of control.

This is to be distinguished from the technical and organizational measures that the service providers used by Maddox AI implement on their part to ensure an appropriate level of protection for the processing activities within their respective area of responsibility.

As an innovative start-up in the field of AI-based quality assurance, Maddox AI uses specialized IT service providers in various areas, partly because experience has shown that specialized providers can guarantee particularly high security standards. The use of specialized IT service providers with particularly high security standards is therefore an important component of Maddox AI's IT security and data protection concept.

The service providers' extensive technical and organizational measures of further increase the level of protection that any personal data processed under the responsibility of Maddox AI enjoys. Those measures are described in Section III.

3. Change Log

Note on the assignment of version numbers	
0.1 - 0.9	The document is currently in the draft stage
1.0	Designates the first released version
Changes to content	The first digit should be increased for content changes (e.g. version 2.0 after fundamental revision of version 1.6)
Minor corrections	When correcting errors (e.g. spelling) with no effect on the content or minimal changes to the content, only the second digit should be increased (e.g. version 1.7 after minor corrections to version 1.6)

Version	Date	Author	Brief description of the change / reason for change

3.0	22.03.2024	Cornelius Widmaier	Creation of version 3 of the TOMs
3.1	25.03.2024	Julian Schneider	Customization and translation

II. Technical and Organizational Measures - Maddox AI GmbH

1. Confidentiality (Art. 32(1)(b) GDPR, Art. 5(1)(f) GDPR)

Personal data must be processed in a manner that ensures appropriate data security. The company has taken appropriate technical and organizational measures for the protection of personal data

- from unauthorized or unlawful processing,
- against unintentional loss,
- from unintentional destruction, and
- from unintentional damage.

a. Access Control

Suitable access control measures **physically prevent unauthorized persons from gaining access** to data processing systems. These measures ensure that only authorized persons are granted access to the data processing systems.

Effective access control measures minimize the following risks in particular:

- Loss/destruction/damage of data processing equipment
- unlawful or unauthorized processing such as unauthorized inspection

Maddox AI has implemented the following measures, among others, to prevent unauthorized access to data processing systems (in particular notebooks, hard drives, IT servers):

(1) Technical Measures

Access control for server room

Manual locking system (e.g. door locks)

Automatically closing and locking doors

Security locks

Locking doors that open outwards

Access security for building technology (e.g. distribution rooms for network or electrical distributors)

(2) Organizational Measures

Key regulation and documentation for business premises

Locking regulations (regulations concerning the opening and locking of buildings and rooms)

Keeping a central visitor list

Visitors must be accompanied by employees

Policy/instructions for external access

Guidelines/instructions for treating visitors

b. Access and User Control

Access control is intended to **prevent the unauthorized use of data processing systems** so that only authorized persons have access to data processing systems and can use these systems. Effective access control measures minimize the following risks in particular:

- Loss/destruction/damage of data processing equipment
- unlawful or unauthorized processing such as unauthorized inspection

Maddox AI has implemented, among others, the following measures in this regard:

(1) Technical Measures

User authentication (name and password)

Network access protection (cable connection)

Adequate use of anti-virus software

Automatic desktop lock (after 5 minutes)

Secured access to the WLAN

Secured access to the company's internal cable network (even if a cable connection is established, only registered devices are granted access to the network)

Intrusion Prevention System

Two-factor authentication

Automatic updates of end devices' operating systems through regular updates/patches

Encryption of storage mediums in laptops/notebooks and cell phones

Encryption of other storage mediums (e.g. USB drives, external hard disks)

(2) Organizational Measures

Password assignment/password rules (the assignment of passwords is based on a valid password policy)

Regular change of passwords

Immediate change of default passwords on all devices

Immediate blocking and deletion of access after an employee leaves the company

Registration of all issued end devices in order to keep track and be able to reclaim devices from employees if necessary

Immediate return of issued end devices after an employee leaves the company

Careful management of user authorizations

Directive for the individual workplace

Directive on the deletion/destruction of documents containing personal data

Logging of access to data processing systems

Clear Desktop Policy

Guidelines for the use of smartphones

Guideline for the use of laptops/tablets

Guideline for Home office

c. Access, Data, and Storage Control

Access control measures should ensure that users of data processing systems only have **access** to personal data that they are **authorized to** process. Effective access control minimizes the following risks:

- unauthorized access during processing and use,
- unauthorized copying,
- unauthorized modification, and
- unauthorized deletion.

Maddox AI has implemented, among others, the following measures to prevent unauthorized reading, copying, modification or removal of data within the system:

(1) Technical Measures

Access logging for applications, in particular when entering, changing, or deleting data

Changes to files are traceable to individual users

Data protection-compliant destruction of end devices and storage media by a specialist company

Physical destruction of storage mediums

Lockable document cabinets

(2) Organizational Measures

Careful assignment of access authorizations on the basis of an authorization concept

Authorization concept based on the need-to-know principle

Access authorizations are limited to the minimum required group of people

Conformity of "digital and analog" access authorizations

Formal process for granting access authorizations

Number of administrators is kept at a minimum

Policies for the disposal of paper documents, storage mediums, and end devices

Clear Screen Clear Desk Policy

Confidentiality obligation of employees

Password assignment/password rules (the assignment of passwords is based on a valid password policy)

Regular change of passwords

d. Separation Control (Ensuring the Separation of Data Collected for Different Purposes)

Separation control measures are intended to ensure that personal data collected for different processing purposes is processed **separately and for a specific purpose.** In addition, separation control ensures the multi-client capability of the processing operations, insofar as this is necessary (e.g., for user accounts on an online platform). An effective separation control minimizes the following risks:

- unauthorized access to personal data,
- processing of personal data in a manner incompatible with the purposes of the processing.

Maddox AI has implemented, among others, the following measures to ensure separate processing of data that was collected for different purposes:

(1) Technical Measures

Physical separation of databases/storage mediums

Effective, software-based separation of different data pools

Separation of operative system and test system

(2) Organizational Measures

User authorization management for databases/applications

Record of processing activities

Data separation policy

2. Integrity (Art. 32(1)(b) GDPR, Art. 5(1)(f) GDPR)

Personal data must be processed in a manner that ensures **appropriate security.** Maddox AI has taken appropriate technical and organizational measures for the protection of personal data

- from unauthorized or unlawful processing,
- against unintentional loss,
- from unintentional destruction, and
- from unintentional damage.

a. Transfer Control

Transfer control prevents personal data from being **read, copied, modified or removed without authorization** during electronic **transmission** or during its transport or storage on storage mediums.

In addition, the recipients who may receive personal data are documented in a verifiable manner as part of the onward transfer control.

Maddox AI has, among others, implemented the following measures to prevent unauthorized reading, copying, modification, or removal of data during electronic transmission or transport:

(1) Technical Measures

Encrypted e-mail communication (e.g. S-MIME)

Encrypted data transmission on the Internet using state of the art encryption protocols (e.g. TLS 1.3, HTTPS, SFTP, etc.)

Secure transportation of storage mediums (secure transport container)

Use of digital signature processes for documents (e.g. digital signature on PDF)

(2) Organizational Measures

Guidelines for the use of smartphones

Guideline for the use of laptops/tablets

Guideline for home office

Careful selection of service providers

Physical data transfer only against receipt

Instructions for the disposal of paper documents, storage mediums, and end devices

Instruction to double-check addressees

Record of electronic/automatic data transmissions

Logging of retrieval and transmission processes

Documentation of data recipients and the duration of the planned transfer or deletion periods

b. Input Control

Input control measures shall ensure that it is possible to **subsequently check** and determine whether and how personal data has been entered, changed, or removed in order to ensure the **accuracy** and integrity of the personal data.

Maddox AI has implemented, among others, the following measures to determine whether and by whom personal data has been entered into, modified, or removed from data processing systems:

(1) Technical Measures

Automatic logging of changes and user entries with a time stamp

Logging of deletion processes

Collision check for databases

(2) Organizational Measures

Defined data deletion responsibilities

Careful assignment of input, modification, and deletion rights on the basis of the authorization concept (see also access, data, and storage control regarding the authorization concept)

3. Pseudonymization (Art. 32(1)(a) GDPR)

Pseudonymization under Art. 32(1)(a) GDPR reduces the possibilities of relating existing data to individuals. This is an **important security measure** for the protection of personal data.

Maddox AI has, among others, implemented the following measures for the purpose of pseudonymization :

If anonymization is not possible, data records are transmitted in pseudonymized form where possible

4. Encryption of Personal Data (Art. 32(1)(a) GDPR)

Art. 32(1)(a) GDPR identifies the **encryption** of personal data as an **important measure** to protect the security of personal data.

Maddox AI has implemented, among others, the following encryption measures:

a. Technical Measures

Encryption of storage mediums in laptops/notebooks and cell phones

Encryption of other storage mediums (e.g. USB drives, external hard disks)

Encrypted e-mail communication (e.g. S-MIME)

Encrypted data transmission on the Internet using current encryption protocols (e.g. TLS 1.3, HTTPS, SFTP, etc.)

Encryption of back-ups

b. Organizational Measures

Encryption guidelines

Regular review of the effectiveness of encryption measures taken

5. Availability and Resilience (Art. 32(1)(b) GDPR)

It is ensured that personal **data** is **protected against destruction or loss.** Effective availability control ensures that personal data is actually available at the required times.

Maddox AI has implemented, among others, the following measures to protect data against accidental destruction or loss:

a. Technical Measures

Fire protection measures

Fire extinguishers in business premises

Surge protection of the building against lightning strikes

Digitization of hard copies

Uninterruptible power supply

Automatic notification system when maximum storage capacity is reached

Preferential use of end devices with rechargeable batteries to bridge power outages

b. Organizational Measures

Outsourcing of data servers to specialized providers with high security standards, redundant systems, and automated data backups

Regular risk and vulnerability analyses

Capacity and resource planning

Emergency manual for IT incidents available

Emergency plan for IT incidents in place

6. Recoverability (Art. 32(1)(c) GDPR)

This ensures that data can be **restored quickly** after incidents.

Maddox AI has implemented, among others, the following measures to enable data recovery:

a. Technical Measures

Automated cyclical execution of a backup routine

External back-ups (e.g. service providers)

b. Organizational Measures

Backup and recovery concept in place

Guidelines for the regular backup of locally stored data

Regular review of recoverability

7. Procedures for Regular Review, Assessment, and Evaluation (Art. 32(1)(d), Art. 25 GDPR)

In particular, the following procedures have been established to regularly **review, assess, and evaluate the effectiveness** of the technical and organizational measures.

a. Data Protection Management (Compliant Corporate Governance)

Maddox AI has implemented, among others, the following measures to organize and administrate internal procedures in a privacy-compliant manner:

(1) Technical Measures

Use of monitoring applications

Use of data protection management software

Central documentation of all data protection procedures and regulations (employee wiki/intranet)

Simple exercise of the data subject's right to withdraw consent through technical measures (e.g., opt-out links on websites or in newsletter emails)

(2) Organizational Measures

Regular review of access control measures

Annual data protection training for employees

Confidentiality obligations of employees

Regular data protection primers for employees, in particular to prevent cyber attacks by means of social engineering

Appointment of a data protection officer

Appointment of an IT security officer

Annual review of technical and organizational measures

Data protection-friendly default settings are taken into account in software development (Art. 25(2) GDPR)

Defined process for reporting privacy incidents

Defined process for the fulfillment of data subject rights

Deletion concept in place

Software allows for data deletion

No more personal data is collected than is necessary for the respective purpose

Privacy-friendly default settings for the software used

Where possible and appropriate, specialized IT service providers with high security standards are used for data processing

Regular check whether the necessary updates and patches for the operating systems have been installed for all end devices

Regular check whether the operating systems of devices in the company's internal IT infrastructure (e.g. own servers, routers) are up to date

b. Order Control

Maddox AI takes the following measures, among others, to ensure that data is processed in **accordance with instructions:**

Careful selection of processors

Prior review of the TOM of each (sub-)processor

Data processing agreements (DPAs) have been executed with the processors used

A clear contract is in place between clients and contractors for the processing of personal data

Regulations on the use of new subcontractors are in place

Data is deleted in compliance with data protection regulations after the processor has completed the order

III. Technical and Organizational Measures of the Service Providers used

1. Microsoft Azure

Domain	Practices
Organization of Information Security	**Security Ownership**. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. Microsoft personnel with access to Customer Data or Professional Services Data are subject to confidentiality obligations. **Risk Management Program**. Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service and before processing Professional Service Data or launching the Professional Services. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory**. Microsoft maintains an inventory of all media on which Customer Data or Professional Services Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. **Asset Handling** -Microsoft classifies Customer Data and Professional Services Data to help identify it and to allow for access to it to be appropriately restricted. -Microsoft imposes restrictions on printing Customer Data and Professional Services Data and has procedures for disposing of printed materials that contain such data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data or Professional Services Data on portable devices, remotely accessing such data, or processing such data outside Microsoft's facilities.
Human Resources Security	**Security Training**. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. Microsoft limits access to facilities where information systems that process Customer Data or Professional Services Data are located to identified authorized individuals. **Physical Access to Components**. Microsoft maintains records of the incoming and outgoing media containing Customer Data or Professional Services Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of such data they contain. **Protection from Disruptions**. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. Microsoft uses industry standard processes to delete Customer Data and Professional Services Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data or Professional Services Data. **Data Recovery Procedures** -On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Microsoft maintains multiple copies of Customer Data and Professional Services Data from which such data can be recovered. -Microsoft stores copies of Customer Data and Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data and Professional Services Data are located. -Microsoft has specific procedures in place governing access to copies of Customer Data and Professional Services Data. -Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Professional Services and for Azure Government Services, which are reviewed every twelve months. -Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data and Professional Services Data, including malicious software originating from public networks. **Data Beyond Boundaries** -Microsoft encrypts, or enables Customer to encrypt, Customer Data and Professional Services Data that is transmitted over public networks. -Microsoft restricts access to Customer Data and Professional Services Data in media leaving its facilities.

Domain	Practices
	Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data or Professional Services Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Customer Data or Professional Services Data. **Access Authorization** -Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data or Professional Services Data. -Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. -Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. -Microsoft ensures that where more than one individual has access to systems containing Customer Data or Professional Services Data, the individuals have separate identifiers/log-ins. **Least Privilege** -Technical support personnel are only permitted to have access to Customer Data and Professional Services Data when needed. -Microsoft restricts access to Customer Data and Professional Services Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** -Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. -Microsoft stores passwords in a way that makes them unintelligible while they are in force. **Authentication** -Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. -Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. -Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. -Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. -Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. -Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. -Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data or Professional Services Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** -Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. -For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. -Microsoft tracks, or enables Customer to track, disclosures of Customer Data and Professional Services Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	-Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data or Professional Services Data are located. -Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data and Professional Services Data in its original or last-replicated state from before the time it was lost or destroyed.

2. MongoDB Atlas

1. definitions

The following terms have the following meanings when used in the Security Measures. Any capitalized terms that are not defined in the Security Measures have the meaning provided in your Agreement.

1.1 "Cloud Provider" means Amazon Web Services (AWS), Microsoft Azure (Azure), or Google Cloud Platform (GCP), as selected by Customer.

1.2 "Customer Data" means any data you or your end users upload into MongoDB Atlas.

1.3 "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

1.4 "Information Security Program" means MongoDB's written security program, policies, and procedures that set forth the administrative, technical, and physical safeguards designed to protect Customer Data.

1.5. "MongoDB Atlas Cluster" means each replica set or sharded cluster of data-bearing nodes running the MongoDB database software that is managed by MongoDB Atlas, subject to your selected configurations.

1.6 "MongoDB Atlas Project" means one or more associated MongoDB Atlas Clusters with a shared set of authorization and network configurations.

1.7 "MongoDB Systems" means MongoDB's internal infrastructure, including development, testing, and production environments, for MongoDB Atlas.

1.8 "Privileged User" means a select MongoDB employee or third-party contractor who has been granted unique authority to access Customer Data or MongoDB Systems as required to perform their job function.

1.9 "Security Incident Response Plan" means MongoDB's documented protocols for evaluating suspected security threats and responding to confirmed Data Breaches and other security incidents.

2 Information Security Program Overview.

2.1 General. MongoDB maintains a comprehensive written Information Security Program to establish effective administrative, technical, and physical safeguards for Customer Data, and to identify, detect, protect against, respond

to, and recover from security incidents. MongoDB's Information Security Program complies with applicable Data Protection Law and is aligned with the NIST Cyber Security Framework (NIST). Additionally, MongoDB Atlas is certified against ISO 27001:2013, ISO 27017:2015, ISO 27018:2019, SOC 2 Type II, Payment Card Industry Data Security Standard v.4, and Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Level 2. MongoDB Atlas has also undergone a HIPAA examination validated by a qualified third-party assessor and can be configured to build HIPAA compliant applications.

2.2 Maintenance and Compliance. MongoDB's Information Security Program is maintained by a dedicated security team, led by our Chief Information Security Officer. MongoDB monitors compliance with its Information Security Program, and conducts ongoing education and training of personnel to ensure compliance. The Information Security Program is reviewed and updated at least annually to reflect changes to our organization, business practices, technology, services, and applicable laws and regulations. We will not alter or modify the Information Security Program in a way that materially weakens or compromises the effectiveness of its security controls.

2.3 MongoDB Personnel Controls.

2.3.1 Background Checks. MongoDB performs industry standard background checks on all MongoDB employees as well as any third-party contractor with access to Customer Data or MongoDB Systems.

2.3.2 Personnel Obligations. Any Privileged User authorized to access Customer Data is required to commit in writing to information security and confidentiality obligations that survive termination and change of employment. MongoDB maintains a formal disciplinary procedure for violations by MongoDB personnel of its security policies and procedures.

2.3.3 Training. Upon hire and subsequently at least once per year, Privileged Users authorized to access Customer Data undergo required training on specific security topics, including phishing, secure coding, insider threats, and the secure handling of Customer Data and personally identifiable information. Further, MongoDB implements mandatory, role-specific training for Privileged Users who are authorized to access Customer Data. MongoDB maintains records of training occurrence and content. In addition to these mandatory

trainings, MongoDB offers employees additional training resources, such as internal security awareness and education groups and hackathons.

2.4 Third Parties. MongoDB maintains and adheres to a documented process for the evaluation and approval of third-party service providers prior to onboarding, which includes appropriate due diligence regarding each third party's security processes and controls. We require third parties to contractually commit to confidentiality, security responsibilities, security controls, and data reporting obligations, and we perform ongoing targeted due diligence on a quarterly basis.

2.5 Security Contact. If you have security concerns or questions, you may contact us via your normal support channels, via support.mongodb.com, or by emailing security@mongodb.com.

3 MongoDB Atlas Security Controls.

3.1 Data Centers and Physical Storage. MongoDB Atlas runs on AWS, Azure, and GCP, and you control which Cloud Provider to use for deploying your MongoDB Atlas Clusters. Each Cloud Provider is responsible for the security of its data centers, which are compliant with a number of physical security and information security standards detailed at the Cloud Provider's respective websites:

- https://aws.amazon.com/security/
- https://www.microsoft.com/en-us/trustcenter/security/azure-security
- https://cloud.google.com/security/

At least twice per year, each of our Cloud Providers is subject to due diligence performed by MongoDB or third-party auditors, which includes obtaining and reviewing security compliance certifications.

In addition to selecting which Cloud Provider to use, you also control the region where your MongoDB Atlas Clusters are deployed. This gives you the flexibility to decide where your Customer Data is physically stored, and you may choose to deploy your Customer Data in a specific geographic region (for example, only within the European Union or only within the United States).

3.2 Encryption.

3.2.1 Encryption in Transit. All MongoDB Atlas network traffic is protected by Transport Layer Security (TLS), which is enabled by default and cannot be disabled. Customer Data that you transmit to MongoDB Atlas, as well as Customer Data transmitted between nodes of your MongoDB Atlas Cluster, is encrypted in transit using TLS. You can select which TLS version to use for your MongoDB Atlas Clusters, with TLS 1.2 being the recommended default and a minimum key length of 128 bits.

3.2.1.1 Key Management Procedures for Encryption in Transit. All encryption in transit is supported by the use of OpenSSL FIPS Object Module. We maintain documented cryptography and key management guidelines for the secure transmission of Customer Data, and we configure our TLS encryption key protocols and parameters accordingly. MongoDB's key management procedures include: (i) generation of keys with approved key length; (ii) secure distribution, activation and storage, recovery and replacement, and update of keys; (iii) recovery of keys that are lost, corrupted, or expired; (iv) backup/archive of keys; (v) maintenance of key history; (vi) allocation of defined key activation and deactivation dates; (vii) restriction of key access to authorized individuals; and (viii) compliance with legal and regulatory requirements. When a key is compromised, it is revoked, retired, and replaced to prevent further use (except for limited use of that compromised key to remove or verify protections). Keys are protected in storage by encryption and are stored separately from encrypted data. TLS certificates are obtained from a major, widely trusted third-party public certificate authority. In the course of standard TLS key negotiation for active sessions, ephemeral session keys are generated which are never persisted to disk, as per the design of the TLS protocol.

3.2.2 Encryption at Rest. Upon creation of a MongoDB Atlas Cluster, by default, Customer Data is encrypted at rest using AES-256 to secure all volume (disk) data. That process is automated by the transparent disk encryption of your selected Cloud Provider, and the Cloud Provider fully manages the encryption keys. You may also choose to enable database-level encryption via the WiredTiger Encrypted Storage Engine

(using AES-256), as well as to bring your own encryption key with AWS Key Management Service (KMS), GCP KMS, or Azure Key Vault (KV).

3.2.3 Encryption in Use. MongoDB Atlas also supports automatic encryption of individual data fields of Customer Data before they are sent to MongoDB Atlas. If you enable this client-side field level encryption feature for a selected data field, an application-side component built into the MongoDB drivers encrypts that field of Customer Data before leaving the driver to be sent to MongoDB Atlas, and only decrypts it upon return to the application once inside the driver. With respect to the Customer Data for which you enable client-side field level encryption, MongoDB Atlas never sees your unencrypted Customer Data and you control the encryption keys, which you can secure using any KMIP-compliant key management service.

3.3 Network Connectivity Options.

3.3.1 Network Isolation. You may choose to deploy your MongoDB Atlas Clusters in a dedicated virtual environment or a shared multi-tenant system. Dedicated MongoDB Atlas Clusters are deployed in a VPC (for AWS and GCP) or VNet (for Azure) that fully isolates your Customer Data and is configured to prevent inbound network access from the internet. Each such MongoDB Atlas VPC or VNet utilizes security groups that act as a virtual firewall for your dedicated MongoDB Atlas Clusters.

3.3.2 Atlas IP Access List. In order to allow inbound network access to your MongoDB Atlas VPC or VNet, you must configure an Atlas IP Access List to enable specific networks to connect to the MongoDB Atlas Clusters within your MongoDB Atlas Project. Unless the Atlas IP Access List for a MongoDB Atlas Project includes a specific network's IP addresses, network traffic is prevented from accessing your MongoDB Atlas Clusters in that MongoDB Atlas Project.

3.3.3 Virtual Private Cloud Peering. You may enable peering between your MongoDB Atlas VPC or VNet to your own dedicated application tier virtual private network with the Cloud Provider of your choice (VPC or VNet). Peering permits you to route encrypted traffic between your MongoDB Atlas VPC or VNet and your own application tier VPC or VNet privately, rather than traversing the public internet. Subject to the capabilities of your selected Cloud Provider, you may also choose to

peer your MongoDB Atlas VPC or VNet to your application tier VPC or VNet across regions.

3.3.4 Private Endpoints. MongoDB Atlas also supports private endpoints on AWS using the AWS PrivateLink feature and on Azure using the Azure Private Link feature. If you enable this feature for any MongoDB Atlas Cluster, that MongoDB Atlas Cluster will only allow a one-way connection from your AWS VPC or Azure VNet to the MongoDB Atlas Cluster and that MongoDB Atlas Cluster cannot initiate connections back to your AWS VPC or Azure VNet. Private endpoints also enable you to reach your MongoDB Atlas Cluster transitively over the network from other application tier AWS VPCs and Azure VNets that you have peered with the private endpoint, or through your own self-managed virtual private network including via AWS DirectConnect and Azure ExpressRoute.

3.4 Configuration Management. The MongoDB Atlas environment, including our production environment and your MongoDB Atlas Clusters, leverages configuration management systems to fully automate configuration based on one-time decisions that are securely applied to new and existing environments to ensure consistency every time. Our production environment and your MongoDB Atlas Clusters use in-house built machine images with secure configuration management applied via industry standard automation software, which includes hardening steps.

4. access controls.

4.1 Customer Access. MongoDB Atlas supports multiple authentication and authorization options and methods to give you the flexibility to meet your individualized requirements and needs. You are responsible for understanding the security configuration options available to you and the impact of your selected configurations on your MongoDB Atlas environment, which consists of a web application administrative interface ("MongoDB Atlas UI") and any MongoDB Atlas Cluster you deploy. MongoDB Atlas provides you with configurable authentication and authorization options for both the MongoDB Atlas UI and your MongoDB Atlas Clusters.

4.1.1 MongoDB Atlas UI Authentication and Authorization. User credentials for the MongoDB Atlas UI are stored using industry standard and audited one-way hashes. The MongoDB Atlas UI supports multi-factor authentication (MFA), including a security

key/biometrics option that enables you to use hardware security keys or built-in authenticators. The MongoDB Atlas UI also supports federated authentication functionality for Single Sign-On (SSO) utilizing Security Assertion Markup Language (SAML).

4.1.2 MongoDB Atlas Cluster Authentication and Authorization. Authentication control for a MongoDB Atlas Cluster is enabled by default with the Salted Challenge Response Authentication Mechanism (SCRAM). You may choose to manage user authentication with self-managed X.509 certificates or through AWS IAM Users or Roles. MongoDB Atlas allows you to define permissions for individual users or applications in order to restrict the Customer Data that is accessible in a query. Further, you may choose to assign each user a MongoDB Atlas Project-specific role, which authorizes that user to perform specific actions on the MongoDB Atlas Clusters within that MongoDB Atlas Project. The MongoDB Atlas UI allows you to tailor your access controls by combining multiple roles and privileges for particular users. You can review, limit, and revoke user access to your MongoDB Atlas Clusters at any time. MongoDB Atlas also provides you with the ability to manage user authentication and authorization using your own Lightweight Directory Access Protocol (LDAP) server over TLS. A single LDAP over TLS (LDAPS) configuration applies to all MongoDB Atlas Clusters in a MongoDB Atlas Project.

4.1.3 Credential Requirements. As part of the configuration options, you may establish minimum password requirements (e.g., length, complexity) through your identity provider after federating authentication to the MongoDB Atlas UI via SAML and to the MongoDB Atlas Clusters via LDAPS.

4.1.4 Customer Database Auditing. MongoDB Atlas offers granular auditing that monitors actions in your MongoDB Atlas environment and is designed to prevent and detect any unauthorized access to Customer Data, including create, read, update, and delete (CRUD) operations, encryption key management, and role-based access controls. You are responsible for enabling database auditing and selecting the users, roles, groups, and event actions that you want to audit.

4.2 MongoDB Personnel Access to MongoDB Atlas Clusters.

4.2.1 Privileged User Access. As a general matter, MongoDB personnel do not have authorization to access your MongoDB Atlas Clusters. Only a small group of Privileged Users are authorized to access your MongoDB Atlas Clusters in rare cases where required to investigate and restore critical services. MongoDB adheres to the principle of "least privilege" with respect to those Privileged Users, and any access is limited to the minimum time and extent necessary to repair the critical issue. Privileged Users may only access your MongoDB Atlas Clusters via a gated process that uses a bastion host, requires MFA both to log in to our MongoDB Systems and to establish a Secure Shell connection (SSH) via the bastion host, and requires approval by MongoDB senior management.

4.2.2 Restricting MongoDB Personnel Access. MongoDB Atlas provides you with the option to entirely restrict access by all MongoDB personnel, including Privileged Users, to your MongoDB Atlas clusters. If you choose to restrict such access and MongoDB determines that access is necessary to resolve a particular support issue, MongoDB must first request your permission and you may then decide whether to temporarily restore Privileged User access for up to 24 hours. You can revoke the temporary 24-hour access grant at any time. Enabling this restriction may result in increased time for the response and resolution of support issues and, as a result, may negatively impact the availability of your MongoDB Atlas Clusters. If you enable client-side field level encryption, even Privileged Users will be unable to access Customer Data within your MongoDB Atlas Clusters in the clear unless you provide MongoDB with the encryption keys.

4.2.3 Credential Requirements. Privileged User accounts may only be used for privileged activities, and Privileged Users must use a separate account to perform non-privileged activities. Privileged User accounts may not use shared credentials. The password requirements described in Section 4.3.3 also apply to Privileged User accounts.

4.2.4 Access Review and Auditing. MongoDB reviews Privileged User access authorization on a quarterly basis. Additionally, we revoke a Privileged User's access when it is no longer needed, including within 24 hours of that Privileged User changing roles or leaving the company. We also log any access by MongoDB personnel to your MongoDB Atlas Clusters. Audit logs are retained for at least six years, and include

a timestamp, actor, action, and output. MongoDB utilizes a combination of automated and human review to scan those audit logs.

4.3 MongoDB Personnel Access to MongoDB Systems.

4.3.1 General. MongoDB's policies and procedures regarding access to MongoDB Systems adhere to the principles of role-based access control (RBAC), least privilege, and separation of duties. In accordance with these principles, with respect to MongoDB Atlas, MongoDB developers are only granted access to our development environments, and access to our production environment is limited to Privileged Users with appropriate authorizations. We review access authorizations to MongoDB Systems on a quarterly basis and we review any changes to authorizations for Privileged Users immediately. As part of the employee off-boarding process, access to MongoDB Systems is revoked within 24 hours of an employee's departure.

4.3.2 Access to MongoDB Atlas Production Environment. Our backend production environment that runs MongoDB Atlas is only accessible by a dedicated group of Privileged Users whose privileges must be approved by senior management. Privileged Users may only access our backend production environment via a bastion host and doing so requires MFA both to log in and to establish a SSH via the bastion host.

4.3.3 Credential Requirements. All MongoDB personnel passwords must conform to industry-standard complexity rules. Additionally, MFA is mandatory for all MongoDB personnel and cannot be disabled.

4.4 Physical Controls at MongoDB Offices. As noted in Section 3.1, Customer Data is deployed at the data centers of your selected Cloud Provider, and not at facilities owned or operated by MongoDB. At MongoDB offices, we follow industry best practices to employ physical security controls that are appropriate to the level of risk posed by the information stored and the nature of operations at our offices. In our offices, we: (i) issue access cards for all personnel through formal provisioning and approval processes; (ii) limit access to restricted areas to personnel with a need to access those areas to carry out their job functions; (iii) require visitors to sign in, execute a non-disclosure agreement, and be escorted in all non-public spaces; (iv) employ surveillance systems to monitor activity at points of entry from public spaces; and (v) revoke personnel access within 12 hours of termination.

4.5 Secure Deletion of Customer Data. If you terminate a MongoDB Atlas Cluster, it will become unavailable to you immediately and any Cloud Backup associated with that MongoDB Atlas Cluster will be terminated. MongoDB may retain a copy of the Customer Data stored in the terminated MongoDB Atlas Cluster for up to 5 days. If you terminate Cloud Backups, all snapshots will become unavailable to you immediately and it may take up to 24 hours for the Customer Data contained in the snapshots to become unrecoverable. When you terminate a MongoDB Atlas Project, the master key used to encrypt Customer Data is securely wiped, rendering all Customer Data effectively unrecoverable. If you choose to use MongoDB Atlas Online Archive, you can delete the entire archive, or pre-define automatic deletion dates for different data sections within MongoDB Atlas Online Archive to help automate any applicable retention restrictions or policies.

5 MongoDB Systems Security.

5.1 Separation of Production and Non-Production Environments.MongoDB Atlas has strict separation between production and non-production environments. Our MongoDB Atlas production environment, your MongoDB Atlas Clusters, and your Customer Data are never utilized for non-production purposes. Our non-production environments are utilized for development, testing, and staging. MongoDB also maintains firewalls to achieve strict separation of our MongoDB Atlas production environment and MongoDB's internal network.

5.2 Software Development Lifecycle. MongoDB has a dedicated security team, reporting to the Chief Information Security Officer, that leads security initiatives in the software development lifecycle (SDLC). We develop new products and features in a multistage process using industry standard methodologies that include defined security acceptance criteria and align with NIST and OWASP guidance. The SDLC includes regular code reviews, documented policies and procedures for tracking and managing all changes to our code, continuous integration of source code commits, code versioning, static and dynamic code analysis, vulnerability management, threat modeling, and bug hunts, as well as automated and manual source code analysis.

5.3 Monitoring and Alerting. MongoDB monitors the health and performance of MongoDB Atlas without needing to access your MongoDB Atlas Clusters. MongoDB maintains a centralized log management system for the collection, storage, and analysis of log data for our MongoDB Atlas production environment and your MongoDB Atlas Clusters. We use this information for

health monitoring, troubleshooting, and security purposes, including intrusion detection. We maintain our log data for at least six years, and we utilize a combination of automated scanning, automated alerting, and human review to monitor the data.

5.4 Vulnerability Management.

5.4.1 MongoDB Atlas Vulnerability Scanning. MongoDB maintains a documented vulnerability enumeration and management program that identifies internet-accessible company assets, scans for known vulnerabilities, evaluates risk, and tracks issue remediation. We conduct quarterly scans of both the underlying systems upon which MongoDB Atlas is deployed, as well as all third-party code integrated into our products. MongoDB's vulnerability management policy requires individual engineering teams to identify known vulnerabilities in system components, and develop remediation timeframes commensurate to the severity of an identified issue. We also utilize automated tooling in conjunction with monitoring security bulletins for relevant software and libraries, and implement patches if security issues are discovered.

5.4.2 Vulnerability Remediation. MongoDB uses a central company-wide ticketing system to track all security issues until remediation. We implement patches to our operating system and applications on a need-to-update basis, as determined in accordance with the Common Vulnerability Scoring System (CVSS). We are also a Mitre CVE Numbering Authority (CNA). Development tasks for all patches, bug fixes, and new features are defined as issues for specific target releases and are deployed to production only after completing requisite checkpoints, including quality assurance testing, staged deployment, and management review.

5.5 Penetration Testing and Internal Risk Assessments. MongoDB Atlas undergoes regular reviews from both internal and external security teams.

5.5.1 External Testing. Our MongoDB Atlas production environment is subject to an external penetration test by a nationally recognized security firm at least once per calendar year. Upon request, we will provide you with a summary letter of engagement that includes the number of high, medium, and low issues identified, but due to the sensitivity of the information gathered during these tests, we cannot allow customers to perform testing of our production platform.

Application-level security testing uses a standard application assessment methodology (e.g., OWASP). Additionally, external engagements with security consultants may include social engineering and phishing testing.

5.5.2 Internal Testing. Internally, MongoDB Atlas undergoes periodic risk assessments, including technical vulnerability discovery and analysis of business risks and concerns. The MongoDB security team is also routinely involved in source code review, architecture review, code commit peer review, and threat modeling.

6. contingency planning.

6.1 High Availability and Failover. Every MongoDB Atlas cluster is deployed as a self-healing replica set that provides automatic failover in the event of a failure. Replica set members are automatically provisioned by MongoDB Atlas across multiple availability zones within a region, providing resilience to localized site failures. All replica set members are full data-bearing nodes, ensuring majority writes in the event of single node failure and higher resilience during recovery. Concurrent writes across replica sets occur in real time. MongoDB Atlas also offers multi-region and multi-cloud deployment options.

6.2 Backups. MongoDB Atlas offers Cloud Backups, which use the native snapshot functionality of your selected Cloud Provider to locally back up your Customer Data. You may enable Cloud Backups when you create or modify a MongoDB Atlas Cluster, and you have control over how often a Cloud Backup is captured and the length of time for which Cloud Backups are retained. Cloud Backup snapshots are stored with your selected Cloud Provider in the primary region of your MongoDB Atlas Cluster. All Cloud Backups are encrypted at rest and you may choose to use self-managed keys with the WiredTiger Encrypted Storage Engine. You may also optionally enable Continuous Cloud Backups with point-in-time recovery stored on our encrypted S3 buckets.

6.3 Business Continuity and Disaster Recovery. MongoDB maintains a documented business continuity and disaster recovery ("BCDR") plan that aligns with ISO/IEC 22301:2019. Our BCDR plan includes: (i) clearly defined roles and responsibilities; (ii) availability requirements for customer services, including recovery point objectives (RPOs) and recovery time objectives (RTOs); and (iii) backup and restoration procedures. We review, update, and

test our BCDR plan at least annually. In the event of an incident that triggers the BCDR plan, the RPO will depend on your impacted MongoDB Atlas Cluster and backup configurations. You can test how your application handles a replica set failover at any time using the MongoDB Atlas UI or API.

7 Incident Response and Communications.

7.1 Security Incident Response Plan. As part of the Information Security Program, MongoDB maintains an established Security Incident Response Plan that aligns with NIST and ISO/IEC 27001:2013. In the event that MongoDB becomes aware of a Data Breach or other security incident, MongoDB will follow the Security Incident Response Plan, which includes: (i) clearly defined roles and responsibilities, including designation of a security incident task force; (ii) reporting mechanisms; (iii) procedures for assessing, classifying, containing, eradicating, and recovering from security incidents; (iv) procedures and timeframes for required notifications to relevant authorities and customers; (v) procedures for forensic investigation and preservation of event and system log data; and (vi) a process for post-incident and resolution analysis designed to prevent future similar incidents. The Security Incident Response Plan is reviewed, updated, and tested annually, including a security tabletop exercise at least once per year.

7.2 Security Incident Tracking. MongoDB maintains a comprehensive security incident tracking system that aligns with ISO/IEC 27001:2013 and documents: (i) incident type and suspected cause; (ii) whether there has been unauthorized or unlawful access, disclosure, loss, alteration, or destruction of data; (iii) if so, the categories of data affected by the incident, including categories of personal information; (iv) the time when the incident occurred or is suspected to have occurred; and (v) the remediation actions taken.

7.3 Customer Communications. MongoDB will notify you without undue delay if we become aware of any Data Breach. Taking into account the information available to us, such notice will include a description of the nature and cause of the Data Breach and the expected resolution time. To the extent possible, we will subsequently update you with information regarding evaluation of the root cause, potential impact, remediation actions taken, and actions planned to prevent a future similar event.

8. audit reporting.

8.1 Third-Party Certifications and Audit Reports. Upon request, and subject to the confidentiality obligations set forth in the Agreement, we will make available to you (or your independent, third-party auditor) information regarding MongoDB's compliance with the security obligations set forth in these Security Measures in the form of third-party certifications and audit reports.

8.2 Security Questionnaires. No more than once per year, we will complete a written security questionnaire provided by you regarding the controls outlined in these Security Measures.

3. DigitalOcean

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures of pseudonymization and encryption of personal data	DigitalOcean's databases that store Customer Personal Data are encrypted using the Advanced Encryption Standard (AES). Customer data is encrypted in transit between the Customer's software application and DigitalOcean using TLS v1.2.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	DigitalOcean uses a variety of tools and mechanisms to achieve high availability and resiliency. DigitalOcean's infrastructure spans multiple fault-independent availability zones in geographic regions physically separated from one another. DigitalOcean's infrastructure is able to detect and route around issues experienced by hosts or even whole data centers in real time and employ orchestration tooling that has the ability to regenerate hosts, building them from the latest backup. DigitalOcean also leverages specialized tools that monitor server performance, data, and traffic load capacity within each availability zone and colocation data center. If suboptimal server performance or overloaded capacity is detected on a server within an availability zone or colocation data center, these tools increase the capacity or shift traffic to relieve any suboptimal server performance or capacity overload. DigitalOcean is also immediately notified in the event of any suboptimal server performance or overloaded capacity.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	DigitalOcean has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems. The Customer Data Use Policy governs the requirements for use of customer data in accordance with several industry standards. DigitalOcean conducts a variety of regular internal and external audits that are inclusive of security operations. For more information please visit: https://www.digitalocean.com/trust/certification-reports/
Measures for user identification and authorization	Access control policies require that access to DigitalOcean assets be granted based on business justification, with the asset owner's authorization and limits based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews.Documentation of these requirements is recorded and provided to external auditors for security certification testing.
Measures for the protection of data during transmission Measures for the protection of data during storage	DigitalOcean's databases that store Customer Personal Data are encrypted using the Advanced Encryption Standard (AES). Customer data stored by DigitalOcean is encrypted in transit between the Customer's software application and DigitalOcean using TLS v1.2.
Measures for ensuring physical security of locations at which personal data are processed	DigitalOcean data centers are located in nondescript buildings that are physically constructed, managed, and monitored 24 hours a day to protect data and services from unauthorized access as well as environmental threats. All data centers are surrounded by a fence with access restricted through badge controlled gates.

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
	CCTV is used to monitor physical access to data centers and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities.
Measures for ensuring events logging	Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally. DigitalOcean restricts access to audit logs to authorized personnel based on job responsibilities. Audit logging procedures are reviewed as part of external audits for security standards.
Measures for internal IT and IT security governance and management Measures for certification/assurance of processes and products	DigitalOcean has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems. DigitalOcean performs an annual internal review of all security management policies and procedures. External auditors perform an annual review of these policies and procedures. DigitalOcean conducts a variety of regular internal and external audits that are inclusive of security operations. For more information please visit: https://www.digitalocean.com/trust/certification-reports/.
Measures for ensuring data minimization Measures for ensuring data quality Measures for ensuring limited data retention Measures for ensuring accountability Measures for allowing data portability and ensuring erasure	More information about how DigitalOcean processes personal data is set forth in the Privacy Policy available at: https://www.digitalocean.com/legal/privacy-policy/.
Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer.	When DigitalOcean engages a Subprocessor, DigitalOcean and the Subprocessor enter into an agreement with data protection obligations substantially similar to those contained in this Schedule. Each Subprocessor agreement must ensure that DigitalOcean is able to meet its obligations to Customer. In addition to implementing technical and organizational measures to protect personal data, sub-processors must (a) notify DigitalOcean in the event of a Security Incident so DigitalOcean may notify Customer; (b) delete personal data when instructed by DigitalOcean in accordance with Customer's instructions to DigitalOcean; (c) not engage additional sub-processors without DigitalOcean's authorization; (d) not change the location where personal data is processed; or (e) process personal data in a manner which conflicts with Customer's instructions to DigitalOcean.

4. Sentry

Technical and Organizational Measures	**Relevant Section(s) of Sentry Service Security Policy**
Measures of pseudonymization and encryption of personal data	• Data Flow – Data into System • Data Flow – Data through System • Data Security and Privacy – Data Encryption • Data Security and Privacy – PII Scrubbing
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• Infrastructure and Network Security – Physical Access Control • Infrastructure and Network Security – Logical Access Control • Application Security – Multi-Factor Authentication • Application Security – Single Sign-On • Application Security – SAML 2.0 • Application Security – REST API Authentication (API Key) • Application Security – Audit Controls
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• Infrastructure and Network Security – Intrusion Detection and Prevention • Business Continuity and Disaster Recovery • Corporate Security – Contingency Planning • Corporate Security – Vulnerability Disclosure
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	• Infrastructure and Network Security – Penetration Testing • Infrastructure and Network Security – Third-Party Audit • Corporate Security – Risk Management • Corporate Security – Security Policies
Measures for user identification and authorization	• Infrastructure and Network Security – Logical Access Control

Technical and Organizational Measures	**Relevant Section(s) of Sentry Service Security Policy**
	• Application Security – Multi-Factor Authentication • Application Security – Single Sign-On • Application Security – SAML 2.0 • Application Security – REST API Authentication (API Key) • Application Security – Audit Controls
Measures for the protection of data during transmission	• Data Flow – Data Through System
Measures for the protection of data during storage	• Data Security and Privacy – Data Encryption
Measures for ensuring physical security of locations at which personal data are processed	• Infrastructure and Network Security – Physical Access Control
Measures for ensuring events logging	• Application Security – Audit Controls
Measures for ensuring system configuration, including default configuration	• Application Security – Secure Application Development (Application Development Lifecycle) • Corporate Security – Risk Management • Corporate Security – Security Policies
Measures for internal IT and IT security governance and management	• Security and Compliance • Infrastructure and Network Security – Third-Party Audit • Corporate Security – Risk Management
Measures for certification/assurance of processes and products	• Infrastructure and Network Security – Third-Party Audit • Corporate Security – Risk Management
Measures for ensuring data minimization	• Data Security and Privacy – Data Retention

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy
	• Data Security and Privacy – Data Removal
Measures for ensuring data quality	• Data Flow – Data Through System • Data Security and Privacy – Data Encryption • Application Security – Audit Controls • Sentry maintains an online form to allow data subjects to request a copy of their personal data, make changes to their personal data or request deletion of their personal data
Measures for ensuring limited data retention	• Data Security and Privacy – Data Retention • Data Security and Privacy – Data Removal
Measures for ensuring accountability	• Corporate Security – Risk Management • Corporate Security – Security Policies
Measures for allowing data portability and ensuring erasure	• Sentry maintains an online form to allow data subjects to request a copy of their personal data, make changes to their personal data or request deletion of their personal data
Measures and assurances regarding U.S. government surveillance (“Additional Safeguards”)	• Sentry uses encryption both in transit and at rest. • As of the date of this DPA, Sentry has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. • No court has found Sentry to be the type of entity eligible to receive process issued under FISA Section 702: (i) an “electronic

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy
	communication service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition. • Sentry shall not comply with any request under FISA for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance). • Sentry shall use all available legal mechanisms to challenge any demands for data access through national security process that Sentry receives, as well as any non-disclosure provisions attached thereto. • Sentry shall take no action pursuant to U.S. Executive Order 12333. • Sentry publishes a transparency report indicating the types of binding legal demands for the personal data it has received, including national security orders and directives, which shall encompass any process issued under FISA Section 702. • Sentry will notify Customer if Sentry can no longer comply with the Standard Contractual Clauses or these Additional Safeguards, without being required to identify the specific provision with which it can no longer comply.

Codecov Service

Security Measures for the Codecov Service include the technical and organizational measures set forth below and in the current version of the Codecov Service Security Policy available at https://about.codecov.io/security/.

Technical and Organizational Measures	**Relevant Section(s) of Codecov Service Security Policy (if applicable)**
Measures of pseudonymization and encryption of personal data	• Data is encrypted at rest. Data transfers are secured using Transport Layer Security (TLS) and industry-standard encryption.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• Codecov Infrastructure Security • Codecov Code Security • Codecov Security Awareness
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• Codecov Code Security • Codecov Vulnerability Testing / Pentesting • Sentry has a documented Disaster Recovery Plan that defines procedures to recover all resources and processes necessary for service and data recovery, including all information security aspects of business continuity management. Sentry has a documented Incident Response Plan, which establishes procedures to be undertaken in response to information security incidents.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	• Codecov Vulnerability Testing / Pentesting
Measures for user identification and authorization	• Codecov Code Security
Measures for the protection of data during transmission	• Data transfers are secured using Transport Layer Security (TLS) and industry-standard encryption.
Measures for the protection of data during storage	• Codecov Infrastructure Security • Codecov Code Security
Measures for ensuring physical security of locations at which personal data are processed	• Sentry uses GCP to provide cloud hosting services for its production environment. The facilities, including the hardware and equipment therein, are maintained by GCP. The physical security, environmental controls and incident management for the facilities are also the responsibility of GCP. Additional information on GCP security measures are available here: https://cloud.google.com/docs/security/overview/whitepaper.

Technical and Organizational Measures	**Relevant Section(s) of Codecov Service Security Policy (if applicable)**
Measures for ensuring events logging	• Sentry logs authentication, availability and error events and uses tools for infrastructure management.
Measures for ensuring system configuration, including default configuration	• Codecov Infrastructure Security • Codecov Code Security
Measures for internal IT and IT security governance and management	• Codecov Security Compliance • Sentry has dedicated teams responsible for architecting, building and owning security.
Measures for certification/assurance of processes and products	• Codecov Security Compliance
Measures for ensuring data minimization	• Sentry retains raw/preprocessed coverage reports for 30 days. Options are provided for customers to request data removal.
Measures for ensuring data quality	• Codecov Infrastructure Security
Measures for ensuring limited data retention	• Sentry retains raw/preprocessed coverage reports for 30 days. Options for customers to request data removal are provided.
Measures for ensuring accountability	• Codecov Security Awareness • Codecov Responsible Disclosure Policy
Measures for allowing data portability and ensuring erasure	• Customers can contact Sentry for a copy of their data and/or request data erasure.
Measures and assurances regarding U.S. government surveillance (“Additional Safeguards”)	• Sentry uses encryption both in transit and at rest. • As of the date of this DPA, Sentry has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. • No court has found Sentry to be the type of entity eligible to receive process issued under FISA Section 702: (i) an “electronic communication service provider” within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition. • Sentry shall not comply with any request under FISA for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific “targeted selector”

Technical and Organizational Measures	Relevant Section(s) of Codecov Service Security Policy (if applicable)
	(an identifier that is unique to the targeted endpoint of communications subject to the surveillance). • Sentry shall use all available legal mechanisms to challenge any demands for data access through national security process that Sentry receives, as well as any non-disclosure provisions attached thereto. • Sentry shall take no action pursuant to U.S. Executive Order 12333. • Sentry will notify Customer if Sentry can no longer comply with the Standard Contractual Clauses or these Additional Safeguards, without being required to identify the specific provision with which it can no longer comply.

5. WorkOS

This Data Processing Addendum (“Addendum”) forms part of the Subscription Service Terms and Conditions (“Agreement”) between Subscriber and WorkOS.

1. 1. Subject Matter and Duration.

a) Subject Matter. This Addendum reflects the parties’ commitment to abide by Data Protection Laws concerning the Processing of Subscriber Personal Data in connection with WorkOS’s execution of the Agreement. All capitalized terms that are not expressly defined in this Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its exhibits conflicts with the Agreement, this Addendum shall control.

b) Duration and Survival. This Addendum will become legally binding upon the effective date of the Agreement. WorkOS will Process Subscriber Personal Data until the relationship terminates as specified in the Agreement.

2. 2. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) “Subscriber Personal Data” means Subscriber Data that is Personal Data Processed by WorkOS on behalf of Subscriber.

b) “Data Protection Laws” means all applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which the Subscriber Personal Data are subject. “Data Protection Laws” may include, but are not limited to, the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act) (“CCPA”) and the EU General Data Protection Regulation 2016/679 (“GDPR”).

c) “Process” or “Processing” means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

d) “Security Incident(s)” means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Subscriber Personal Data attributable to WorkOS.

e) “Subprocessor(s)” means WorkOS’s authorized vendors and third party service providers that Process Subscriber Personal Data.

3. 3. Data Use and Processing.

a) Documented Instructions. WorkOS shall Process Subscriber Personal Data to provide the Service in accordance with the Agreement, this Addendum, and

any instructions agreed upon by the parties. WorkOS will, unless legally prohibited from doing so, inform Subscriber in writing if it reasonably believes that there is a conflict between Subscriber's instructions and applicable law or otherwise seeks to Process Subscriber Personal Data in a manner that is inconsistent with Subscriber's instructions.

b) Authorization to Use Subprocessors. To the extent necessary to fulfill WorkOS's contractual obligations under the Agreement, Subscriber hereby authorizes WorkOS to engage Subprocessors.

c) WorkOS and Subprocessor Compliance. WorkOS agrees to (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Subscriber Personal Data that imposes on such Subprocessors data protection requirements for Subscriber Personal Data that are consistent with this Addendum; and (ii) remain responsible to Subscriber for WorkOS's Subprocessors' failure to perform their obligations with respect to the Processing of Subscriber Personal Data.

d) Right to Object to Subprocessors. Where required by Data Protection Laws, WorkOS will notify Subscriber prior to engaging any new Subprocessors by updating following website: www.workos.com/legal/subprocessors. WorkOS will allow Subscriber fourteen (14) calendar days to object to the new Subprocessor after notice is given. It is Subscriber's responsibility to check this website regularly for updates. If Subscriber emails support@workos.com with legitimate objections to the appointment of any new Subprocessor within the objection period set forth above, the parties will work together in good faith to resolve the grounds for the objection.

e) Confidentiality. Any person authorized to Process Subscriber Personal Data must contractually agree to maintain the confidentiality of such information or be under an appropriate statutory obligation of confidentiality.

f) Personal Data Inquiries and Requests. Where required by Data Protection Laws, WorkOS agrees to provide reasonable assistance and comply with reasonable instructions from Subscriber related to any requests from individuals exercising their rights in Subscriber Personal Data granted to them under Data Protection Laws.

g) Data Protection Impact Assessment and Prior Consultation. Where required by Data Protection Laws, WorkOS agrees to provide reasonable assistance at Subscriber's expense to Subscriber where, in Subscriber's judgement, the type of Processing performed by WorkOS requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

h) Demonstrable Compliance. WorkOS agrees to provide information reasonably necessary to demonstrate compliance with this Addendum upon Subscriber's reasonable request.

i) Service Optimization. Where permitted by Data Protection Laws, WorkOS may Process Subscriber Personal Data: (i) for its internal uses to build or improve the quality of its services; (ii) to detect Security Incidents; and (iii) to protect against fraudulent or illegal activity.

j) California Specific Terms. To the extent that WorkOS's Processing of Subscriber Personal Data is subject to the CCPA, this Section shall also apply. Subscriber discloses or otherwise makes available Subscriber Personal Data to WorkOS for the limited and specific purpose of WorkOS providing the Services to Subscriber in accordance with the Agreement and this Addendum. WorkOS shall: (i) comply with its applicable obligations under the CCPA; (ii) provide the same level of protection as required under the CCPA; (iii) notify Subscriber if it can no longer meet its obligations under the CCPA; (iv) not "sell" or "share" (as such terms are defined by the CCPA) Subscriber Personal Data; (v) not retain, use, or disclose Subscriber Personal Data for any purpose (including any commercial purpose) other than to provide the Services under the Agreement or as otherwise permitted under the CCPA; (vi) not retain, use, or disclose Subscriber Personal Data outside of the direct business relationship between Subscriber and WorkOS; and (vii) unless otherwise permitted by the CCPA, not combine Subscriber Personal Data with Personal Data that WorkOS (a) receives from, or on behalf of, another person, or (b) collects from its own, independent consumer interaction. Subscriber may: (1) take reasonable and appropriate steps agreed upon by the parties to help ensure that WorkOS Processes Subscriber Personal Data in a manner consistent with Subscriber's CCPA obligations; and (2) upon notice, take reasonable and appropriate steps agreed upon by the parties to stop and remediate unauthorized Processing of Subscriber Personal Data by WorkOS.

4. 4. Information Security Program.

a) Security Measures. WorkOS shall implement and maintain reasonable administrative, technical, and physical safeguards designed to protect Subscriber Personal Data in accordance with WorkOS's Information Security Standards attached hereto as Exhibit A.

5. 5. Security Incidents.

a) Notice. Upon becoming aware of a Security Incident, WorkOS agrees to provide written notice without undue delay and within the time frame required under Data Protection Laws to Subscriber. Where possible, such notice will include all available details required under Data Protection Laws for Subscriber

to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

6. 6. Cross-Border Transfers of Subscriber Personal Data.

a) Cross-Border Transfers of Personal Data. Subscriber authorizes WorkOS and its Subprocessors to transfer Subscriber Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States.

b) Data Transfer Impact Assessment Questionnaire. WorkOS agrees that it has provided true, complete, and accurate responses to the Data Transfer Impact Assessment Questionnaire attached hereto as Exhibit B.

c) EEA, Swiss, and UK Standard Contractual Clauses. If Subscriber Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Subscriber to WorkOS in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by the Standard Contractual Clauses attached hereto as Exhibit C. Where the Standard Contractual Clauses are applicable and Subscriber acts as a controller of Subscriber Personal Data with WorkOS acting as a processor of Subscriber Personal Data, each party shall comply with its obligations under Module Two of the Standard Contractual Clauses. Where the Standard Contractual Clauses are applicable and Subscriber acts as a processor of Subscriber Personal Data with WorkOS also acting as a processor of Subscriber Personal Data, each party shall comply with its obligations under Module Three of the Standard Contractual Clauses. The parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Standard Contractual Clauses will be provided upon Customer's written request; (ii) the measures WorkOS is required to take under Clause 8.6(c) of the Standard Contractual Clauses will only cover WorkOS's impacted systems; (iii) the audit described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section 5 of this Addendum; (iv) under Module 3, Clause 9(a), Subscriber shall be responsible for communicating any changes in subprocessors to the controller; (v) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Standard Contractual Clauses will be limited to the termination of the Standard Contractual Clauses, in which case, the corresponding Processing of Subscriber Personal Data affected by such termination shall be discontinued unless otherwise agreed by the parties; (vi) unless otherwise stated by WorkOS, Subscriber will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Standard Contractual Clauses; (vii) the information required under Clause 15.1(c) will be provided upon Subscriber's written request; and (viii) notwithstanding anything to the contrary, Subscriber will

reimburse WorkOS for all costs and expenses incurred by WorkOS in connection with the performance of WorkOS's obligations under Clause 15.1(b) and Clause 15.2 of the Standard Contractual Clauses without regard for any limitation of liability set forth in the Agreement. Each party's execution of the Agreement shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

d) Data Transfer Impact Assessment Outcome. Taking into account the information and obligations set forth in this Addendum and, as may be the case for a party, such party's independent research, to the parties' knowledge, the Subscriber Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the attached Standard Contractual Clauses to a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws is afforded a level of protection that is essentially equivalent to that guaranteed by applicable Data Protection Laws.

7. 7. Audits.

a) Subscriber Audit. Where Data Protection Laws afford Subscriber an audit right, Subscriber (or its appointed representative) may carry out an audit of WorkOS's policies, procedures, and records relevant to the Processing of Subscriber Personal Data by having WorkOS complete a data protection questionnaire of reasonable length. Any audit shall be: (i) be limited to once per year; and (ii) subject to reasonable confidentiality procedures.

8. 8. Data Deletion.

a) Data Deletion. At the expiry or termination of the Agreement, WorkOS will delete all Subscriber Personal Data (excluding any back-up or archival copies which shall be deleted in accordance with WorkOS' data retention schedule), except where WorkOS is required to retain copies under applicable laws, in which case WorkOS will isolate and protect that Subscriber Personal Data from any further Processing except to the extent required by applicable laws.

9. 9. Processing Details.

a) Subject Matter. The subject matter of the Processing is the Service pursuant to the Agreement.

b) Duration. The Processing will continue until the expiration or termination of the Agreement.

c) Categories of Data Subjects. Data subjects whose Subscriber Personal Data will be Processed pursuant to the Agreement.

d) Nature and Purpose of the Processing. The purpose of the Processing of Subscriber Personal Data by WorkOS is the performance of the Service.

e) Types of Subscriber Personal Data. Subscriber Personal Data that is Processed pursuant to the Agreement.

Exhibit A to the Data Processing Addendum
WorkOS Information Security Standards

This Exhibit A forms part of the Addendum. Capitalized terms not defined in this Exhibit A have the meaning set forth in the Addendum.

WorkOS shall implement and maintain an information security program ("Information Security Program") that: (i) is consistent with WorkOS's then current SOC 2 Type II certification and industry standard practices taking into consideration the sensitivity of the relevant Subscriber Personal Data, and the nature and scope of the Service to be provided; (ii) includes reasonable administrative, technical and physical safeguards designed to protect Subscriber Personal Data; and (iii) complies with Data Protection Laws. At a minimum, the Information Security Program shall include:

10. Information Security Policy. WorkOS shall maintain a written information security policy applicable to all authorized personnel.
11. Training. WorkOS shall provide information security awareness training to all employees annually.
12. Access Control. WorkOS shall maintain access control procedures and controls consistent with industry standard practices. WorkOS shall limit access to Subscriber Personal Data to those employees and Subprocessors with a need-to-know.
13. Logical Separation. WorkOS shall ensure Subscriber Personal Data is logically separated from other WorkOS client data.
14. Encryption. Where appropriate, WorkOS shall encrypt Subscriber Personal Data in-transit and at rest using industry standard encryption technologies.
15. Password Management. WorkOS shall maintain a password management policy designed to ensure strong passwords consistent with industry standard practices.
16. Incident Response Plan. WorkOS shall maintain an incident response plan that addresses Security Incident handling.
17. Malware Protection. WorkOS shall maintain up-to-date malware prevention measures designed to protect against malicious code and viruses.

18. Backups of Subscriber Personal Data. WorkOS shall maintain an industry standard backup system and backup of Subscriber Personal Data to facilitate timely recovery in the event of a service interruption.

19. Disaster Recovery and Business Continuity Plans. WorkOS shall maintain disaster recovery and business continuity plans consistent with industry standard practices.

Exhibit B to the Data Processing Addendum
Data Transfer Impact Assessment Questionnaire

This Exhibit B forms part of the Addendum. Capitalized terms not defined in this Exhibit B have the meaning set forth in the Addendum.

1. What countries will Subscriber Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from? If this varies by region, please specify each country for each region.

   Answer: United States of America.

2. What are the categories of data subjects whose Subscriber Personal Data will be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

   Answer: As set forth in Section 9(c) of the Addendum.

3. What are the categories of Subscriber Personal Data transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

   Answer: As set forth in Section 9(e) of the Addendum.

4. Will any Subscriber Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom? If so, are there any 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?

   Answer: Not to WorkOS's knowledge.

5. What business sector is WorkOS involved in?

Answer: Software.

6. Broadly speaking, what are the services to be provided and the corresponding purposes for which Subscriber Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

Answer: WorkOS provides services for software/app development. Subscriber Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom in order to provide the Service.

7. What is the frequency of the transfer of Subscriber Personal Data outside of outside of the European Economic Area, Switzerland, and/or the United Kingdom? E.g., is Subscriber Personal Data transferred on a one-off or continuous basis?

Answer: Subscriber Personal Data is transferred on a continuous basis by virtue of Subscriber's use of the Service.

8. When Subscriber Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom to WorkOS, how is it transmitted to WorkOS? Is the Subscriber Personal Data in plain text, pseudonymized, and/or encrypted?

Answer: Subscriber Personal Data is encrypted during transmission to WorkOS.

9. What is the period for which the Subscriber Personal Data will be retained, or, if that is not possible, the criteria used to determine that period?

Answer: Subscriber Personal Data will be retained in accordance with the Addendum.

10. Please list the Subprocessors that will have access to Subscriber Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom:

Answer: A current list of WorkOS's Subprocessors can be found at: https://workos.com/legal/subprocessors.

11. Is WorkOS subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where Subscriber Personal Data is stored or accessed from that would interfere with WorkOS fulfilling its obligations under the attached Standard Contractual Clauses? For example, FISA Section 702. If yes, please list these laws.

Answer: As of the effective date of the Addendum, no court has found WorkOS to be eligible to receive process issued under the laws contemplated

by Question 11, including FISA Section 702, and no such court action is pending.

12. Has WorkOS ever received a request from public authorities for information pursuant to the laws contemplated by Question 11 above (if any)? If yes, please explain.

Answer: No.

13. Has WorkOS ever received a request from public authorities for Personal Data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.

Answer: No.

14. What safeguards will WorkOS apply during transmission and to the processing of Subscriber Personal Data in countries outside of the European Economic Area, Switzerland, and/or the United Kingdom that have not been found to provide an adequate level of protection under applicable Data Protection Laws?

Answer: Those safeguards set forth in the Addendum.

Exhibit C to the Data Processing Addendum

This Exhibit C forms part of the Addendum.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b)The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’)

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

(e) To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.

(f) To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III).

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d), and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules Two and Three: Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause – Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its

behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories

and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the

instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the

data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least two (2) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under

Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.

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

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least two (2) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.

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

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Where the data exporter is established in an EU Member State, the following section applies: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the following section applies: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the following section applies: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed

in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in

consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting

authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.