ANNEX A

Information Protection and Security Standards of Docebo Learning Suite

PREMISES

This document constitutes the Information Protection and Security Standard Annex (the "***IPSS Annex***") of the Data Processing Addendum (the "***Addendum***"). All terms used and not otherwise defined herein, shall have the meanings ascribed to them in the Addendum.

The Docebo Learning Suite (DLS) relies on AWS and Docebo leverages the comprehensive and state-of-the-art security capabilities provided by AWS.

The respective security responsibilities among Docebo and AWS are defined in the AWS Shared Responsibility Model (available at https://aws.amazon.com/compliance/shared-responsibility-model), as the same may be updated, from time to time.

Docebo has implemented and maintains an Information Security Management System ("***ISMS***") and is committed to the standards contained in and available at https://www.docebo.com/company/compliance-security/.

Within this framework, Docebo has defined an information security program implementing, in accordance with ISO/IEC 27001 and AICPA/ISAE 3000 SOC 2, policies, procedures, administrative and technical safeguards to minimize security risks, through risk assessment, and to protect its customers' data against accidental or unlawful loss, access or disclosure or other misuse.

The information security program includes the following measures:

INFORMATION SECURITY ORGANIZATION AND POLICIES

Docebo has implemented and maintains an Information Security Management System (ISMS) and a comprehensive information security program which is documented, available, and communicated to employees and subcontractors.

The effectiveness of the information security program is regularly monitored and reviewed, and, in any event, at least annually. Adjustments and strengthening are applied as appropriate, based on the results of such monitoring, as well as in response to operational changes that may affect the ISMS.

HUMAN RESOURCES SECURITY

Docebo has implemented and maintains appropriate measures to ensure that personnel (employees and contractors) involved in the processing of Customer Data are authorized with a need to access the data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection and handling of Customer Data.

Docebo has implemented and maintains an acceptable use policy for Docebo personnel usage of Docebo devices, systems, and infrastructure, as well as management of customer information, including Customer Data. Docebo monitors policy compliance and will take appropriate action in response to violations.

An Information Security Awareness Program is defined in relation to the handling and protection of Customer Data and to compliance with the ISMS so that personnel are aware of established information security policies and security rules. Such Information Security Awareness Program provides initial education, on-going awareness and addresses the evolving non-technical security threats introduced by human behavior as well as data protection regulations.

Docebo ensures that access to Customer Data is revoked immediately upon termination or when access is no longer required for personnel involved in the processing of Customer Data.

Docebo ensures that personnel involved in the Customer Data processing are screened, to the extent permitted under applicable law, in accordance with industry best practices for performing criminal background screening.

PHYSICAL SECURITY

Policies and procedures, and supporting business processes, are in place for maintaining a safe and secure working environment in Docebo's offices and to control physical access including appropriate alarms, access provisioning, CCTV cameras, and escorting of visitors.

The Docebo Learning Suite relies on AWS who is responsible, in accordance with the AWS Shared Responsibility Model, (available at https://aws.amazon.com/compliance/shared-responsibility-model), for implementing controls for physical security of data center facilities, backup media, and other physical systems, providing comprehensive and state-of-the-art security capabilities (available at https://aws.amazon.com/compliance/data-center/controls).

Docebo ensures that such physical security controls provided by AWS for its datacenter include:

- Access is restricted by the use of an electronic key card and/or biometric system, which is unique to each individual.
- CCTV is present on all access and exit doors, and recordings stored for at least thirty 30 days.
- Access areas to the building are guarded by security on a 24/7 basis, 365 days a year, either by internal or external staff and an intruder alarm is in place for all building access points to detect and alert against unauthorized entry.
- Access to the location of the servers and network components, which deliver Services, i.e. servers, dialers, switches, routers, firewalls, etc., are restricted to authorized personnel only and adequately logged.

ACCESS CONTROL

Docebo has implemented and maintains access control processes and mechanisms to prevent unauthorized access to Customer Data and to limit access only to authorized personnel with a business need to know. Such processes and mechanisms are supported by an Identity Access Management (IAM) tool centrally managed for the most relevant Docebo systems and internal applications and include password configuration and management procedures for all end user and system accounts related to the processing environment following recognized industry best practices for password length, structure and rotation.

The access to Customer Data is achieved by means of authenticated individual accounts and is limited solely to personnel which need access to perform specific responsibilities or functions in support of the Services.

Administrator accounts are used only for the purpose of performing administrative activities, and each account is traced to a uniquely-identifiable individual and two-factor authentication is required for access to the Docebo Learning Suite platforms' control plane and other critical resources.

Accounts are disabled upon personnel termination or change of roles and responsibilities, and it is an established and maintained process to periodically review access controls.

APPLICATION USER ACCESS

Docebo Learning Suite provides advanced access mechanisms with appropriate control over application features and data allowing configuring user access restrictions as stated in the specific Docebo Learning Suite (DLS) service documentation.

Users are required to verify their login using unique credentials (username and password) and anonymous logins are not permitted.

Docebo Learning Suite allows the configuration of different levels of password complexity, including but not limited to the following, as stated in the specific DLS service documentation:

- Set a minimum password length
- Request to create a password with mixed alphanumeric characters
- Request a change of password at a user's next sign-in

Support for Single Sign On (SSO) modalities through external Identity Providers federation is provided for some of the DLS Services as stated in the specific documentation.

DATA SEGMENTATION

Docebo has implemented and maintains logical data segregation to ensure Customer Data is not viewable by unauthorized users and that the Customer can access its data set only.

DATA DESTRUCTION

Docebo relies on AWS for data destruction and can only perform logical deletion.

Deleted Customer Data is rendered unreadable or disabled by AWS and the underlying storage areas on the AWS network that were used to store the content are wiped, prior to being reclaimed and overwritten, in accordance with AWS standard policies and deletion timelines.

AWS procedures also include a secure decommissioning process conducted prior to disposal of storage media used to provide the AWS services. As part of that process, storage media is degaussed or erased and physically destroyed or disabled in accordance with industry standard practices."

The AWS practices for data destruction are contained in the "Amazon Web Services – EU Data Protection Whitepaper" available at:
https://d1.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf

DATA ENCRYPTION

Cryptography: Docebo utilizes encryption key management services and encryption algorithms which are auditable, aligned with industry standards, in wide use and meet the following minimums:

- For symmetric encryption: key length of at least 256 bits;
- For asymmetric encryption: key length of at least 2048 bits;
- Elliptic curve systems 224-bit ECC or higher; and
- Hashing algorithms: SHA2 or SHA256 or better.

Data in transit: Access to the Docebo Learning Suite can be limited to connecting only through SSL/HTTPS secure connections.

Data at rest: Encryption at the storage level is provided by leveraging the capability of Amazon S3 and DynamoDB to store the file with 256-bit AES encryption and by leveraging AWS Key Management Service for the RDS database volume encryption.

MALICIOUS CODE PROTECTION

An endpoint protection antivirus centrally managed solution has been deployed.

BACKUP

Docebo provides a state-of-art backup policy for Customer Data.
The frequency of the backup policies vary, based on the specific Docebo Learning Suite service and the service type subscribed for in the Agreement, and may range from a daily basis up to three (3) or more complete backup jobs per day.

Backups are subject to recurring integrity tests, performed at least once per year, in order to ensure that the backups are correct, complete, and recoverable.

Backups are kept as long as the Service is active and they are encrypted at rest.

DESKTOP AND LAPTOP SECURITY

Docebo has implemented and maintains desktop and laptop system administration procedures that meet or exceed industry standards including automatic operating system patching and upgrading, anti-virus software and hard drive encryption.

SERVER AND SYSTEM SECURITY

Docebo has implemented and maintains system administration procedures that meet or exceed industry standards including system and device patching processes and system hardening based on pre-configured virtual machine image secured baseline.

NETWORK SECURITY

The Docebo Learning Suite relies on Amazon AWS who is responsible, in accordance with the AWS Shared Responsibility Model (available at https://aws.amazon.com/compliance/shared-responsibility-model), for implementing data center network security providing comprehensive and state-of-the-art security capabilities (available at https://aws.amazon.com/compliance/data-center/controls).

Docebo has implemented and maintains technical measures designed to meet or exceed industry standards aimed to monitor, detect, and prevent malicious network activity on the network infrastructures under its control and management responsibility.

Such measures include, but are not limited to firewalls and intrusion detection that may be implemented on the AWS Virtual Private Cloud (VPC) through the mechanisms provided by AWS like, for example, the AWS Security Group virtual firewalls that are configured to enforce boundaries of VPC and restrict access to the computing environment of the Docebo Learning Suite.

For DDoS protection the Docebo Learning Suite relies on AWS Shield Standard service.

Docebo ensures that firewalls, network routers, switches, load balancers, domain name servers, mail servers, and other network components of the network infrastructures under its control and management responsibility are configured and secured in accordance with commercially reasonable industry standards.

REMOTE ACCESS

Docebo has implemented and maintains remote access policies and procedures that meet or exceed industry standards for Docebo personnel who require remote access to a network or system that protects, processes or stores Customer Data. These policies and procedures include, without limitation, a restriction of user access to systems, a minimum of two-factor authentication and logging, limited to what is compatible with AWS technology logging features, detailing all activity conducted during each user session, and VPN connection through Bastion Host gateway in accordance with the Amazon AWS best practices.

EVENT LOGGING AND MONITORING

Docebo has implemented and maintains systems event logging procedures designed to meet or exceed industry standards in the detection, investigation and response to suspicious activity in a timely manner.

Logs are sent to a centralized logging repository, and monitoring tools are in place in order to analyze the logs for possible or actual security incident.

Logging capabilities of each DLS service is specified, when provided, in the relevant documentation.

THREATS AND VULNERABILITIES MANAGEMENT

Docebo has implemented and maintains a threat and vulnerability management program to continuously monitor for vulnerabilities in the Docebo Learning Suite that are acknowledged by vendors, reported by researchers, or discovered through the scheduling and execution of internal and external vulnerability scans and penetration tests.

Identified vulnerabilities are assessed to evaluate the associated risks, and the appropriate remediation actions are carried out according to the established change management policy with the assigned priority.

Docebo will use its best efforts to remediate high severity vulnerabilities (as identified in the CVSS base score of 7.0 or higher) in a timely manner.

PATCH MANAGEMENT

Docebo has implemented and maintains patch management procedures that meet or exceed industry standards and that require patches to be prioritized, tested and installed based upon criticality for all systems which are part of the Docebo Learning Suite.

Patches will be installed according to Docebo's change management policy with the assigned priority and scheduling based on assessed risk and operational criteria defined by Docebo, after being previously tested and evaluated to avoid adverse side effects.

SYSTEM DEVELOPMENT AND MAINTENANCE

Docebo has implemented and maintains a secure development lifecycle (“***SDLC***”) methodology to govern the acquisition, development, implementation, configuration, maintenance, modification, and management of infrastructure and software components of the Docebo Learning Suite.

The SDLC includes procedures for user involvement, testing, conversion, and management approvals of system features that are designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications, NIST) and at minimum address OWASP top 10 vulnerabilities.

The developed code is reviewed and validated by at least one other developer against the security requirements and coding guidelines and a static and dynamic code/program analysis are conducted as appropriate or when and if available prior the release on production.

TEST DATA

Any use of Customer Data in non-production environments requires explicit and documented approval from the Customer and must comply with all legal and regulatory requirements for the scrubbing of sensitive data elements.
All fields that could have any Personal Data must be obfuscated.

QUALITY ASSURANCE

Docebo has implemented and maintains a quality assurance program that meets or exceeds industry standards and that is developed, resourced and executed to maintain the quality levels for the Services as defined in the Agreement and Docebo's quality policies and procedures.

CHANGE MANAGEMENT

Docebo has implemented and maintains a change management program that meets or exceeds industry standards including, without limitation, maintenance, patches, data formatting changes, new deployments of code or systems, or for any work to restore services as the result of an Incident, where as “incidents” are intended events that are not part of the standard operation of the Services and cause an interruption to, or a reduction in, the quality of the Services, or events causing integrity or confidentiality issues on Customer Data or security incidents.

A systematic approach with a division of roles and responsibilities is applied to managing change and ensuring that changes of any Docebo Learning Suite functionality are reviewed, tested and approved. Development, testing and implementation are segmented functions within the process and a dedicated environment separate from production is maintained for development and testing activities. Change management standards are based on established guidelines and tailored to the specifics of each change request.

SUPPLIERS AND THIRD PARTIES MANAGEMENT

Docebo has implemented and maintains policies and procedures to engage third-party suppliers and to regularly monitor, review and audit its suppliers service delivery.

Docebo third-party suppliers' involvement in the processing of Customer Data is subject to the conditions established in the Addendum.

INCIDENT MANAGEMENT

Docebo has implemented and maintains policies and procedures for identifying, acting upon, remediating and reporting incidents, where as "incidents" are intended events that are not part of the standard operation of the Services and cause an interruption to, or a reduction in, the quality of the Services, or events causing integrity or confidentiality issues on Customer Data or Security Breaches .

Incidents are logged within a ticketing system, assigned a severity rating and tracked to resolution.

Documented escalation procedures for managing incidents are in place to guide the response and mitigation activities, as well as procedures for the investigation into the root cause(s) of identified incidents.

Docebo will notify the Customer of confirmed incidents as established in the Agreement and in the Addendum for Security Breaches.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Docebo has implemented and maintains a Business Continuity and Disaster Recovery program that meets or exceeds industry standards and that provides a formal framework and methodology, including without limitation, a business impact analysis, risk assessment process to identify and prioritize critical business functions and define appropriate contingency plans. The Recovery Time Objectives (RTO) is thirty-six 36 hours and the Recovery Point Objective (RPO) is determined by the frequency of the backups, based on the specific DLS service type subscribed for in the Agreement.
Docebo will update the operability of any applicable contingency plan and test its Disaster Recovery plan at least annually.

AUDIT

Docebo is committed to achieve by engagement of a competent third-party provider, a security audit (whether or not the audit is for certification purpose) at least once a year, at its own expenses in order to verify its compliance with this IPSS Annex.

Such audit will be performed according to ISO 27001 and AICPA/ISAE 3000 SOC 2 standards or such other alternative standards that are substantially equivalent to ISO 27001 and AICPA/ISAE 3000 SOC2.

Docebo undertakes to communicate, upon the Customer's request, the summary report of the most recent audit performed in the last twelve (12) months.

The Customer agrees to exercise any right that it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing Docebo to carry out the audit described above. Alternatively, upon the Customer's written request Docebo will allow the Customer to perform audit activity for the purpose of verifying Docebo's compliance with the obligations of this Addendum and applicable law. Such audit activities shall be conducted no more frequently than once per calendar year in accordance with the conditions established in the Addendum and shall be subject to the confidentiality obligations set forth in the Agreement.

For all Docebo material subcontractors or cloud service providers which access, process, or store Customer Data, Docebo will establish written contracts with the same that include appropriate assessment rights. For any that will not agree specifically to onsite assessment rights, Docebo will ensure that an appropriate independent audit occurs annually, according to ISO 27001 and AICPA/ISAE 3000 SOC 2 standards or such other alternative standards that are substantially equivalent to ISO 27001 and AICPA/ISAE 3000 SOC 2, and that the resulting reports are reviewed by Docebo.
Docebo will provide the details of its audit report review to the Customer, including any identified items of noncompliance upon the Customer's request.

VULNERABILITY ASSESSMENT AND PENETRATION TEST

Docebo will conduct at least once per year an application vulnerability assessment and penetration tests ("***VAPT***") by use of an external company and have a process in place to manage and remediate any newly found vulnerabilities.

Docebo will provide the details of its VAPT report to the Customer, upon the Customer's request.

Docebo will allow the Customer to conduct no more than annually an application VAPT in accordance with the conditions established in the Addendum.