




Docebo and GDPR compliance

docebo

Activity Overview

My Profile









Jerry Miles
arturo.mckenzie@mycompany.com

Level: Super Admin Occupation: UX-Designer

Date of Birth: 25 December, 89 Country: Canada

[CHANGE PASSWORD](#) [MY ACTIVITIES](#) [MY PROFILE](#)

Top 3 Experts by shared contents

-  **Christopher Reese**
12345 shared contents
Weekly Trend: 
-  **Howard Arnold**
2453 shared contents
Weekly Trend: 
-  **Jessie Ball**
1346 shared contents
Weekly Trend: 

Learning Platform

Drive employee, partner, and customer growth


Increase performance

Drive revenues

Retain top talents

My Courses and Learning Plans


[FILTER](#)



WEBINAR

Life Advice Looking Through A Window

English [***](#)




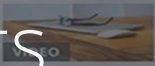
CLASSROOM


Video Games Playing With Imagination

English [***](#)

Activity Stream

 **Stacy Miller** has been enrolled in course **Consumer Psychology In The Industrial And Manufacturing Equipment Marketplace**
23 min ago


 **Consumer Psychology In The Industrial And Manufacturing Equipment Marketplace**
English

 **Frank Miller** asked:
How can I retain the talent in the organization during a recession and without a dedicated budget?

Related to: **Perform Module 1 - Roles and Skills**

Answer Now | [View all 5 replies](#)

Yesterday at 20:45 76 view

 **Paul Livingston** The way to retain talent is the same in times of recession...

www.docebo.com



5

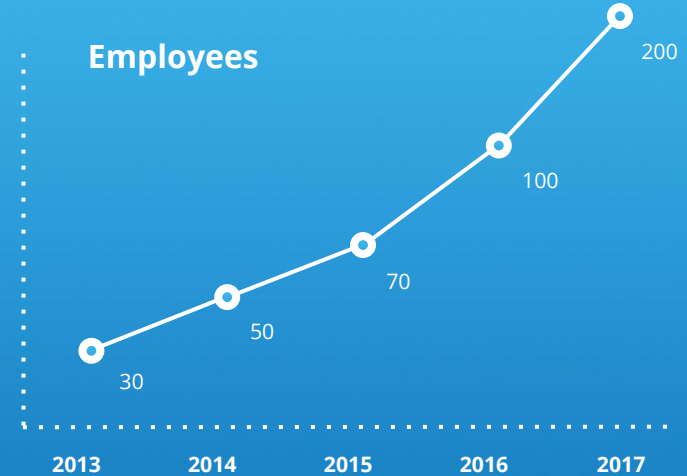
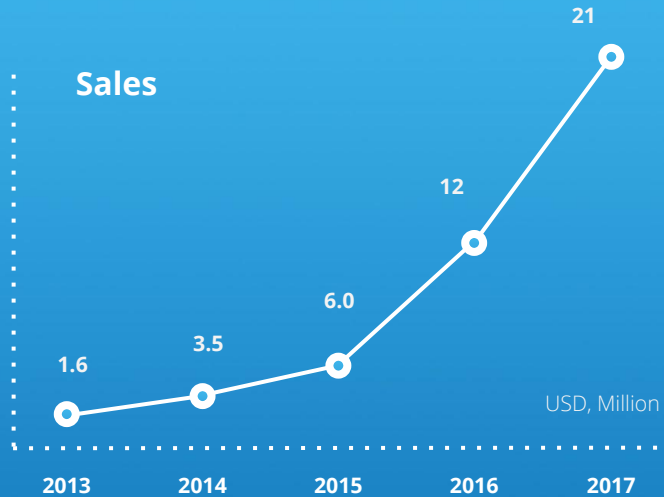
OFFICES

230+

EMPLOYEES

1450

CLIENTS IN 80 COUNTRIES
WORLDWIDE NETWORK OF PARTNERS

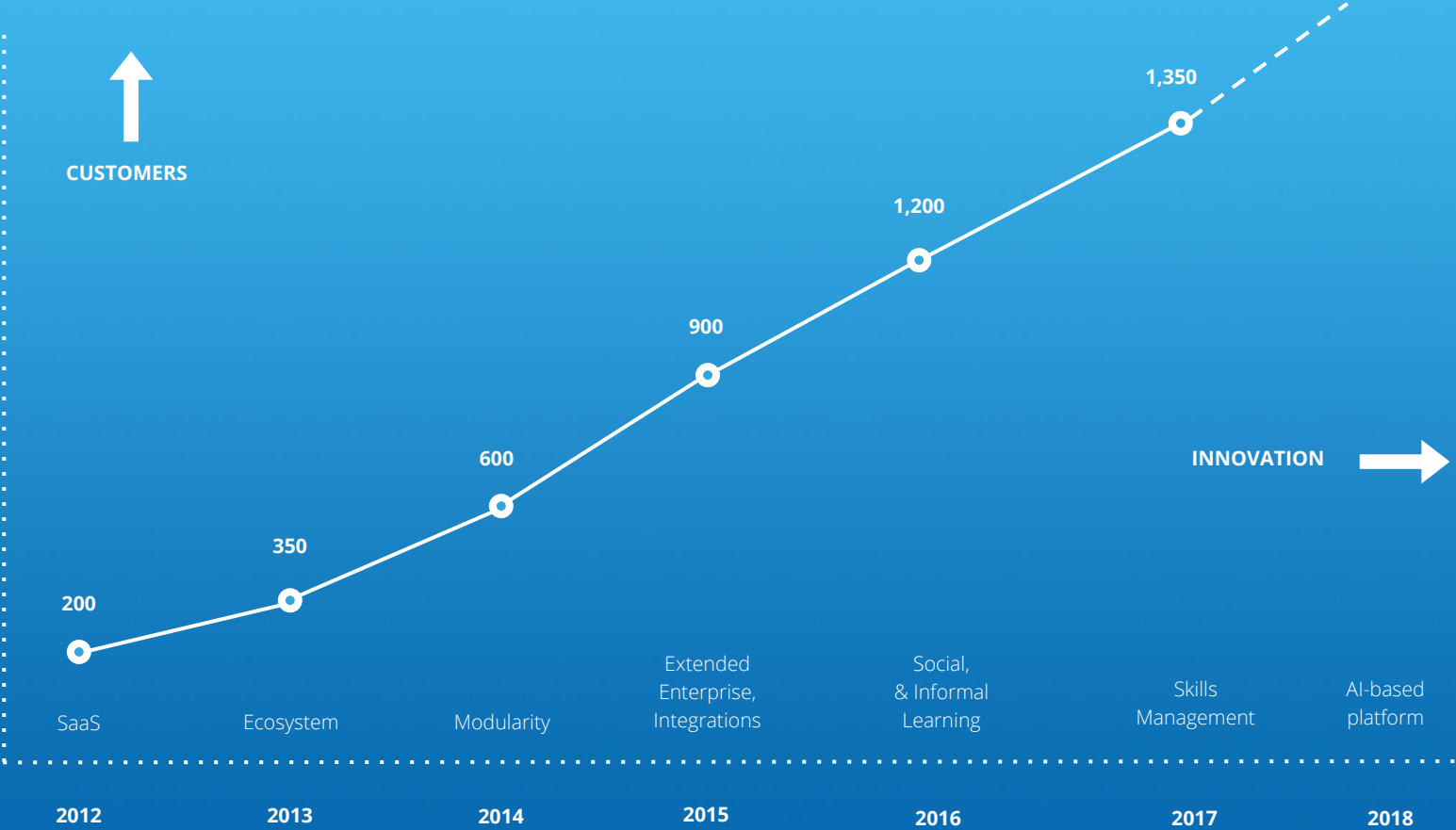


3 Millions
Learners

61%
North
America

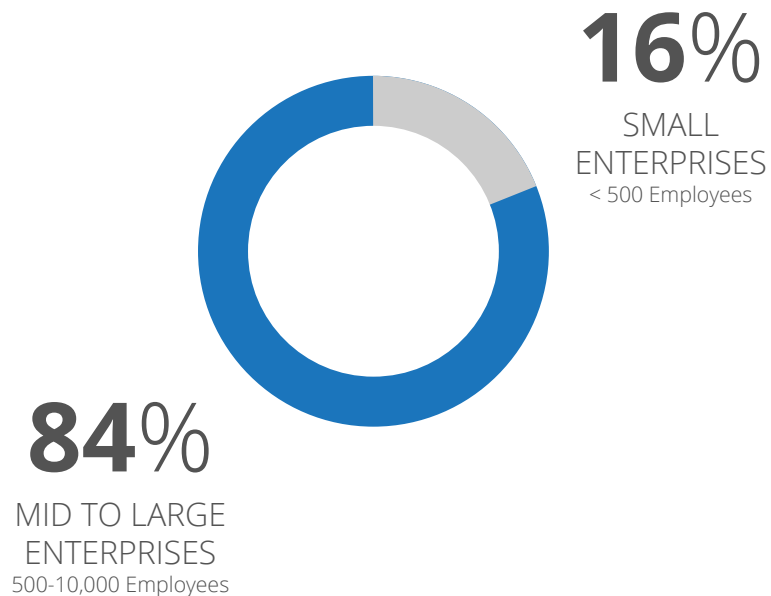
31%
EMEA

7%
APAC
South America

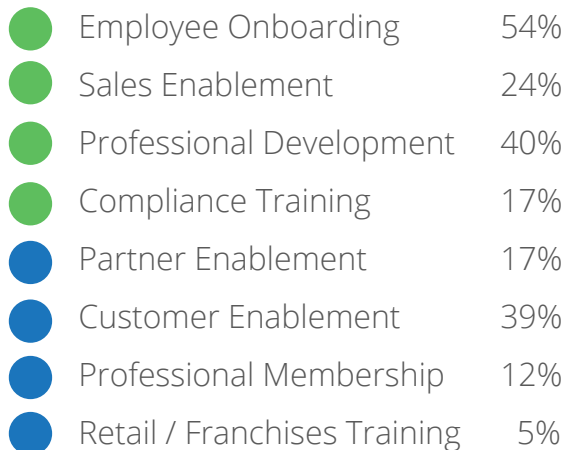


Top Industries

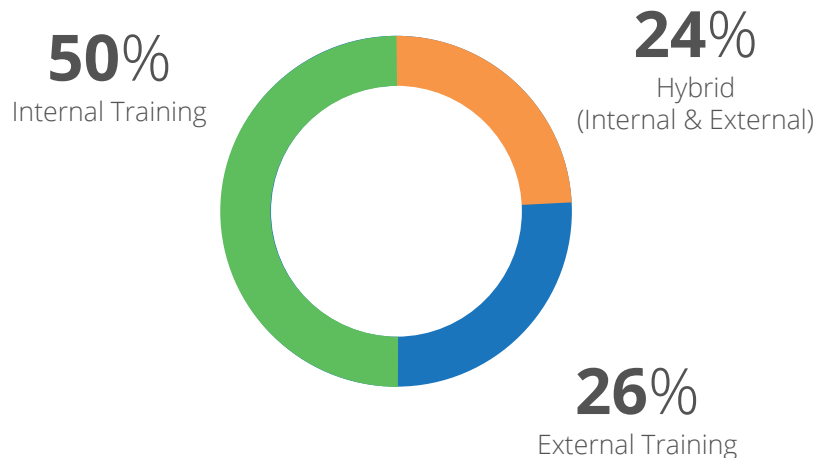
Internet, Technology, Financial Services,
Retail, Healthcare, Manufacturing, Media,
Training, Consulting



Our customers use Docebo for ...



Any given customer often uses Docebo to support different use cases with the same platform





Best Advance in
Learning Management Technology



Best Advance in
Social Learning Technology



Best Advance in
Creating a Learning Strategy



Best Strategy for a
Corporate Learning University

datto docebo®

 **CINEPLEX** **docebo**®



*"Best online training platform
for business on the market."*





Modern design, ultimate learning experience



Address formal, informal and social learning modalities



Scale as learning projects grow



White-label and publish your own apps



Extended Enterprise



Highly flexible, limitless configurability



30+ Productized Integrations
Rest APIs



Exclusive focus on Learning

Releasing first to market, learner-centric technology at an unmatched pace in the industry.

How Docebo explained to Customers its GDPR approach

Communication campaign to worldwide customers

- **GDPR overview and main concepts: information on GDPR**
- **Docebo roles (Controller/Processor): roles played by Docebo**
- **Docebo GDPR compliance and security posture: how we comply**
- **What Docebo provides to comply with GDPR: what we provide you**

GDPR overview and main concepts

What is the GDPR ?

- The "GDPR" is the General Data Protection Regulation, the new EU Data Protection Regulation, whose purpose is to strengthen the rights of European Union (EU) citizens with regard to how their personal data is used and how it's protected
- Introduces robust requirements that will raise and harmonize standards for data protection, security, and compliance across the EU
- The **GDPR is enforceable May 25th, 2018** and it replaces the EU Data Protection Directive (Directive 95/46/EC)
- Territorial scope: Organisations established in the EU and Organisations without an EU presence who target or monitor EU individuals, that is any organization inside or outside the EU who is doing business with Europeans that involves the processing of their personal data

[Find more information about GDPR here](#)

docebo®

Copyright © 2018 Docebo - All rights reserved.

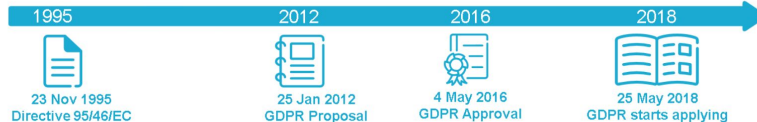
13

www.docebo.com

What is the GDPR ?

GDPR comprises 99 articles
and 173 recitals
divided into 11 chapters

GDPR
General Data Protection Regulation



Chapter 1	- General provisions - (1 2 3 4)
Chapter 2	- Principles - (5 6 7 8 9 10 11)
Chapter 3	- Rights of the data subject - (12 13 14 15 16 17 18 19 20 21 22 23)
Chapter 4	- Controller and processor - (24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43)
Chapter 5	- Transfers of personal data to third countries or international organisations - (44 45 46 47 48 49 50)
Chapter 6	- Independent supervisory authorities - (51 52 53 54 55 56 57 58 59)
Chapter 7	- Cooperation and consistency - (60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76)
Chapter 8	- Remedies, liability and penalties - (77 78 79 80 81 82 83 84)
Chapter 9	- Provisions relating to specific processing situations - (85 86 87 88 89 90 91)
Chapter 10	- Delegated acts and implementing acts - (92 93)
Chapter 11	- Final provisions - (94 95 96 97 98 99)

docebo®

[Here you can find many more information about GDPR](#)



14

www.docebo.com

What is the GDPR ?

General key issues

GDPR
General Data Protection Regulation



INCREASED SANCTIONS

- Fines up to €20 million or 4% of annual global turnover
- Depending on the seriousness or repeated nature of GDPR breach
- Determined by a local country's supervisory authority

EXTENDED BORDERS

GDPR concerns the protection of personal data of, or relating to EU citizens, processed both in and outside of the EU.

EXPANDED COMPLIANCE

- Controllers and Processors must demonstrate compliance of GDPR by adopting detailed processing of records.
- Both are now equally liable (in case of breach)

ENHANCED RIGHTS FOR INDIVIDUALS

Access, Data portability, Rectification, Object, Erasure, Restriction

DATA PROTECTION OFFICER

Organisations will be obliged to appoint a Data Protection Officer (DPO) when:

- processing 'large scale' systematic monitoring of individuals,
- 'large scale' processing of sensitive data;
- if organizations are public authority.

EXPLICIT INFORMED CONSENT

Organisations must receive clear and affirmative consent to process personal data

MANDATORY BREACH REPORTING

The GDPR imposes a requirement on data controllers to notify data breaches to the national data protection authority

docebo®

www.docebo.com

docebo®

GDPR overview and main concepts

What is personal data?

"Personal data" means any information relating to an identified or identifiable natural person ("data subject")

An **identifiable person** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

Content

Anything that a customer (or any end user) stores, or processes using Docebo LMS, including:
Data | Text | Audio | Video

Personal Data

Information from which a living individual may be identified or identifiable (under EU data protection law)

- Customer's "content" might include "personal data"

PERSONAL DATA

=
DATA EXPLOITABLE TO IDENTIFY A
NATURAL PERSON

Under GDPR can be personal data:
IP addresses, application user IDs, GPS data, cookies, MAC addresses, unique mobile device identifiers (UDID), and International Mobile Equipment IDs (IMEI)

docebo®

Copyright © 2018 Docebo - All rights reserved.

14

www.docebo.com

Involved entities



The Data subject

Identified or identifiable natural person to whom personal data are related

docebo®



The Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data



The Processor

The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Copyright © 2018 Docebo - All rights reserved.

15

www.docebo.com

docebo®

Copyright © 2018 Docebo - All rights reserved.

13

www.docebo.com

GDPR overview and main concepts

GDPR main principles

The GDPR is structured around six key principles (detailed in [Article 5](#) of the legislation):

- | | |
|------------------------------|--|
| 1) LAWFULNESS | Transparency on how data will be used and what it will be used for |
| 2) PURPOSE | Ensuring that the data collected is used only for the purposes explicitly specified at the time of collection |
| 3) DATA MINIMIZATION | Limiting the data collection to what is necessary to serve the purpose for which it is collected |
| 4) DATA ACCURACY | Make sure that data is accurate and ideally stored in a way that allows users to update and delete them |
| 5) STORAGE LIMITATION | Storing the data for only as long as necessary within its intended purpose (Retention policy) |
| 6) DATA SECURITY | Prevention against unauthorized use or accidental loss of the data through the deployment of appropriate security measures |



docebo®

Copyright © 2018 Docebo - All rights reserved.

15

www.docebo.com

Accountability

Moreover the **accountability** requirement demonstrates how compliance with the above principles is being managed and tracked.

This means maintaining records (providing evidence) of how and why personal data was collected as well as the documentation of the processes put in place to protect it.



docebo®

Copyright © 2018 Docebo - All rights reserved.

16

www.docebo.com

What Else Comes With GDPR?

Data subjects rights

LMS functionalities and Docebo support services

The right to Data Portability

Individuals have the right to get a copy of all the personal data that controllers have regarding him or her. It also must be provided in a way that facilitates reuse.

SQL dump or csv from DB extraction on request

The right To Be Forgotten (Erasure)

This gives individuals the right to have certain personal data deleted so third parties can no longer trace them.

User and LMS admins can delete/modify user profile

docebo®

Copyright © 2018 Docebo - All rights reserved.

17

www.docebo.com

What Else Comes With GDPR?

Controller/Processor responsibilities

LMS functionalities and Docebo support services

Privacy by Design

This helps to facilitate the inclusion of policies, guidelines, and work instructions related to data protection in the earliest stages of projects including personal data.

- Privacy and data protection considered among the development requirements
- ISO 27001 ISMS SDLC procedures include privacy by design

Data Breach Notification

Controllers must report personal data breaches to the relevant supervisory authority within 72 hours. If there is a high risk to the rights and freedoms of data subjects, they must also notify the data subjects.

- 72 hours is for controllers only.
- Specific deadline not required for Processor.
- Processor notifies "without undue delay"
- Ruled in the DPA

docebo®

Copyright © 2018 Docebo - All rights reserved.

18

www.docebo.com

Role playing

Controller

The organization who determines the purposes and means of the processing of personal data

Processor

The organization who processes personal data on behalf of the controller



Role playing

Controller

The organization who determines the purposes and means of the processing of personal data

Processor

The organization who processes personal data on behalf of the controller



Data Subjects

=

Prospects refers to
Customers refers to
Docebo's employee



**Docebo as
Controller**



**Third parties providers
as Processor**

Purpose of processing by Docebo

- Respond to demo requests
- Send order confirmation
- Respond to customer service requests
- Administer Customer's account
- Send newsletter
- Send marketing communications

(as established in [Docebo's Privacy Policy](#))

Is Docebo LMS GDPR compliant ?

The answer is always YES, Docebo LMS is GDPR compliant but Docebo LMS must be used in a GDPR compliant way and this is borne to Docebo's Customer as Controller

- ❑ Docebo is designed, developed and operated in a GDPR compliant way
- ❑ Docebo LMS provides functionalities to support GDPR compliance
- ❑ Docebo provides services to support customer for GDPR compliance

Does Docebo (as organization) comply with GDPR ?

- YES, Docebo has carried out a rigorous process of adjustment and conformance to the new European regulation, covering the whole organization
- Docebo compliance to GDPR has been verified both for Docebo as a Controller and Docebo as a Processor
- Docebo information security management system ("ISMS") is ISO 27001 certified and the company's information security program includes a full set of controls in accordance with ISO 27001 and AICPA SOC 2 ensuring a full and adequate coverage of GDPR
- Docebo LMS is developed, maintained and operated applying the Security by Design and Security by default principles



What Docebo provides to comply with GDPR

- **LMS functionalities and Docebo support services**
- **Compliance Framework**
 - ISO 27001
 - AICPA SOC 2
 - EU-US and Swiss-US Privacy Shield
- **Data Processing Addendum**



GDPR in practice: Implementing TOMs

Under GDPR
Controllers and Processors
are required to implement appropriate
Technical and Organization Measures (“TOMs”)

(1) Pseudonymisation and encryption of personal data

(2) Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services

(3) Ability to restore availability and access personal data in a timely manner in the event of a physical or technical incident

(4) Process for regularly testing, assessing, and evaluating the effectiveness of TOMs

- Docebo LMS features support customer in providing adequate security to LMS users
- Docebo maintains an information security management system (“ISMS”), which is ISO 27001 certified. Within this framework, Docebo has defined a comprehensive information security program including a full set of controls implemented in accordance with ISO 27001 and AICPA SOC 2.

GDPR in practice: Implementing TOMs

Under GDPR
Controllers and Processors
are required to implement appropriate
Technical and Organization Measures (“TOMs”)



Pseudonymisation and encryption of personal data

- Docebo LMS supports encryption in transit through HTTPS
- Encryption at rest: user content encryption at the storage level is provided as an additional service by leveraging the capability of Amazon S3 to store the file with 256-bit AES.
User metadata encryption is provided by leveraging AWS Key Management Service for the RDS database volume encryption.

Docebo commitment to information security

Docebo commitment to information security and data protection is paramount

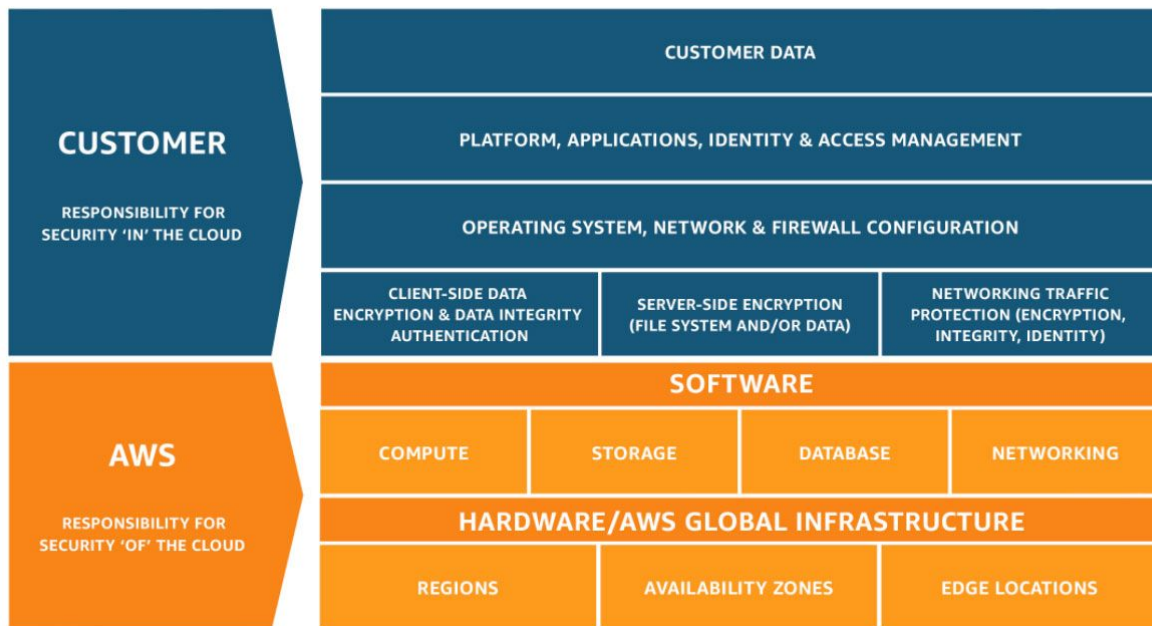
- Docebo maintains an information security management system (“ISMS”), which is ISO 27001 certified.
- Docebo has defined a comprehensive information security program including a full set of controls implemented in accordance with ISO 27001 and AICPA SOC 2, managed by a dedicated security team.
- Appropriate training is provided to employees and subcontractors
- Documented Software Development Life Cycle (SDLC) and Change Management including security by design, accurate testing, vulnerabilities remediation and application of security patches
- Access control mechanisms based on a sophisticated Identity Access Management infrastructure
- Event detection based on a sophisticated Security Information and Event Management (SIEM) platform
- Incident management and response procedure for identifying, acting upon, and reporting failures, incidents and other security concerns, including data breaches



Docebo commitment to information security

Docebo leverages the comprehensive and state-of-the-art security capabilities provided by Amazon Web Services (AWS)

- The respective security responsibilities among Docebo S.p.A and AWS are defined in the AWS Shared Responsibility Model



What Docebo provides to comply with GDPR

- **LMS functionalities and Docebo support services**
- **Compliance Framework**
- **Data Processing Addendum**

CUSTOMIZABLE PRIVACY POLICY NOTIFICATION AND CONSENT OBTAINING

The LMS should enable the Controller to track the version of a site policy and any opt-ins that a user has agreed to.

Users should also be able to visit the site policy pages they have signed up to and amend their agreements

Customized privacy policy notification and acceptance: Customer can publish a customized privacy policy that will be shown translated in the user selected language. The privacy policy must include an acceptance checkbox with a customizable acceptance statement.

Privacy policy differentiated by domain: Customer can publish privacy policy differentiated by domain basis.

Multiple acceptance checkbox: For each privacy policy can be defined multiple acceptance checkbox with a customizable acceptance statement (up to other 3 after the first one included as default) . For each checkbox the superadmin can configure if the acceptance is mandatory.

Consent reporting: The LMS allows to produce reports showing the collected consents relevant to the privacy policy version accepted along with the privacy policy version date.

How GDPR affects LMS

THE RIGHT OF ACCESS

Under GDPR, the right of access means that the Controller must be able to give to an LMS users all of the information hold about them, including training records, performance evaluations, management feedback and appraisal comments

THE RIGHT TO RECTIFICATION

LMS users have the right to have their data rectified within the LMS system. For instance, if a user can prove that they completed a course that is not showing up on the system, this must be updated accurately.

LMS functionalities and Docebo support services

- **LMS user profile management**
- **LMS Activity Report**
- **GCS support**

- **LMS user profile management**
- **GCS support**

How GDPR affects LMS

THE RIGHT TO ERASURE

LMS users have the right to request that all of their data is deleted from the LMS.

Except for request for the erasure of data which is legally required, such as a record of compliance training.

THE RIGHT TO RESTRICTION OF PROCESSING

The Controller may store data, but not further process it.

For instance, an LMS user may contest an assessment score stored in the LMS: in this case, data can be stored in the LMS but not processed further until the data has been either verified or amended

LMS functionalities and Docebo support services

- **LMS user profile management**
- **GCS support**

- **LMS user profile management**
- **IDP Responsibility**
- **GCS support**

How GDPR affects LMS

THE RIGHT TO DATA PORTABILITY

LMS users have the right to request their personal data that is stored in the LMS for reuse them in another system. The Controller must provide this data in a structured, commonly used and machine-readable format, such as a CSV file

THE RIGHT TO OBJECT

Users must be allowed to object to having their personal data used for direct marketing, profiling or for research and statistics. This right must be presented at the point of first communication and in the privacy notice, adding explicit mentions of any other reasons for collecting personal data.

LMS functionalities and Docebo support services

- **LMS user activity profile**
- **LMS user report**
 - **Excel**
 - **CSV**
- **LMS API**
- **GCS support**

- **LMS newsletter feature**
- **LMS notifications**
- **GCS support**

How GDPR affects LMS

THE RIGHT NOT TO BE SUBJECT TO AUTOMATED INDIVIDUAL DECISION-MAKING RESULTING IN DECISIONS HAVING LEGAL OR SIGNIFICANT EFFECTS

here is an extreme example: Let's assume an employee has to keep his compliance training up-to-date as a condition of his employment. If an automated system in the organisation should terminate the employment by detecting a fail to complete a compliance training on time and go overdue. In this case that decision can be challenged and request human intervention in the decision as it has a significant effect on the user. It's highly likely the organisation would be forced to change this process.

What Docebo provides to comply with GDPR

➤ LMS functionalities and Docebo support services

➤ **Compliance Framework**

➤ Data Processing Addendum

Compliance Framework

- ❑ Docebo maintains an information security management system (“ISMS”) ISO 27001 certified.
- ❑ Docebo has defined a comprehensive information security program including a full set of controls implemented in accordance with ISO 27001 and AICPA SOC 2 that provide an adequate coverage of GDPR Article 32, privacy by design and other GDPR requirements.
- ❑ Docebo is compliant to EU-U.S. and Swiss-U.S. Privacy Shield and have got the relevant seal by TRUSTarc.



Standards, Regulations & Certifications

To help you with compliance and reporting, we share information, best practices, and easy access to documentation. Our organization and our platform regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards to earn your trust. We're constantly working to expand our coverage.



Docebo commitment to information security and data protection is paramount

Docebo maintains an information security management system (ISMS) and within this framework, has defined a comprehensive information security program including a full set of controls implemented in accordance with ISO 27001 and AICPA SOC 2 managed by a dedicated security team. Docebo LMS is developed, maintained and operated through a Software Development Life Cycle (SDLC) and a Change Management process including the security by design principle and the highest security and quality standards.

ISO 9001

ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization.

The key to the ongoing certification under this standard is establishing, maintaining and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where Docebo products and services consistently satisfy ISO 9001 quality requirements.

We can provide the following ISO 9001 documentation

- Certificate

[Click here to request the documentation](#)

SOC 2

SOC 2 is a report based on AICPA's existing Trust Services principles and criteria. The purpose of the SOC 2 report is to evaluate an organization's information systems relevant to security, availability, processing integrity, and confidentiality or privacy. Docebo undergoes a regular third-party audit to certify individual products against this standard. Docebo has completed SOC 2 Type 1 audit for The Docebo Learning Management System and is on the process to undergo SOC 2 Type 2 audit.

We can provide you the following SOC documentation:

- Current SOC 2 report (under NDA)

[Click here to request the documentation](#)

ISO 27001

Managing information risks.

The ISO/IEC 27000 family of standards helps organizations keep information assets secure. ISO/IEC 27001 is a security standard that outlines and provides the requirements for an information security management system (ISMS). It specifies a set of best practices and details a list of security controls concerning the management of information risks.

The 27001 framework and checklist of controls allows Docebo to ensure a comprehensive and continually improving model for security management.

We can provide you the following ISO 27001 documentation:

- Certificate
- Statement Of Applicability (under NDA)
- Last third party annual surveillance audit report (under NDA)

[Click here to request the documentation](#)

GDPR and PRIVACY

Many of Docebo LMS Platform's business customers operate in Europe or have European citizens as user of our platform and need to comply with the European Union's General Data Protection Regulation (GDPR). The GDPR specifies a number of requirements companies must meet around protecting personal data.

Docebo is fully compliant with GDPR across Docebo LMS services.

Customer can require to inspect and accept our Data Processing Addendum.

Docebo is certified under both the EU-U.S. and Swiss-U.S. Privacy Shield frameworks and our certifications can be viewed on the Privacy Shield list.

Website Compliance Page

<https://www.docebo.com/compliance-security/>

Docebo's Compliance Framework

- ISO/IEC 27001 provides the requirements for an information security management system (ISMS) and defines a full set of controls that we have implemented
- AICPA SOC 2 ensures that Docebo as a service providers securely manages his customer's data and that the security controls implemented are effective

What Docebo provides to comply with GDPR

- LMS functionalities and Docebo support services
- Compliance Framework
- Data Processing Addendum

Data Processing Addendum

[Article 28 \(3\) of GDPR](#) requires a contract in writing between the Controller and Processor, which clearly sets out the subject matter of the processing and its duration as well as the nature and purposes of processing, the types of personal data, any particular special categories of data and the obligations and rights of both parties.

Docebo complies with these requirement by providing a standard **Data Processing Addendum (DPA)** composed by several documents, that must be signed along with our MSSA:

- ❑ Data Processing Addendum
- ❑ ANNEX A - Information Protection and Security Standard

**Docebo's DPA is fully GDPR compliant,
it has been thoroughly legally verified and
it is aligned to the standard adopted by the major SaaS players.**



Review and compliance adjustment

Progetto adeguamento GDPR con ingaggio di



- **Verifica stato as-is della conformità**
- **Definizione dei gap e delle criticità**
- **Prioritizzazione ed attuazione interventi adeguamento entro 25 maggio**
- **Action plan per ottimizzare gestione compliance**

Main challenges to achieve and manage compliance

Registro dei trattamenti

- Più di 80 trattamenti intra gruppo con circa 50 applicazioni cloud
- Titolarità dei trattamenti e rapporti intra gruppo
- Registro come titolare e come responsabile
- Rappresentazione e gestione del registro

Main challenges to achieve and manage compliance

Notifiche e contrattualistica

- **Revisione privacy policy con mantenimento compliance EU-US privacy shield**
- **Revisione cookie policy**
- **Revisione Data Processing Agreement e MSSA**
- **Procedure e gestione processo firma DPA standard Docebo**
- **Gestione eccezioni e trattativa per DPA non standard e supporto legale**

Main challenges to achieve and manage compliance

Funzionalità LMS e servizi di supporto

- Revisione privacy policy notice feature ed altre feature entro 25/05/2018
- Pianificazione miglioramenti su features LMS anche da feedback clienti
- Pianificazione nuove features LMS anche da feedback clienti
- Revisione procedure Global Customer Success (GCS)
- Formazione GDPR per operatori GCS
- Miglioramento servizi di supporto ed assistenza clienti

Main challenges to achieve and manage compliance

Revisione processi operativi

➤ Marketing & Sales

- Gestione acquisizione consenso
- Marketing database lifecycle process

➤ Human resources

- Revisione procedure e informative impiegati e candidati

➤ Gestione fornitori

- Revisione processo qualifica e firma DPA

Action plan and work in progress

- **Revisione procedure Marketing & Sales**
- **Monitoraggio processi supporto ai Titolari per gestione richieste utenti LMS**
- **Integrazione procedura DPIA in Risk Management attuale e in SDLC**
- **Revisione e monitoraggio Incident Management per gestione data breach**
- **Completamento integrazione del “Modello organizzativo della data protection” in ISO 27001 Information Security Management System (ISMS) esistente**
- **Formazione continua GDPR**
- **Valutazione opportunità nomina DPO**



docebo®

Any questions?

docebo®

Copyright © 2016 Docebo. All rights reserved.

<#>

www.docebo.com