eloomi

IT Security & Infrastructure

Capterra ★★★★☆ eLearning Industry ★★★★☆ G2 CROWD ★★★★☆

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations
INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS
ISAE 3402
GDPR
Information Security Management System
ISO 27001
Certified
IT security best practice for employees
45 min

Table of Contents

Introduction 1

IT Security Policy 2

Audit Reports 3

Best-in-class data integrity 4

Information Security Incident Management 5

24/7 Infrastructure Monitoring & Support 6

Supplier Service Delivery Management 7

Data Storage & Location 8

Network Security 9

Vulnerability Scanning 10

Change Governance 11

Backup Procedures 12

Integrations 13

API Access Package 14

Native Integrations 15

SSO Access Package 16

Support & SLA 17

Ongoing access to live-help & chat 18

Introduction

About this presentation

At eloomi, we know how critical security, privacy and reliability are to both yours and our company. Have peace of mind by knowing that eloomi takes the IT security and compliance needs of our global clients seriously, and we support the security requirements of many industries across the world.

This presentation is made to summarise our commitment and prioritisation of IT Security, infrastructure and compliance. The descriptions are based on eloomi's yearly IT audit by Deloitte in accordance with the International Standard on Assurance Engagements 3000 (ISAE 3000). And the controls are based on selected areas from the ISO 27001 framework.

About eloomi

The eloomi platform simplifies continuous performance development and corporate training. The platform connects the dots between learning and performance to gain greater employee output, engagement and productivity.

The solution is provided to customers and organisations as software-as-a-service (SaaS), using a subscription-based model. Modules are available to each customer depending on license terms and contract.

IT Security Policy

It is essential for eloomi that eloomi's employees know what is expected and required of them when using our technology stack at the job. eloomi must protect ourself and our customers by having policies to govern areas such as personal internet and email usage, security, software, hardware inventory and data retention.

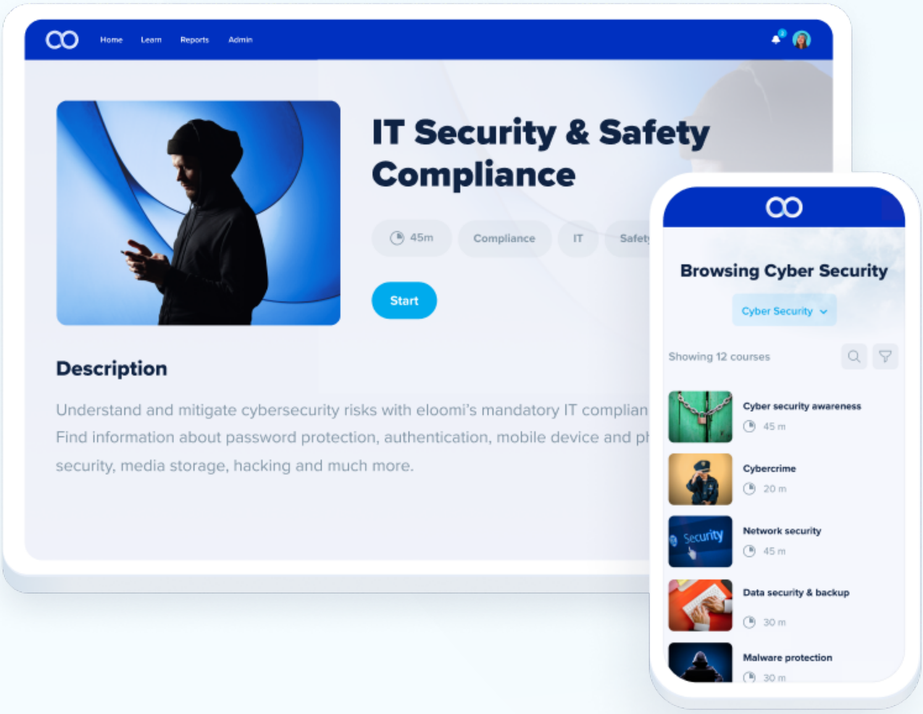
Compliance

eloomi has defined a set of policies for information security which is approved by management and communicated to employees and relevant external parties. The procedures for information security is reviewed at planned intervals or if significant changes occur.

Every employee at eloomi is 100% compliant with the "eloomi IT Security Policy" and bound by confidentiality in the employee contract. The compliance course is renewed once a year, and customers or external auditors can achieve documentation of certifications by contacting eloomi.

The employee compliance program contains:

- IT Security Policy compliance training
- Disaster Recovery
- Standard Operating Procedures document



IT Security & Safety Compliance

Description

Understand and mitigate cybersecurity risks with eloomi's mandatory IT complian Find information about password protection, authentication, mobile device and pl security, media storage, hacking and much more.

Browsing Cyber Security

Showing 12 courses

Cyber security awareness 45 m

Cybercrime 20 m

Network security 45 m

Data security & backup 30 m

Malware protection 30 m

Audit Reports

ISAE 3000

eloomi’s ISAE 3000 audit report cover, Change Governance, IT Security, GDPR, Confidentiality of employees, Access control handling, Use of IT-equipment, System operation, Backup procedures, Malware and encryption, are based on the ISO 27001 framework.

To monitor compliance with Microsoft Azure, we as a partner acquire the audit reports from Microsoft, perform a supplier risk assessments, and review their reports to find any conflict and secure they comply with all the clauses. This monitoring is a part of our internal audit by Deloitte.

We can only share our own internal ISAE 3000 report; however, we confirm, that Microsoft Azure as our supplier of cloud infrastructure, are fully compliant with the mentioned standards and many other standards.

Deloitte.

Independent auditor's report (ISAE 3000) on the description of selected control objectives and related controls and their design and operating effectiveness related to eloomi's application software

Throughout the period from [illegible]

Our internal
compliance report

ISO 27001

Microsoft Azure

Microsoft Azure’s compliance with ISO 27001 standard, is a strong foundation of Information Security principles and contain detailed documentation of IT policy and procedures.

bsi. Microsoft

Assessment Report
ISO/IEC 27001

Microsoft Corporation
Microsoft Azure

ISAE 3402 SOC 1-3 reports

Microsoft Azure

ISAE 3402 SOC2 Security demonstrates that good security practices are in place and operating effectively at Microsoft Azure.

Microsoft

Microsoft Corporation –
Microsoft Azure
[illegible]

Service Organization Controls Report

[illegible]

Best-in-class data integrity

eloomi stores sensitive information about customers, business connections and contacts in compliance with the Personal-data-law and DPA regulations to ensure that information receives an appropriate level of protection in accordance with its nature and importance. All processes with personal data are identified, and responsibilities are defined and communicated.

All employees of eloomi must, every year, examine and pass a compliance test of the eloomi IT-security policy, as well as a compliance test in the management of sensitive data.

- Data storage and 24/7 cloud hosting via ISO certified Microsoft Azure
- Network security and vulnerability scanning
- Backup procedures and incident management
- Audited and Certified ISO 27001 by Deloitte
- eloomi internal employee IT security policy
- Accessibility and integration

GDPR

INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS ISAE 3402

Information Security Management System ISO 27001 Certified

AICPA SOC

Information Security Incident Management

In order to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses, eloomi has established standard operating procedures and responsibilities to ensure a quick, effective and orderly response to information security incidents.

Established standard operating procedures will be used if a data breach occurs. Either if its discovered by internal employee's or reported from outside eloomi. It is eloomi's responsible for IT Security Policy or DPO that immediately will be contacted if a data breach event occurs. A data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Notice to the supervisory authority (Datatilsynet) will be provided no later than 72 hours after having become aware of the breach. If notification is not made within 72 hours, eloomi will provide a ''reasoned justification'' for the delay when notifying of the personal data breach. Notice to affected individuals will be done without undue.

eloomi also documents any personal data breaches, which must at least include information on the facts relating to the personal data breach, the effects of the breach and the efforts and remedial actions taken. The standard operating procedure for data breach and data security is a part of the internal eloomi compliance program, which means that it is covered by 100% compliance and knowledge as soon as a person is employed by eloomi.

24/7 Infrastructure Monitoring & Support

System operation

In order to ensure correct and secure operations of the eloomi application and information processing facilities, eloomi has defined operating procedures.

The “eloomi Runbook” was developed to ensure that the eloomi platform is operating and functional 24/7/365. It contains a set of defined procedures developed by our IT administrators and Infrastructure Team for maintaining the operations of the eloomi application on our Cloud environment.

The Runbook also contains all the information for starting and stopping the system, instructions for disaster recovery, patching, handling alerts, and procedures for how to perform backups and restore.

As a cloud-based solution being accessible is one of our most mission-critical tasks. eloomi’s infrastructure foundation is therefore built on a stable cloud platform at Microsoft Azure. eloomi continues to monitor the use of resources on all of our critical instances and an advanced alarm and notification system is build on the environment to secure that systems and eloomi application are operational 24 hours a day.

Our operating performance is analysed every month via a monthly report that contains usage, uptime, availability, incident and resolutions. Any improvement and actions are handled, documented and initiated via our operational backlog.

Supplier Service Delivery Management

Protection of processed data is essential for information security at eloomi. Therefore we have created a data processing log that contains all information about processing data and third party suppliers.

eloomi stores all information about which business unit in eloomi that are using software, if there is any data processing, which the data processor is being used, who is the responsible, the data protection officer, the purpose of processing, the categories of data, if the data is transferred outside of EU and the duration of retention.

Supplier compliance (Including Microsoft Azure)

To monitor compliance with our suppliers, we identify security measures, and log when we have done a compliance audit review of the supplier, and when the next audit review will be performed.
In practical, this happens by acquired audit reports from the suppliers, perform supplier risk assessments, and review their reports to find any conflict and secure they comply with all the clauses.

Data Storage & Location

The physical storage location of customer data can be of great importance. However, we are used to working in the cloud.

eloomi's main cloud infrastructure is located on Microsoft Azure's servers in US or Northern Europe (Ireland).

Multi tenancy – Separate database per tenant

Each customer has its own set of database tables within its unique database schema, which ensures complete segregation of tenants' data.

Encrypted data storage

All encrypted data is stored on disks using a minimum of AES 256-bit encryption.

Network Security

Access Through Secured Connection (TLS/SSL and HTTPS)

Access to the eloomi application is limited to connecting only through a secure connection to ensure that all the data exchanged between the eloomi servers and the user's PCs is securely encrypted.

Network security

eloomi's servers at Microsoft Azure are protected by a strong firewall layer that works from principle default closed.

This means that we must actively open a port/service for being able to receive traffic from the Internet.

The environment includes, among other things, following layers of security:

- All servers can only be accessed from a bastion host
- The bastion host is closed for access based on IP
- All users must have a personal certificate, matching for access

We have set up tests of the security of the production environment through an automated monthly vulnerability scan.

Vulnerability Scanning

Application vulnerability scanning

Vulnerability scanning and penetration testing at eloomi have the primary purpose of detecting software flaws to determine how well the application is patched. The scanning runs automatically in intervals, and after each scanning, the potential findings are documented, prioritised, and optimisations are initiated. The reports are stored on dedicated database servers out of reach from the web servers.

Malware

To ensure that information and information processing facilities are protected against malware and to prevent exploitation of technical vulnerabilities, eloomi has established controls against malware. Files and servers are automatically scanned for virus, malware or other dangerous content which may harm eloomi or our customers. Each customer directory is scanned individually to find potential threats.

Change Governance

In order to ensure the integrity of the eloomi application and that information security is designed and implemented within the development lifecycle, eloomi has defined a secure development policy and change control procedures that are audited by Deloitte.

To limit access to information, release management, information processing facilities, data and network, eloomi has established an access control policy. It is required that all employees have completed the eloomi IT Security Policy compliance program before access to any system or data will be granted. All-access rights are evaluated periodically, every 6-months, and adjusted if access is necessary. If the employee doesn't exist in the "eloomi ACL" no access has been granted. The ACL does not contain any passwords or private keys of any kind, and all passwords are person-specific and only known by the employee.

Deloitte.

Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR no. 33 96 35 56
Weidekampsgade 6
2300 Copenhagen S

Phone: 36102030
www.deloitte.dk

Independent auditor's report (ISAE 3000) on the description of selected control objectives and related controls and their design and operating effectiveness related to eloomi's application software

Throughout the period from July 1, 2019 to December 31, 2020

Backup Procedures

In order to protect against loss of data, eloomi has back up copies of information and software that are regularly tested according to our backup policy.

The eloomi backup process is handled in our Cloud Files Backup at Microsoft Azure. Backups are automatically taken every day with a retention period for seven days. The backups are done with the “soft delete” functionality of Azure Blob storage. This allows blobs to be restored if they are deleted or overwritten.

In case eloomi backup sets are not running as expected, the system will send out warnings for failed backups. The escalation policy is within business hours only. Once a year, the eloomi team perform a full disaster recovery test with backup data. This is documented in our documentation tool.

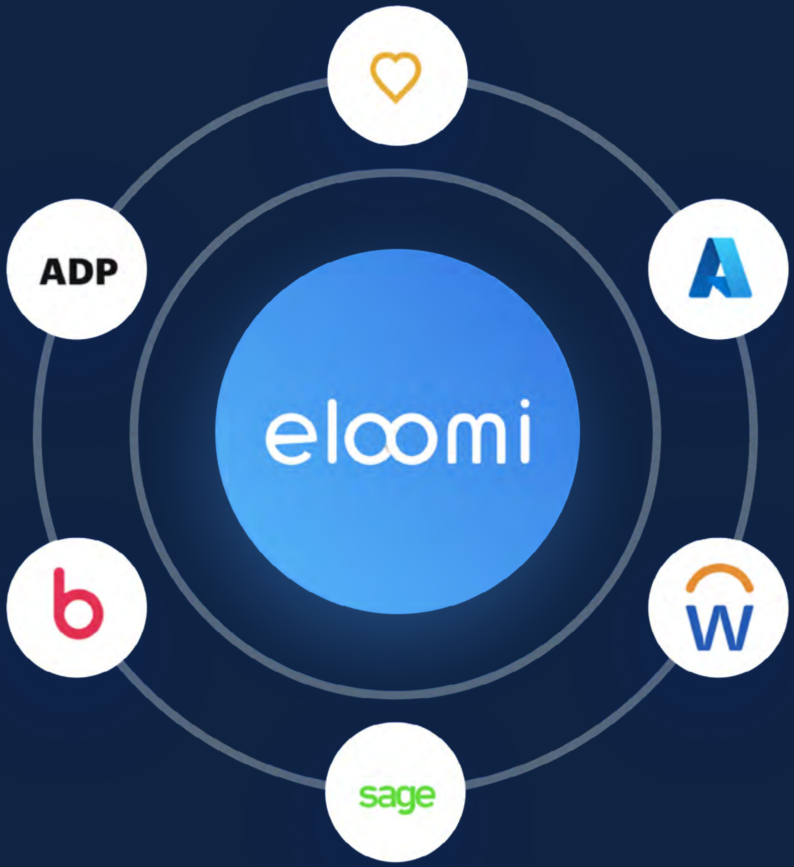
Integrations

Connect your systems with eloomi via eloomi API

eloomi is not a stand-alone solution. You can use our API functionality to integrate your eloomi platform with other IT-systems you have in your organisation or utilize our Native Integration to more than 40 HRIS/ HR system

Automatically syncs user data

- Eliminate the need for time-consuming data entry and mitigate possible human error
- Streamline your HR workflow with maximal flexibility to meet your needs
- Saves HR reps valuable time, allowing them to focus their attention on growing people



Looking for a specific integration? Get in touch!

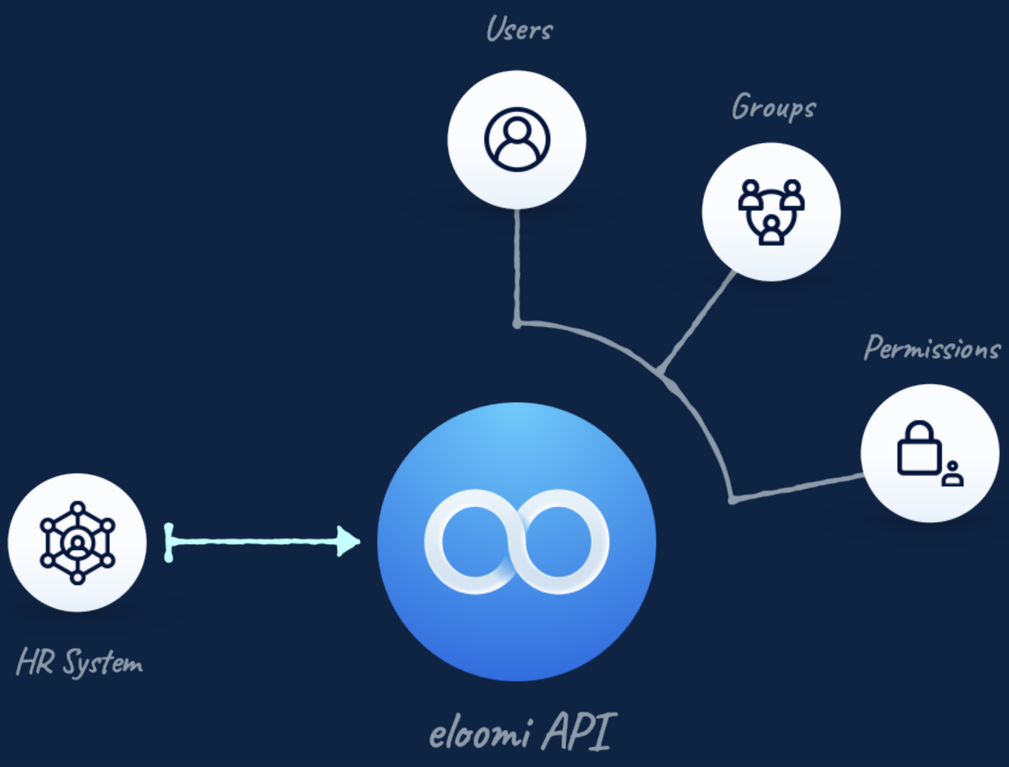
1 API Access Package

At eloomi we use an Open REST API. An API is an Application Programming Interface. Essentially, it's a rulebook for how different computer systems can interact with each other.

We follow standard HTTP methods, in JSON formats, so when data is sent to and from our platform using the eloomi API we keep your systems safe and protected.

Services includes:

- Access to eloomi REST API Infrastructure
- Access to API documentation
- Extra platform for testing incl. client ID and client secret for test
- API client ID and client secret
- Free API support via **helpdesk.eloomi.com** within business hours

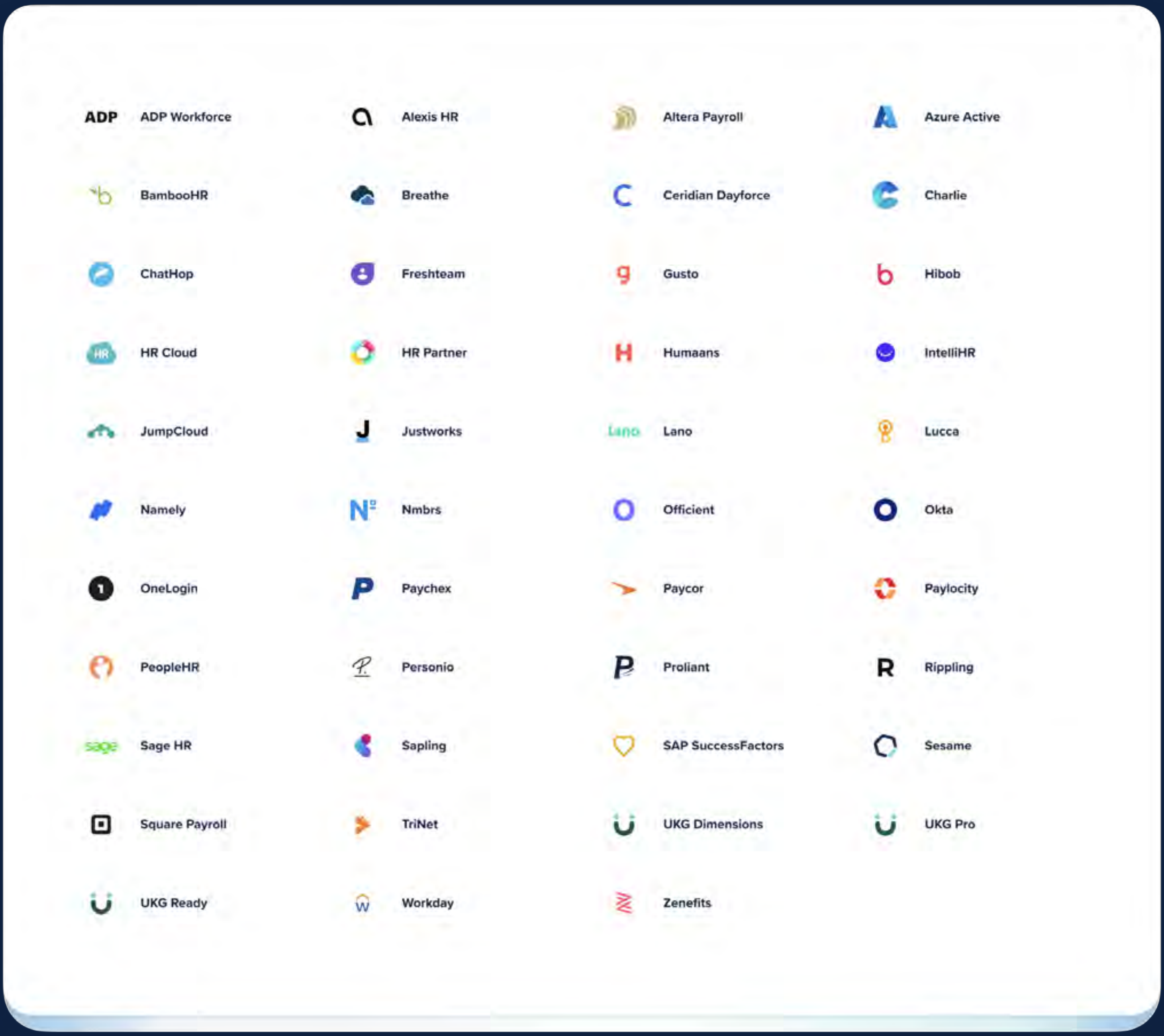


Need for consultancy or meetings?

Any consultancy or meeting hours spent outside of the included services in the API access subscription will be invoiced per commenced hour.

2 Native Integrations

With eloomi Native HR & HCM Integrations your platform stays in sync with the rest of your user management systems.



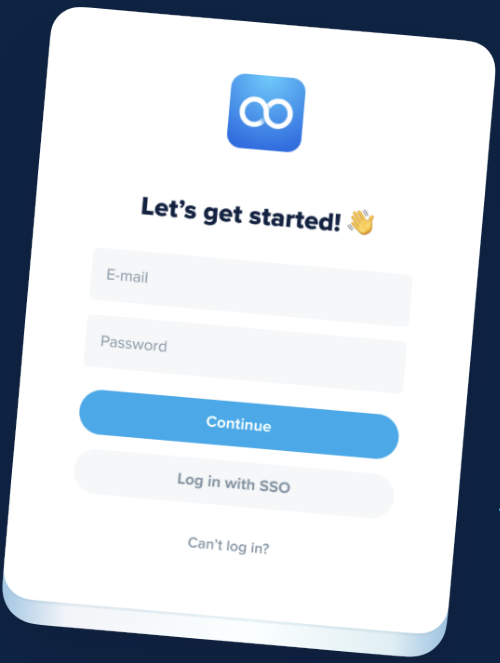
ADP Workforce	Alexis HR	Altera Payroll	Azure Active
BambooHR	Breathe	Ceridian Dayforce	Charlie
ChatHop	Freshteam	Gusto	Hibob
HR Cloud	HR Partner	Humaans	IntelliHR
JumpCloud	Justworks	Lano	Lucca
Namely	Nmbrs	Officient	Okta
OneLogin	Paychex	Paycor	Paylocity
PeopleHR	Personio	Proliant	Rippling
Sage HR	Sapling	SAP SuccessFactors	Sesame
Square Payroll	TriNet	UKG Dimensions	UKG Pro
UKG Ready	Workday	Zenefits	

SSO Access Package

eloomi SSO eliminates the problem of employees having separate logins to applications within your organisation. By using eloomi SSO, you can make sure that users who are already logged-in at application A will also be logged in automatically in eloomi. This is mostly implemented if your organisation works with: Azure AD or AD(FS). We support the SSO protocols, SAML 2.0 and oAuth 2.0.

Services includes:

- Access to SSO Infrastructure (This will be available in Admin/Integrations/SSO)
- Possibility to combine SSO with standard mail/username and password authentication
- Access to SSO documentation
- Free SSO support via **helpdesk.eloomi.com** within business hours



We support SSO through SAML 2.0 and oAuth 2.0 protocols

Need for consultancy or meetings?

Any consultancy or meeting hours spent outside of the included services in the SSO access subscription will be invoiced per commenced hour.

Support & SLA

helpdesk.eloomi.com

Any eloomi online support requests must be submitted via helpdesk.eloomi.com, or via any available “contact support” feature in eloomi. Requests must include a detailed description of the issue. eloomi will then create a support case and ticket with feedback directly to the sender.

Our Help Desk categorisation and SLA is:

Priority Level 1 – Critical

Interruption making a critical functionality inaccessible or a complete infrastructure interruption causing a severe impact on services availability. There is no possible alternative.

Example:	Platforms are down
First response:	15 min
Resolution:	2 hours

Priority Level 2 – High

Core functionality or platform access interrupted, degraded or unusable, having a severe impact on services availability.

No acceptable alternative is possible.

Example:	SCORM not working
First response:	1 hour
Resolution:	2 business days (16h)

Priority Level 3 – High

Non-critical function or procedure, unusable or hard to use having an operational impact, but with no direct impact on services availability. A workaround is available.

Example:	Unable to share Notes
First response:	1 business day (8h)
Resolution:	5 business days (40h)

Priority Level 4 – Low

Non-critical functionality which is only environment specific and a workaround is possible. Note that this will also include Tasks like Custom Domain etc.

Example:	User or module specific issue
First response:	1 business day (8h)
Resolution:	2 weeks (80h)

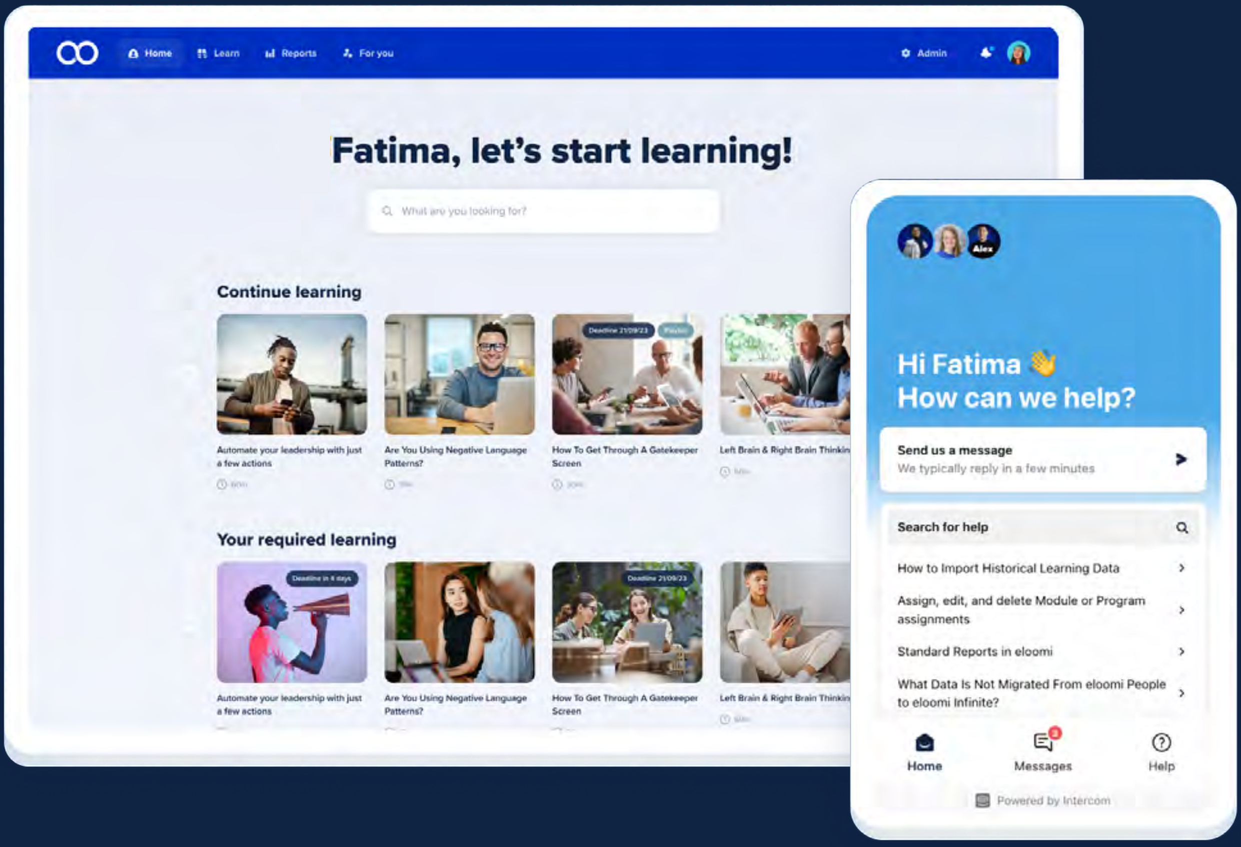
Priority Level 5 – Minimal

Application or personal procedure unusable, where a workaround is available or a repair is possible. Note: Development can be rejected in some instances

Example:	Minor UI/UX issues
First response:	1 business day (8h)
Resolution:	1 month (176h)

Ongoing access to live-help & chat

All users with administrative rights in the system will have access to a live chat tool where eloomi experts are ready to answer all types of product questions. In addition to the live chat, you can also search for videos or text-based tutorials, so that you always have eloomi help at your fingertips. This chat function can be useful for implementation, but also ongoing support and training.



Fatima, let's start learning!

What are you looking for?

Continue learning

Automate your leadership with just a few actions

Are You Using Negative Language Patterns?

Deadline 21/09/23

How To Get Through A Gatekeeper Screen

Left Brain & Right Brain Thinkin

Your required learning

Deadline in 4 days

Automate your leadership with just a few actions

Are You Using Negative Language Patterns?

Deadline 21/09/23

How To Get Through A Gatekeeper Screen

Left Brain & Right Brain Thinkin

Hi Fatima 👋
How can we help?

Send us a message
We typically reply in a few minutes

Search for help

How to Import Historical Learning Data

Assign, edit, and delete Module or Program assignments

Standard Reports in eloomi

What Data Is Not Migrated From eloomi People to eloomi Infinite?

Powered by Intercom