sosafe

INFOSHEET

Compliance is key

How SoSafe helps your organization meet GDPR and ISO requirements

www.sosafe-awareness.com

The highest level of security and compliance

In an increasing cyber threat landscape, many cyber security and privacy regulations have tightened – with increased liability risks for organizations and even individual managers in the case of an incident.

Two of the most important frameworks in cyber security awareness and training are:

EU-GDPR 2016/679

The General Data Protection Regulation (GDPR) requires organizations to adopt appropriate technical and organizational measures to protect the personal data they process. This includes setting up policies, procedures, and processes.

ISO/IEC 27001

The ISO 27001 is an international standard that provides a framework for information security management systems (ISMS). Fulfilling all technical and organizational requirements enables an organization to successfully reduce business risks.

INFOBOX

Contact us and we'll work with you to design and deliver learning experiences for your unique needs, that will help you meet your compliance requirements.

Why should you care?

Compliance and certifications as an important success factor:

Ensure compliance with the law

All organizations processing data within the EU are required to comply with the GDPR and local privacy laws. Additional certifications such as the ISO 27001 are becoming an obligatory unwritten rule for many sectors in order to show compliance.

Mitigate costs

By making sure your organization is compliant with the latest standards, you can better prevent against costly breaches and mitigate liability (and financial) risks in the case of an incident.

Build a business advantage

An increasing number of companies requires their vendors to be ISO 27001-compliant. Certification is an advantage when building new partnerships and business.

Improve your security culture

Use the regulations and frameworks as guidelines that help you protect your data and people, and further improve your security posture.

Be a trusted partner

Use proof of your compliance and certifications to boost your brand reputation and customer trust.

Boost your ISO 27001 compliance with SoSafe

To get ISO 27001-certified, organizations have to implement an information security management system (ISMS) as well as dedicated security measures. Each organization must select a set of measures to be applied to their ISMS which have to be adequate for their business.

One of the most important things in the framework: security awareness. According to the framework, all employees need to receive both continuous training on information security and regular updates on how their organizational policies and procedures impact their individual job function.

What helps you become ISO 27001-certified	What SoSafe offers
Measure and report on organizational awareness and the human risk factor of your ISMS	**Strategic Risk & Reporting Cockpit** Generate and export ISO-compatible reports on simulations and e-learning as proof
Communicate matters related to information security internally	**Awareness Bites** Snackable information security updates regularly sent out to learners via email
Be guided by the Plan Do Check Act (PDCA) Cycle	**Attack Simulations** Phishing simulations in line with the PDCA Cycle: Plan and run campaigns, check their success, and act based on KPIs (e.g., raise the challenge difficulty of simulated emails)
Have an incident response process in place	**Phishing Report Button** Add-on for your email program that enables users to report suspicious email and send to the proper contact within your organization with all the necessary information
Make sure all employees are trained in cyber security	**Learning reminders** Regular reminder emails that encourage learners to complete the courses and boost engagement
Make sure employees are aware of your organization's information security policies	**Policy Upload** Enables you to upload and track acceptance of policies within our e-learning platform

Stay GDPR-compliant with SoSafe

The GDPR Art. 39 (1b) requires company's data protection officers to train employees in all relevant data processing activities. This includes how to process personal data correctly and how to act in case of an incident, for example.

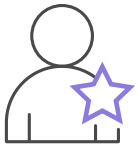
Enable your employees to better understand GDPR through these learning topics:

- What constitutes personal data
- What is personal data, how to handle it correctly and differentiate between direct and indirect association
- What are the essentials of the EU-GDPR
- What the EU-GDPR covers, as well as which rights of deletion, processing and correction of the data you have
- What are the typical privacy and security incidents
- What are data subject requests, how to inform the data protection officer about them, and how to comply with the response period
- How to report data privacy and security incidents within the organization and what are the biggest threats
- Confidentiality levels of information
- How to properly handle information and different levels of confidentiality
- Responding correctly to data subjects' requests

We only process data within the EU where all our legal entities reside. Compliance with the EU General Data Protection Regulation 2016/679 and processing data securely is essential to us – always. Wherever possible, we pseudonymize and encrypt personal data

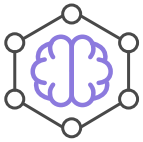
Why SoSafe

Choosing SoSafe as your security awareness provider lets you rest easy knowing your privacy is in good hands.



The training is developed in collaboration with our in-house legal experts, external professionals, and our customers to make sure all aspects are covered.

All employees who complete the training receive a certificate to let you easily prove your organization is in compliance with GDPR training obligations.



The modules convey relevant information on data privacy and help to foster secure behavior with contextual and actionable learning experiences for your employees.

We enable you to export stakeholder dashboards for compliance tracking, which you can use to demonstrate that your employees received appropriate training.