



INFOSHEET

Compliance is cruciaal

Hoe SoSafe jouw organisatie helpt
de regels van de AVG en ISO na te leven

www.sosafe-awareness.com



AVG
COMPLIANT

De striktste normen voor security en compliance

Omdat er steeds meer cyberdreigingen zijn, zijn veel regels voor cybersecurity en privacy strikter geworden, met meer aansprakelijkheid bij incidenten voor organisaties en zelfs managers.

Twee van de belangrijkste kaders bij cyber security awareness en training zijn:



EU-AVG 2016/679

Bedrijven en overheden die persoonsgegevens gebruiken moeten deze volgens de **Algemene verordening gegevensbescherming (AVG)** beveiligen. Volgens de AVG moeten bedrijven en overheden hiervoor passende technische en organisatorische maatregelen nemen.



ISO/IEC 27001

ISO 27001 is de internationale standaard voor informatiebeveiliging. In deze standaard staat beschreven hoe je procesmatig om kunt gaan met het beveiligen van informatie. Ook stelt de standaard eisen voor het vaststellen, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd managementsysteem.

KLEINE INFOBOX

Neem contact met ons op zodat we jou kunnen helpen met het samenstellen van een leerervaring afgestemd op jouw specifieke wensen, die jouw organisatie helpt om compliant te worden.

Waarom is dit voor jou belangrijk?

Compliance en certificatie dragen bij aan jouw succes



- **Loop in lijn met de wet:**
Alle organisaties die in de EU data verwerken, moeten de AVG en plaatselijke privacy-wetgeving naleven. Andere certificaten, zoals ISO 27001, zijn in veel sectoren een ongeschreven regel om compliance aan te tonen.
- **Beperk kosten:**
Als jouw organisatie de meest recente richtlijnen volgt, voorkom je dure overtredingen en kun je, in het geval van een incident, de aansprakelijkheid (inclusief de bijbehorende kosten) tot een minimum beperken.
- **Creëer een concurrentievoordeel:**
Steeds meer bedrijven willen dat hun leveranciers ISO 27001 naleven. Certificatie is een voordeel als je met nieuwe klanten wilt samenwerken.
- **Versterk jouw securitycultuur:**
Gebruik de voorschriften en kaders als richtlijnen waarmee je data en medewerkers beter kunt beschermen en jouw securityaanpak kunt verbeteren.
- **Wees een betrouwbare partner:**
Gebruik het bewijs van compliance en certificatie om de reputatie van jouw merk en het vertrouwen van klanten een boost te geven.

Regel jouw ISO 27001 met SoSafe

Om ISO 27001-gecertificeerd te worden, moeten organisaties een ISMS (Information Security Management System) implementeren en speciale securitymaatregelen treffen. Elke organisatie kiest maatregelen die op het ISMS worden toegepast en die toereikend voor het bedrijf zijn.

Een van de belangrijkste onderdelen van ISO 27001? Security awareness. Volgens de richtlijnen moeten alle medewerkers doorlopend worden getraind in informatiesecurity en regelmatig op de hoogte worden gehouden van hoe het beleid en de procedures van de organisatie hun functie beïnvloeden.

Wat heb je nodig voor ISO 27001-certificatie	Het aanbod van SoSafe
Meet en rapporteer de awareness binnen de organisatie en de humanriskfactor van jouw ISMS	Risk Cockpit en analyses Genereer en exporteer ISO-compatibele rapporten over simulaties en e-learning als bewijs
Communiceer intern over informatiesecurity	Awareness bites Beknopte informatie over security wordt regelmatig per e-mail verzonden
De PDCA-cyclus (Plan Do Check Act) als leidraad	Aanvalsimulaties Phishingsimulaties op basis van de PDCA-cyclus: Campagnes plannen en uitvoeren, het succes meten en actie ondernemen op basis van KPI's (bijv. de simulaties steeds wat moeilijker maken)
Beschik over een incident-response-proces	Phishing Report Button Een knop voor jouw e-mailprogramma waarmee gebruikers verdachte e-mails kunnen doorgeven en automatisch kunnen doorsturen naar de juiste persoon binnen jouw organisatie
Alle medewerkers moeten getraind zijn in cybersecurity	Trainingsherinneringen Regelmatige berichten waarin medewerkers worden aangemoedigd de lessen te voltooien en waarmee de betrokkenheid wordt vergroot
Alle medewerkers moeten het informatiesecuritybeleid van de organisatie kennen	Policyupload Via ons e-learningplatform kun je policies uploaden en bijhouden wie deze gelezen heeft

Blijf AVG-compliant met SoSafe

Artikel 39 (1b) uit de AVG verplicht de Data Protection Officers van een bedrijf om medewerkers te trainen in alle relevante activiteiten voor dataverwerking. Ze moeten bijvoorbeeld leren hoe ze persoonsgegevens juist verwerken en wat ze moeten doen in het geval van een incident.

Stel jouw medewerkers in staat de AVG beter te begrijpen via deze trainingsmodules:

Wat zijn persoonsgegevens?

Wat zijn persoonsgegevens, hoe ga je hier op de juiste wijze mee om en wat is het verschil tussen directe en indirecte identificatie?

Wat zijn de belangrijkste onderdelen van de AVG?

Wat wordt er door de AVG behandeld? En welke rechten op vergetelheid, verwerking en correctie van gegevens zijn er?

Wat zijn veelvoorkomende privacy- en security-incidenten?

Wat is een inzageverzoek van een betrokkene, hoe informeer je de Data Protection Officer hierover op de juiste manier en hoe leef je de reactietermijn na?

Hoe rapporteer je incidenten op het gebied van dataprivacy en -security binnen de organisatie en wat zijn de grootste bedreigingen?

Niveaus van vertrouwelijkheid van informatie

Hoe ga je op de juiste manier met informatie en de verschillende niveaus van vertrouwelijkheid om?

Op de juiste manier reageren op inzageverzoeken van betrokkene

Waarom SoSafe?

Als je kiest voor SoSafe als provider van security awareness, weet je zeker dat jouw privacy in goede handen is.



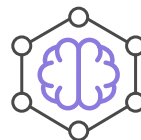
We verwerken gegevens alleen binnen de EU waar al onze wettelijke entiteiten gevestigd zijn. Naleving van voorschrift 2016/679 uit de Europese algemene verordening gegevensbescherming en een veilige verwerking van gegevens zijn altijd essentieel voor ons. We anonimiseren en versleutelen persoonsgegevens als dat mogelijk is.



De training is ontwikkeld samen met onze interne juridische experts op het gebied van privacy, externe experts en onze klanten om te zorgen dat alle belangrijke onderwerpen behandeld worden.



Alle medewerkers die de training afronden, krijgen een certificaat. Hiermee kun je gemakkelijk laten zien dat de organisatie de trainingsverplichtingen van de AVG nakomt.



De modules bevatten relevante informatie over dataprivacy. Ze werken veilig gedrag in de hand via contextuele, praktische lessen voor jouw medewerkers.



Ons platform stelt je in staat stakeholder dashboards te exporteren om compliance bij te houden. Gebruik deze rapportage om aan te tonen dat jouw personeel passende security awareness training heeft doorlopen.