



Onemeeting.com

Beveiligingsmaatregelen en ISO27001

Wij van Onemeeting.com zijn officieel **ISO 27001 gecertificeerd**. Een geslaagde audit door Kiwa heeft aangetoond dat wij voldoen aan alle punten van de norm voor informatie-beveiligingseisen. Wij hebben geïnvesteerd in deze informatiebeveiliging zodat wij voor klanten, locaties en partners een betrouwbare en veilig partner zijn. Alle informatiebeveiliging is van toepassing op de primaire en ondersteunende processen van boeking tot betaling.

Wat is ISO27001?

De ISO 27001-norm legt de eisen vast voor het opzetten, implementeren, onderhouden en continu verbeteren van een **Information Security Management System (ISMS)**. Een ISMS is een raamwerk van processen en procedures die zijn ontworpen om informatie binnen een organisatie te beschermen tegen diverse bedreigingen, zoals ongeautoriseerde toegang, datalekken, en andere vormen van cybercriminaliteit.

Welke beveiligingsmaatregelen neemt Onemeeting.com?

AVG

AVG staat voor Algemene Verordening Gegevensbescherming en is een wetgeving in de Europese Unie die de privacy van individuen beschermt en regelt hoe organisaties persoonlijke gegevens mogen verzamelen, opslaan, verwerken en delen. Onemeeting.com, als een toonaangevend platform voor het boeken van vergader- en evenementenlocaties, erkent het belang van gegevensbescherming en voldoet volledig aan de AVG om de privacy van haar klanten te waarborgen. Onemeeting.com heeft een grondige aanpak ontwikkeld om te voldoen aan deze wetgeving en tegelijkertijd een hoog niveau van dienstverlening te behouden.

Onemeeting.com gebruikt alleen voor het verwerken van gegevens zakelijke klantgegevens zoals naam, e-mailadressen en bedrijfsgegevens. Onemeeting.com gebruikt geen privé gegevens van zakelijke klanten.

Data opslag

Onemeeting.com hanteert een professionele aanpak als het gaat om dataopslag, wij nemen dataopslag zeer serieus en hebben zorgvuldige maatregelen genomen om ervoor te zorgen dat de opslag van gegevens veilig, betrouwbaar en in overeenstemming met de geldende wet- en regelgeving gebeurt.

Onemeeting.com heeft een private cloud omgeving die uitsluitend in Nederland gehost wordt.

Encryptie

Onemeeting.com maakt gebruik van versleutelingstechnologie om gevoelige gegevens te beschermen tijdens zowel de opslag als het transport. Dit betekent dat zelfs als er ongeautoriseerde toegang zou plaatsvinden, de gegevens onleesbaar blijven zonder de juiste decoderingssleutels

Back-ups



Onemeeting.com

Onemeeting.com maakt meerdere back-ups van de opgeslagen gegevens om ervoor te zorgen dat er geen verlies van informatie optreedt in het geval van onvoorziene omstandigheden, zoals technische storingen of datacorruptie. Deze back-ups worden ook op een veilige manier bewaard, met passende beveiligingsmaatregelen.

Operationeel

Best practices staat voor de maatregelen die genomen worden om gegevens beschermt te houden en te waarborgen, zoals het implementeren van een sterk wachtwoordbeleid en het gebruik maken van encryptie, regelmatige updates en patches, bewustwordingstraining voor medewerkers, enz.

Onemeeting.com medewerkers worden regelmatig getraind middels E-learning om zich bewust te blijven van de gevaren.

Interne borging

Onemeeting.com identificeert informatiebeveiligingsrisico's, het beoordelen van hun impact en waarschijnlijkheid, en het implementeren van passende maatregelen om deze risico's te beheren.

Onemeeting.com heeft een continue verbetering. Het evalueren en verbeteren van het ISMS door regelmatige interne audits, managementreviews en correctieve acties uit te voeren.

Onemeeting.com is continu bezig hun medewerker te trainen en op de hoogte te houden van bestaande en nieuwe gevaren. Hoofdgebruikers hebben een VOG verklaring om integriteit en vertrouwelijkheid te kunnen waarborgen.

CONNECTING
THE MEETING
BUSINESS