

Opleiding : Bescherming van persoonsgegevens: goede praktijken in het dagelijks leven

Synthese cursus - 3.30 uur - Ref. 9DP
Prijs : 350 € V.B.

Artikel 32 van de General Data Protection Regulation (GDPR) verplicht bedrijven om defensieve beveiligingsmaatregelen te implementeren. Ontdek wat er op het spel staat en welke best practices dagelijks moeten worden toegepast.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- ✓ Inzicht in digitale identiteit en de bijbehorende risico's
- ✓ Weet wat de beste werkwijzen zijn om uw gegevens dagelijks te beschermen, in uw persoonlijke en professionele leven
- ✓ Weten wat u moet doen in het geval van een datalek

Doelgroep

Iedereen die de uitdagingen van de bescherming van persoonsgegevens wil begrijpen.

Voorafgaande vereisten

Geen speciale kennis vereist.

Praktische modaliteiten

Leer methodes

Conferentie met tijd voor discussie met de deelnemers.

Opleidingsprogramma

DEELNEMERS

Iedereen die de uitdagingen van de bescherming van persoonsgegevens wil begrijpen.

VOORAFGAANDE VEREISTEN

Geen speciale kennis vereist.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vak kennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

1 De context begrijpen

- Wat is een digitale identiteit?
- Waarom de RGPD?
- Herinnering aan de rol van de CNIL.
- Wat definieert de CNIL als persoonlijke gegevens en gevoelige gegevens?

2 Goede dagelijkse praktijk

- Cyberbeveiligingsrisico: kwetsbaarheden/bedreigingen/gevolgen. Social engineering.
- Een phishing/vishing-aanval herkennen waarbij om persoonlijke gegevens wordt gevraagd.
- Wachtwoordbeheer.
- Je digitale identiteit bewaken.
- Andere aanbevelingen in het professionele leven: gegevens bewaren, partitioneren, enz.

3 Wat moet ik doen in geval van een datalek?

- Mijn digitale identiteit is uitgelekt of aangevallen: dien een klacht in, meld het bij de CNIL...
- Mijn bedrijf is het slachtoffer van een datalek: de eerste stappen.
- Cybercrisisbeheer (crisiseenheid, communicatieplan).
- Wat zegt de wet?

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

- De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
- Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
- Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.