EXIN Privacy & Data Protection

FOUNDATION

Certified by EXIN

Voorbeeldexamen

Editie 201803

Inhoud

Introductie

Dit is het voorbeeldexamen EXIN Privacy & Data Protection Foundation (PDPF.NL). Op dit voorbeeldexamen is het Reglement voor de Examens van EXIN van toepassing.

Dit voorbeeldexamen bestaat uit 40 meerkeuzevragen. Elke vraag heeft een aantal antwoorden waarvan één correct is.

Het maximaal aantal te behalen punten is 40. Elke goed beantwoorde vraag levert u 1 punt op. Bij 26 punten of meer bent u geslaagd.

De beschikbare tijd is 60 minuten.

Veel succes!

Voorbeeldexamen

1 / 40
Het illegaal verzamelen, opslaan, wijzigen, bekendmaken of verspreiden van persoonsgegevens is strafbaar onder Europees recht.

Wat voor soort strafbaar feit is dit?

A) een inhoudsgerelateerd delict
B) een economisch delict
C) een inbreuk op het intellectuele eigendomsrecht
D) een privacydelict

2 / 40
Wat is het verband tussen privacy en gegevensbescherming?

A) Gegevensbescherming is een onderdeel van privacy.
B) Privacy is een onderdeel van gegevensbescherming.
C) Dat is hetzelfde.
D) Privacy is niet mogelijk zonder gegevensbescherming.

3 / 40
Waar is de AVG **voornamelijk** voor bedoeld?

A) Om als gemeenschappelijke basis te dienen voor door de lidstaten zelf te ontwerpen wetten
B) Om niet-EU-landen te dwingen het recht op privacy van personen binnen de EU te respecteren
C) Om privacy als fundamenteel mensenrecht voor iedereen te waarborgen
D) Om gegevensbescherming voor individuen binnen de EU te verbeteren en gelijk te maken (te harmoniseren)

4 / 40
De AVG heeft te maken met de bescherming van persoonsgegevens.

Wat is de definitie van persoonsgegevens?

A) Alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon
B) Alle informatie die de Europese burgers willen beschermen
C) Gegevens waaruit direct of indirect iemands ras of etnische achtergrond, religieuze overtuigingen, gezondheidsinformatie of seksuele gewoonten blijken
D) Behoud van vertrouwelijkheid, integriteit en beschikbaarheid van informatie

5 / 40
Welke categorie persoonsgegevens wordt in de AVG beschouwd als gevoelige gegevens?

A) Creditcardgegevens
B) Lidmaatschap van een vakbond
C) Paspoortnummer
D) Burgerservicenummer

6 / 40
Wat is volgens de AVG de definitie van 'verwerking' van persoonsgegevens?

A) Iedere bewerking die op persoonsgegevens kan worden uitgevoerd
B) Iedere bewerking die op persoonsgegevens kan worden uitgevoerd, behalve wissen en vernietigen
C) Alleen handelingen waarbij de gegevens worden gedeeld op sociale media of per e-mail of op andere wijze via internet worden verstuurd
D) Alleen bewerkingen waarbij de persoonsgegevens worden gebruikt voor de doeleinden waarvoor ze zijn verzameld

7 / 40
"*Een onafhankelijke overheidsinstantie die door een lidstaat is opgericht krachtens artikel 51.*"

Van welke rol in de gegevensbescherming is dit de definitie?

A) Verwerkingsverantwoordelijke
B) Verwerker
C) Toezichthoudende autoriteit
D) Derde partij

8 / 40
Geïnformeerde toestemming' is onder de AVG een rechtmatige basis om persoonsgegevens te verwerken. Het doel van de verwerking waarvoor toestemming wordt gegeven moet worden gedocumenteerd.

Op welk moment in het proces moet de toestemming van de betrokkene worden verkregen?

A) Nadat de toelichting over het doel is gepresenteerd en voordat persoonsgegevens worden verzameld
B) Voordat de specificatie van het doel is bedacht en gepresenteerd
C) Voordat de persoonsgegevens verwerkt worden
D) Voordat de persoonsgegevens worden gepubliceerd of verspreid

9 / 40
De AVG is gebaseerd op de beginselen van proportionaliteit en subsidiariteit.

Wat betekent ‘proportionaliteit' in deze context?

A) Persoonsgegevens mogen alleen in overeenstemming met het gespecificeerde doel worden verwerkt.
B) Persoonsgegevens mogen niet worden hergebruikt zonder expliciete en geïnformeerde toestemming.
C) Persoonsgegevens mogen alleen worden verwerkt als er geen andere manier is om de doeleinden te bereiken.
D) Persoonsgegevens moeten toereikend en relevant zijn en niet overmatig ten opzichte van de doeleinden.

10 / 40
De verwerking van persoonsgegevens moet voldoen aan bepaalde kwaliteitseisen.

Wat is een van deze kwaliteitseisen die in de AVG is gedefinieerd?

A) De verwerkte gegevens moeten worden gearchiveerd.
B) De verwerkte gegevens moeten worden versleuteld.
C) De verwerkte gegevens moeten worden geïndexeerd.
D) De verwerkte gegevens moeten relevant zijn.

11 / 40
Iedere keer dat persoonsgegevens worden verwerkt moeten proportionaliteit en subsidiariteit worden gecontroleerd.

Welk vereiste geldt er voor de persoonsgegevens die worden verwerkt?

A) Ze moeten altijd beperkt blijven tot de informatie die nodig is om de gespecificeerde doelen te bereiken en tot de minst 'indringende’ gegevens.
B) Ze moeten door zo min mogelijk werknemers worden verwerkt en deze werknemers moeten voor de verwerkingsverantwoordelijke of een filiaal werken.
C) De verwerking moet beperkt worden tot een vooraf gedefinieerd opslagformaat en het systeem dat gebruikt wordt moet door de verwerkingsverantwoordelijke worden gefinancierd.
D) Ze moeten voor zo min mogelijk doeleinden worden gebruikt en dit gebruik mag niet buiten het pand van de verwerker plaatsvinden.

12 / 40
"*De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te zorgen dat (...) alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor ieder specifiek doel van de verwerking.*"

Van welke term in de AVG is dit de definitie?

A) Naleving
B) Gegevensbescherming door standaardinstellingen
C) Privacy door ontwerp
D) Ingebouwde bescherming

13 / 40
Welke term wordt in de AVG gebruikt voor ongeoorloofde verstrekking van, of toegang tot persoonsgegevens?

A) Verlies van vertrouwelijkheid
B) Inbreuk in verband met persoonsgegevens
C) Incident
D) Inbreuk op de beveiliging

14 / 40
Er is vastgesteld dat er een inbreuk in verband met gevoelige persoonsgegevens is opgetreden.

Aan wie moet dit uiteindelijk worden gerapporteerd volgens de AVG?

A) de toezichthoudende autoriteit
B) de functionaris voor gegevensbescherming (FG)
C) de manager van de afdeling
D) de politie

15 / 40
Tijdens het uitvoeren van een back-up gaat een harde schijf van een dataserver stuk. Zowel de gegevens als de back-up gaan verloren. De harde schijf bevatte persoonsgegevens, maar geen gevoelige gegevens.

Wat voor type incident is dit?

A) Inbreuk in verband met persoonsgegevens
B) Inbreuk op de beveiliging
C) Incident

16 / 40
Iemand die voor een vakbond werkt heeft een concept-nieuwsbrief voor de leden mee naar huis genomen, om hem daar af kunnen maken. Hij is de USB-stick met het concept en de mailinglijst verloren.

Aan wie moet deze inbreuk in verband met persoonsgegevens in ieder geval worden gerapporteerd?

A) Alle leden op de mailinglijst
B) Het personeel van de vakbond
C) De politie

17 / 40
Een organisatie voor sociale voorzieningen is van plan een nieuwe database te ontwerpen waarin staat wie hun klanten zijn en welke zorg zij nodig hebben.

Wat is een van de eerste belangrijke stappen die genomen moet worden om goedkeuring van de toezichthoudende autoriteit te krijgen?

A) Informatie verzamelen over de klanten en het type en de hoeveelheid zorg die ze nodig hebben en krijgen
B) Een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren om de risico's van de beoogde verwerking te beoordelen
C) Toestemming van de klanten verkrijgen voor de beoogde verwerking van hun persoonsgegevens

18 / 40
In welk geval moeten de betrokkenen altijd op de hoogte worden gesteld van een inbreuk in verband met persoonsgegevens?

A) Als de persoonsgegevens zijn verwerkt bij een faciliteit van de verwerker die niet binnen de grenzen van de EU gelegen is.
B) Als de persoonsgegevens zijn verwerkt door een partij die wel heeft ingestemd met het contract dat de verwerkingsverantwoordelijke stuurde, maar het nog niet heeft getekend.
C) Als het systeem waarop de persoonsgegevens verwerkt zijn, is aangevallen en daarbij de opslagapparaten beschadigd zijn.
D) Als er een reële kans is dat de inbreuk nadelige gevolgen zal hebben voor de privacy van de betrokkenen.

19 / 40
Een Nederlandse verwerkingsverantwoordelijke heeft de verwerking van gevoelige persoonsgegevens uitbesteed aan een verwerker in een Noord-Afrikaans land, zonder hierover de toezichthoudende autoriteit te raadplegen. Dit is ontdekt en hij is gestraft door de toezichthoudende autoriteit. Zes maanden later stelt de autoriteit vast dat de verwerkingsverantwoordelijke zich weer schuldig heeft gemaakt aan dezelfde overtreding bij een andere verwerking.

Wat is de maximale geldboete die de toezichthoudende autoriteit in dit geval kan opleggen?

A) € 750.000
B) €1.230.000
C) € 10.000.000, of 2% van de wereldwijde omzet van het bedrijf, indien dit cijfer hoger is.
D) € 20.000.000, of 4% van de wereldwijde omzet van het bedrijf, indien dit cijfer hoger is.

20 / 40
Toezichthoudende autoriteiten krijgen een aantal verantwoordelijkheden toegewezen om ervoor te zorgen dat regelgeving over gegevensbescherming wordt nageleefd.

Wat is een van deze verantwoordelijkheden?

A) Beoordelen van gedragscodes voor specifieke sectoren over de verwerking van persoonsgegevens
B) Definiëren van een minimumpakket van maatregelen die moeten worden genomen om persoonsgegevens te beschermen
C) Onderzoeken van alle inbreuken in verband met persoonsgegevens waarvan ze op de hoogte zijn gesteld
D) Contracten en bindende bedrijfsvoorschriften controleren op conformiteit met de regelgeving

21 / 40
Een religieuze organisatie wil persoonsgegevens delen met hun religieuze autoriteit in een niet-Europees land om te voldoen aan een wettelijk verzoek van de betreffende regering.

Welke bepaling uit de AVG is in dit geval van toepassing?

A) Bij wijze van uitzondering is de verwerking van gevoelige gegevens waaruit religieuze overtuigingen blijken toegestaan aan religieuze organisaties.
B) Het is niet geoorloofd om persoonsgegevens buiten de EER te brengen naar aanleiding van een wettelijk vereiste van een derde land.
C) Verwerking is rechtmatig mits specifieke en ondubbelzinnige toestemming van de betrokkene is verkregen.
D) Persoonsgegevens buiten de EER verwerken is toegestaan op basis van modelcontractclausules die door de Europese Commissie ontworpen zijn.

22 / 40
Op 12 juli 2016 heeft de Europese Commissie een uitspraak uitgevoerd met betrekking tot de doorgifte van persoonsgegevens aan of door de V.S. (EU-VS-privacyschild).

Wat voor uitspraak is dit in termen van de AVG?

A) Een adequaatheidsbesluit
B) Een vrijstellingsbesluit
C) Een standaard bindend contract
D) Een verdrag dat voorrang heeft op de AVG

23 / 40
Bindende bedrijfsvoorschriften zijn een manier waarop organisaties hun administratieve lasten om te voldoen aan de AVG kunnen verminderen.

Waarom zijn deze regels nuttig voor hen?

A) Ze stellen hen in staat om underpinning contracts (externe onderliggende contracten) met alle betrokken partijen in het buitenland af te sluiten.
B) Ze staan hen toe derden buiten de Europese Economische Ruimte persoonsgegevens te laten verwerken.
C) Ze voorkomen dat organisaties iedere toezichthoudende autoriteit in de EU apart moet benaderen.
D) Wanneer de bindende bedrijfsvoorschriften zijn geaccepteerd voorkomen deze dat ze een toezichthoudende autoriteit om toestemming moeten vragen om de gegevens te verwerken.

24 / 40
Als een contractant verwerking van persoonsgegevens uitbesteedt, gaan de partijen een schriftelijke overeenkomst aan. In deze overeenkomst zijn het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het type persoonsgegevens en de categorieën van betrokkenen gedefinieerd.

Welk ander aspect moet door dit schriftelijke contract worden geregeld?

A) de aansprakelijkheid van de verwerker
B) de meldplicht inbreuk persoonsgegevens
C) de verplichting voor verwerkers om medewerking te verlenen aan de toezichthoudende autoriteit
D) de verplichtingen en rechten van de verwerkingsverantwoordelijke

25 / 40
Wat moet er worden gedaan om te zorgen dat een verwerkingsverantwoordelijke de verwerking van persoonsgegevens kan uitbesteden aan een verwerker?

A) De verwerkingsverantwoordelijke moet de toezichthoudende autoriteit om toestemming vragen om de gegevensverwerking uit te besteden.
B) De verwerkingsverantwoordelijke moet de toezichthoudende autoriteit vragen of het overeengekomen schriftelijke contract aan de regelgeving voldoet.
C) De verwerkingsverantwoordelijke en de verwerker moeten een schriftelijke overeenkomst opstellen en ondertekenen waarin ze de vertrouwelijkheid van de gegevens garanderen.
D) De verwerker moet de verwerkingsverantwoordelijke laten zien dat aan alle vereisten die zijn overeengekomen in de dienstenniveau-overeenkomst (ofwel SLA) wordt voldaan.

26 / 40
Gegevensbescherming door ontwerp, zoals beschreven in artikel 25 van de AVG, is gebaseerd op zeven principes. Een hiervan wordt meestal *'Functionaliteit - positive sum in plaats van zero sum'* genoemd.

Wat is de kern van dit principe?

A) Toegepaste beveiligingsnormen moeten vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens waarborgen gedurende de volledige levenscyclus.
B) Als verschillende soorten legitieme doelstellingen tegenstrijdig zijn dan moeten de privacydoelstellingen prioriteit krijgen boven andere beveiligingsdoelstellingen.
C) Wanneer privacy in een bepaalde technologie, proces of systeem wordt gebouwd, moet dit zo worden gedaan dat de volledige functionaliteit niet nadelig wordt beïnvloed.
D) Wanneer dat mogelijk is moeten er altijd gedetailleerde evaluaties van de privacy-effecten en risico's worden uitgevoerd en gepubliceerd, waarbij de privacyrisico's duidelijk worden gedocumenteerd.

27 / 40
Personeel dat met persoonsgegevens werkt beschouwt privacy en informatiebeveiliging vaak als twee los van elkaar staande kwesties.

Waarom klopt dit niet?

A) Het is niet mogelijk privacy te garanderen zonder passende informatiebeveiligingsmaatregelen te bepalen, implementeren en bewaken.
B) De toezichthoudende autoriteit verwacht dat de rollen van functionaris voor gegevensbescherming en informatiebeveiliger zijn geïntegreerd.
C) De regelgeving omschrijft specifieke informatiebeveiligingsmaatregelen die moeten worden genomen voordat persoonsgegevens mogen worden verwerkt.

28 / 40
Een van de doelen van een gegevensbeschermingseffectbeoordeling (DPIA) is om 'klanten of burgers meer vertrouwen te geven in de manier waarop persoonsgegevens verwerkt worden en privacy wordt gerespecteerd'.

Hoe kan een DPIA 'meer vertrouwen geven'?

A) De organisatie beperkt het risico op kostbare aanpassingen in processen of herontwerp van systemen in een later stadium tot een minimum.
B) De organisatie voorkomt niet-naleving van de AVG en beperkt het risico op boetes tot een minimum.
C) De organisatie bewijst dat ze privacy serieus neemt en ernaar streeft om aan de AVG te voldoen.

29 / 40
Wat is het doel van een controle van gegevensbescherming door de toezichthoudende autoriteit?

A) Aan de verplichting van de AVG voldoen om passende technische en organisatorische maatregelen voor gegevensbescherming te implementeren.
B) De toepassing van de AVG bewaken en afdwingen door te beoordelen of verwerking wordt uitgevoerd in overeenstemming met de AVG.
C) De verwerkingsverantwoordelijke adviseren over de vermindering van privacyrisico's om hem/haar te beschermen tegen aansprakelijkheidsvorderingen voor niet-naleving van de AVG.

30 / 40
Wat is de **beste** beschrijving van het principe van minimale gegevensverwerking?

A) Om de privacy en de belangen van de betrokkenen te beschermen moet er zorg aan besteed worden om zo min mogelijk gegevens te verzamelen.
B) Gegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.
C) Om gegevens beheersbaar te houden, moeten ze zo worden opgeslagen dat ze zo min mogelijk opslagruimte vereisen.
D) Het aantal items dat per betrokkene wordt verzameld mag niet hoger zijn dan de bovengrens die de toezichthoudende autoriteit heeft gesteld.

31 / 40
Sessiecookies zijn een van de meest voorkomende soorten cookies.

Wat is de **beste** beschrijving van een sessiecookie?

A) Het bevat informatie over wat u aan het doen bent, bijvoorbeeld welke producten u in een webwinkel selecteert voordat u daadwerkelijk bestelt.
B) Het onthult uw browsergeschiedenis, zodat andere websites kunnen achterhalen welke websites u bezocht hebt voordat u daar aankwam.
C) Het slaat uw browsegeschiedenis op, zodat u kunt traceren waar u op het net was en deze site(s) opnieuw bezoeken als u dat wilt.
D) Het verzamelt uw persoonsgegevens, zodat de website u met uw naam kan aanspreken en uw instellingen kan hergebruiken wanneer u terugkeert.

32 / 40
Soms volgen websites bezoekers en slaan ze hun informatie op voor marketingdoeleinden.

Is de website verplicht de bezoeker op de hoogte te stellen dat zijn/haar gegevens voor marketingdoeleinden worden gebruikt?

A) Ja
B) Nee

33 / 40
Een bedrijf kan zichzelf presenteren als expert in een specifiek vakgebied waarbij het gebruikmaakt van sociale media.

Wat is de **beste** manier om expertise in een specifiek onderwerp aan te tonen?

A) Door informatie over het bedrijf op sociale media te plaatsen
B) Door actief vragen over hun product te beantwoorden op sociale media
C) Door berichten te plaatsen over de redenen waarom het product van de concurrent minderwaardig is aan dat van het bedrijf
D) Door over nieuwe producten te berichten die het bedrijf aan het ontwikkelen is

34 / 40
Er is een inbreuk op de beveiliging opgetreden in een informatiesysteem dat ook persoonsgegevens bevat.

Wat moet de verwerkingsverantwoordelijke als **eerste** doen?

A) Controleren of de inbreuk verlies of onrechtmatige verwerking van persoonsgegevens tot gevolg kan hebben gehad
B) Het risico op nadelige effecten voor de betrokkenen beoordelen middels een gegevensbeschermingseffectbeoordeling (DPIA)
C) Beoordelen of er onrechtmatig persoonsgegevens van gevoelige aard verwerkt (kunnen) zijn
D) De inbreuk onmiddellijk rapporteren aan de relevante toezichthoudende autoriteit

35 / 40
Het woord 'privacy' komt niet voor in de AVG.

Wat is het verband tussen 'privacy' en 'gegevensbescherming'?

A) Gegevensbescherming is een verzameling regels en bepalingen over het verwerken van persoonsgegevens. Privacy is het resultaat van gegevensbescherming.
B) Privacy is het recht om tegen inmenging in persoonlijke aangelegenheden beschermd te worden. Gegevensbescherming is het middel om die bescherming te realiseren.
C) Privacy is het recht om persoonlijke aangelegenheden geheim te houden. Gegevensbescherming is het recht om persoonsgegevens geheim te houden.
D) De termen 'privacy' en 'gegevensbescherming' zijn uitwisselbaar. Er is geen relevant betekenisverschil.

36 / 40
Verordening (EU) 2016/679, ook wel bekend als de AVG, herroept een eerdere EU-verordening.

Welke verordening wordt ingetrokken (vervangen)?

A) Verordening 2002/58/EG van 12 juli 2002
B) Verordening 2006/24/EG van 15 maart 2006
C) Verordening 95/46/EG van 24 oktober 1995
D) Verordening 97/66/EG van 15 december 1997

37 / 40
Welk recht van betrokkenen wordt expliciet gedefinieerd in de AVG?

A) Er moet een kopie van de persoonsgegevens worden verstrekt in de door de betrokkene verzochte vorm.
B) Kosteloze toegang tot persoonsgegevens voor de betrokkene.
C) Persoonsgegevens moeten bij een verzoek daartoe van de betrokkene altijd gewijzigd worden.
D) Persoonsgegevens moeten altijd worden gewist als de betrokkene daarom vraagt.

38 / 40
De AVG kenmerkt 'gevoelige persoonsgegevens' als een bijzondere categorie persoonsgegevens.

Wat is een voorbeeld van dergelijke gegevens?

A) Een afspraak in het ziekenhuis met een medisch specialist
B) Een internationaal bankrekeningnummer (IBAN)
C) Aanmelding voor een wetenschappelijk tijdschrift over politiek
D) Het lidmaatschap van een brancheverenigingen

39 / 40
Welke rol in de gegevensbescherming bepaalt de doelen en middelen voor het verwerken van persoonsgegevens?

A) Verwerkingsverantwoordelijke
B) Functionaris voor gegevensbescherming
C) Verwerker

40 / 40
Welke informatie wordt in de AVG als persoonsgegevens beschouwd?

A) Informatie over een persoon die de privacy van die persoon kan schenden, ook al is de betreffende informatie onjuist
B) Alle informatie met betrekking tot een identificeerbare natuurlijke persoon
C) Informatie, over een identificeerbare natuurlijke persoon, die is gedigitaliseerd

Antwoordsleutel

1 / 40
Het illegaal verzamelen, opslaan, wijzigen, bekendmaken of verspreiden van persoonsgegevens is strafbaar onder Europees recht.

Wat voor soort strafbaar feit is dit?

A) een inhoudsgerelateerd delict
B) een economisch delict
C) een inbreuk op het intellectuele eigendomsrecht
D) een privacydelict

A) Incorrect. Een inhoudsgerelateerd delict heeft betrekking op de verspreiding van racistische uitspraken, (kinder-)pornografie of informatie die aanzet tot geweld.
B) Incorrect. Economische delicten hebben betrekking op de ongeoorloofde toegang tot systemen (hacking, verspreiding van virussen, enz.), computerspionage, -vervalsing en -fraude.
C) Incorrect. Inbreuken op het individuele eigendomsrecht behoren tot schendingen van het auteursrecht en naburige rechten.
D) Correct. Iedere illegale verwerking van persoonsgegevens is een delict. Geen bron: algemene ontwikkeling.

2 / 40
Wat is het verband tussen privacy en gegevensbescherming?

A) Gegevensbescherming is een onderdeel van privacy.
B) Privacy is een onderdeel van gegevensbescherming.
C) Dat is hetzelfde.
D) Privacy is niet mogelijk zonder gegevensbescherming.

A) Incorrect. Privacy omvat veel begrippen zoals ruimtelijke, relationele, lichamelijke en informatieprivacy. Gegevensbescherming heeft met sommige van deze begrippen niets te maken.
B) Incorrect. Privacy omvat veel begrippen zoals ruimtelijke, relationele, lichamelijke en informatieprivacy. Gegevensbescherming helpt een aantal hiervan te waarborgen.
C) Incorrect. Gegevensbescherming heeft bijvoorbeeld niets met ruimtelijke privacy te maken.
D) Correct. Gegevensbescherming is een noodzakelijke maatregel om het fundamentele recht op privacy te beschermen. Bron: White Paper – Privacy, Personal Data and the GDPR - § 1.3 Definitions.

3 / 40
Waar is de AVG **voornamelijk** voor bedoeld?

A) Om als gemeenschappelijke basis te dienen voor door de lidstaten zelf te ontwerpen wetten
B) Om niet-EU-landen te dwingen het recht op privacy van personen binnen de EU te respecteren
C) Om privacy als fundamenteel mensenrecht voor iedereen te waarborgen
D) Om gegevensbescherming voor individuen binnen de EU te verbeteren en gelijk te maken (te harmoniseren)

A) Incorrect. De AVG is een verordening, wat betekent dat deze gegevensbeschermingswetten in de lidstaten vervangt.
B) Incorrect. Het belangrijkste doel van de AVG is om de rechten op gegevensbescherming van personen binnen de EU te beschrijven.
C) Incorrect. In de AVG staat expliciet vermeld dat gegevensbescherming een grondrecht is, maar de reikwijdte ervan is beperkt tot personen binnen de EU.
D) Correct. De reikwijdte van de AVG is beperkt tot gegevensbescherming als recht van personen binnen de EU en heeft tot doel de regels hiervoor binnen de EU te harmoniseren. Bron: EU GDPR, A pocket guide – Introduction.

4 / 40
De AVG heeft te maken met de bescherming van persoonsgegevens.

Wat is de definitie van persoonsgegevens?

A) Alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon
B) Alle informatie die de Europese burgers willen beschermen
C) Gegevens waaruit direct of indirect iemands ras of etnische achtergrond, religieuze overtuigingen, gezondheidsinformatie of seksuele gewoonten blijken
D) Behoud van vertrouwelijkheid, integriteit en beschikbaarheid van informatie

A) Correct. Dit is de officiële definitie van de gegevensbescherming. Bron: EU GDPR, A pocket guide - Chapter 2 Terms and definitions GDPR 2016/679 Article 4: definition
B) Incorrect. Deze definitie is te algemeen.
C) Incorrect. Dit is de definitie van gevoelige gegevens, niet van algemene persoonsgegevens.
D) Incorrect. Dit is de definitie van informatiebeveiliging uit ISO/IEC 27000:2014.

5 / 40
Welke categorie persoonsgegevens wordt in de AVG beschouwd als gevoelige gegevens?

A) Creditcardgegevens
B) Lidmaatschap van een vakbond
C) Paspoortnummer
D) Burgerservicenummer

A) Incorrect. Creditcardgegevens zijn volgens de AVG geen gevoelige gegevens.
B) Correct. Lidmaatschap van een vakbond valt in de categorie gevoelige gegevens. Bron: AVG Art. 9 lid 1 en overweging (10) - Verwerking van bijzondere categorieën van persoonsgegevens.
C) Incorrect. Paspoortgegevens zijn volgens de AVG geen gevoelige gegevens.
D) Incorrect. Een burgerservicenummer valt volgens de AVG niet in de categorie gevoelige gegevens.

6 / 40
Wat is volgens de AVG de definitie van 'verwerking' van persoonsgegevens?

A) Iedere bewerking die op persoonsgegevens kan worden uitgevoerd
B) Iedere bewerking die op persoonsgegevens kan worden uitgevoerd, behalve wissen en vernietigen
C) Alleen handelingen waarbij de gegevens worden gedeeld op sociale media of per e-mail of op andere wijze via internet worden verstuurd
D) Alleen bewerkingen waarbij de persoonsgegevens worden gebruikt voor de doeleinden waarvoor ze zijn verzameld

A) Correct. Bron: AVG art.4 (2)
B) Incorrect. 'verwerking' slaat op iedere actie die wordt uitgevoerd met persoonsgegevens.
C) Incorrect. 'verwerking' slaat op iedere actie die wordt uitgevoerd met persoonsgegevens.
D) Incorrect. 'verwerking' slaat op iedere actie die wordt uitgevoerd met persoonsgegevens.

7 / 40
"*Een onafhankelijke overheidsinstantie die door een lidstaat is opgericht krachtens artikel 51.*"

Van welke rol in de gegevensbescherming is dit de definitie?

A) Verwerkingsverantwoordelijke
B) Verwerker
C) Toezichthoudende autoriteit
D) Derde partij

A) Incorrect. Zie verordening 2016/679, artikel 4.
B) Incorrect. Zie verordening 2016/679, artikel 4.
C) Correct. Bron: AVG 2016/679, artikel 4 en artikel 51.
D) Incorrect. Zie verordening 2016/679, artikel 4.

8 / 40
Geïnformeerde toestemming' is onder de AVG een rechtmatige basis om persoonsgegevens te verwerken. Het doel van de verwerking waarvoor toestemming wordt gegeven moet worden gedocumenteerd.

Op welk moment in het proces moet de toestemming van de betrokkene worden verkregen?

A) Nadat de toelichting over het doel is gepresenteerd en voordat persoonsgegevens worden verzameld
B) Voordat de specificatie van het doel is bedacht en gepresenteerd
C) Voordat de persoonsgegevens verwerkt worden
D) Voordat de persoonsgegevens worden gepubliceerd of verspreid

A) Correct. Toestemming kan alleen geïnformeerd zijn nadat de specificatie van de doelstelling aan de betrokkene is gepresenteerd. Bron: Overwegingen 32 en 42 van de AVG.
B) Incorrect. Toestemming kan alleen geïnformeerd zijn nadat de specificatie van de doelstelling aan de betrokkene is gepresenteerd.
C) Incorrect. Het verzamelen van persoonsgegevens is 'verwerking' en als zodanig is hiervoor geïnformeerde toestemming van de betrokkene nodig.
D) Incorrect. Het publiceren en verspreiden van persoonsgegevens is 'verwerking' en als zodanig is hiervoor geïnformeerde toestemming van de betrokkene nodig.

9 / 40
De AVG is gebaseerd op de beginselen van proportionaliteit en subsidiariteit.

Wat betekent 'proportionaliteit' in deze context?

A) Persoonsgegevens mogen alleen in overeenstemming met het gespecificeerde doel worden verwerkt.
B) Persoonsgegevens mogen niet worden hergebruikt zonder expliciete en geïnformeerde toestemming.
C) Persoonsgegevens mogen alleen worden verwerkt als er geen andere manier is om de doeleinden te bereiken.
D) Persoonsgegevens moeten toereikend en relevant zijn en niet overmatig ten opzichte van de doeleinden.

A) Incorrect. Dit is een van de wettelijke beperkingen.
B) Incorrect. Dit is een van de wettelijke beperkingen.
C) Incorrect. Dit is de definitie van subsidiariteit.
D) Correct. Bron: White Paper – Privacy, Personal Data and the GDPR - § 3.1.2 Proportionality and subsidiarity & AVG art. 35 (7)

10 / 40
De verwerking van persoonsgegevens moet voldoen aan bepaalde kwaliteitseisen.

Wat is een van deze kwaliteitseisen die in de AVG is gedefinieerd?

A) De verwerkte gegevens moeten worden gearchiveerd.
B) De verwerkte gegevens moeten worden versleuteld.
C) De verwerkte gegevens moeten worden geïndexeerd.
D) De verwerkte gegevens moeten relevant zijn.

A) Incorrect. In de AVG is geen dergelijk vereiste gedefinieerd.
B) Incorrect. In de AVG is geen dergelijk vereiste gedefinieerd.
C) Incorrect. In de AVG is geen dergelijk vereiste gedefinieerd.
D) Correct. Dit vereiste is gedefinieerd in de AVG. Bron: White Paper – Privacy, Personal Data and the GDPR - § 3.1.2 Proportionality and subsidiarity

11 / 40
Iedere keer dat persoonsgegevens worden verwerkt moeten proportionaliteit en subsidiariteit worden gecontroleerd.

Welk vereiste geldt er voor de persoonsgegevens die worden verwerkt?

A) Ze moeten altijd beperkt blijven tot de informatie die nodig is om de gespecificeerde doelen te bereiken en tot de minst 'indringende' gegevens.
B) Ze moeten door zo min mogelijk werknemers worden verwerkt en deze werknemers moeten voor de verwerkingsverantwoordelijke of een filiaal werken.
C) De verwerking moet beperkt worden tot een vooraf gedefinieerd opslagformaat en het systeem dat gebruikt wordt moet door de verwerkingsverantwoordelijke worden gefinancierd.
D) Ze moeten voor zo min mogelijk doeleinden worden gebruikt en dit gebruik mag niet buiten het pand van de verwerker plaatsvinden.

A) Correct. Deze termen betekenen dat u niet meer gegevens inzamelt dan nodig is om het (de) vooraf gedefinieerde doeleinde(s) te bereiken en dat u altijd probeert gegevens te gebruiken die het kleinst mogelijke effect hebben op de privacy van de betrokkene. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation – Lawful processing
B) Incorrect. Het aantal werknemers of het feit dat ze bij een dochteronderneming werken heeft niets met deze voorwaarden te maken.
C) Incorrect. Opslaggrootte en wie het systeem financiert hebben niets met deze termen te maken.
D) Incorrect. Zo lang de betrokkene toestemming verleent is het aantal doeleinden niet expliciet beperkt, en de locatie ook niet.

12 / 40
"*De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te zorgen dat (...) alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor ieder specifiek doel van de verwerking.*"

Van welke term in de AVG is dit de definitie?

A) Naleving
B) Gegevensbescherming door standaardinstellingen
C) Privacy door ontwerp
D) Ingebouwde bescherming

A) Incorrect. Naleving is de toestand of het feit van overeenstemmen met of voldoen aan regels of normen.
B) Correct. Standaard moet het minimum aantal persoonsgegevens worden verwerkt voor de kortst mogelijke tijd, met de best mogelijke beveiligingsmaatregelen om ongeoorloofde toegang te voorkomen. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data protection by design and by default & AVG art. 20 (2).
C) Incorrect. Gegevensbescherming door ontwerp verwijst naar een ontwerp waarin passende maatregelen zijn opgenomen om principes inzake gegevensbescherming te implementeren.
D) Incorrect. Ingebouwde gegevensbescherming is het resultaat van gegevensbescherming door ontwerp.

13 / 40
Welke term wordt in de AVG gebruikt voor ongeoorloofde verstrekking van, of toegang tot persoonsgegevens?

A) Verlies van vertrouwelijkheid
B) Inbreuk in verband met persoonsgegevens
C) Incident
D) Inbreuk op de beveiliging

A) Incorrect. De AVG gebruikt de term inbreuk in verband met persoonsgegevens. Niet iedere inbreuk in verband met persoonsgegevens is een inbreuk op de vertrouwelijkheid.
B) Correct. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation Data breaches & AVG artikel 4 (12)
C) Incorrect. De AVG gebruikt de term inbreuk in verband met persoonsgegevens. Niet ieder incident is een inbreuk in verband met persoonsgegevens.
D) Incorrect. De AVG gebruikt de term inbreuk in verband met persoonsgegevens. Niet iedere inbreuk op de beveiliging is een inbreuk in verband met persoonsgegevens.

14 / 40
Er is vastgesteld dat er een inbreuk in verband met gevoelige persoonsgegevens is opgetreden.

Aan wie moet dit uiteindelijk worden gerapporteerd volgens de AVG?

A) de toezichthoudende autoriteit
B) de functionaris voor gegevensbescherming (FG)
C) de manager van de afdeling
D) de politie

A) Correct. Inbreuken in verband met persoonsgegevens moeten aan de toezichthoudende autoriteit worden gerapporteerd als ze een belangrijk effect kunnen hebben op de veiligheid van de betrokkene of diens persoonsgegevens. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation Data breaches & AVG artikel 4 (12)
B) Incorrect. Hoewel het aan een interne FG kan worden gerapporteerd, moet het uiteindelijk aan de toezichthoudende autoriteit worden gerapporteerd.
C) Incorrect. Hoewel het aan de manager kan worden gerapporteerd, moet het uiteindelijk aan de toezichthoudende autoriteit worden gerapporteerd.
D) Incorrect. Inbreuken in verband met persoonsgegevens hoeven niet noodzakelijk aan de politie te worden gemeld, maar moeten uiteindelijk wel aan de toezichthoudende autoriteit worden gemeld.

15 / 40
Tijdens het uitvoeren van een back-up gaat een harde schijf van een dataserver stuk. Zowel de gegevens als de back-up gaan verloren. De harde schijf bevatte persoonsgegevens, maar geen gevoelige gegevens.

Wat voor type incident is dit?

A) Inbreuk in verband met persoonsgegevens
B) Inbreuk op de beveiliging
C) Incident

A) Correct. Wanneer er persoonsgegevens onherstelbaar verloren gaan, wordt dit aangemerkt als een ongeoorloofde verwerking, dus een inbreuk in verband met persoonsgegevens. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches & AVG Hoofdstuk I, artikel 4, Definities.
B) Incorrect. Wanneer er persoonsgegevens onherstelbaar verloren gaan, wordt dit aangemerkt als een ongeoorloofde verwerking, dus een inbreuk in verband met persoonsgegevens.
C) Incorrect. Wanneer er persoonsgegevens onherstelbaar verloren gaan, wordt dit aangemerkt als een ongeoorloofde verwerking, dus een inbreuk in verband met persoonsgegevens.

16 / 40
Iemand die voor een vakbond werkt heeft een concept-nieuwsbrief voor de leden mee naar huis genomen, om hem daar af kunnen maken. Hij is de USB-stick met het concept en de mailinglijst verloren.

Aan wie moet deze inbreuk in verband met persoonsgegevens in ieder geval worden gerapporteerd?

A) Alle leden op de mailinglijst
B) Het personeel van de vakbond
C) De politie

A) Correct. Dit zijn gevoelige gegevens, dus het verlies moet worden gerapporteerd aan zowel de toezichthoudende autoriteit als de betrokkenen. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches
B) Incorrect. Dit zijn gevoelige gegevens, dus het verlies moet worden gerapporteerd aan zowel de toezichthoudende autoriteit als de betrokkenen.
C) Incorrect. Dit zijn gevoelige gegevens, dus het verlies moet worden gerapporteerd aan zowel de toezichthoudende autoriteit als de betrokkenen.

17 / 40
Een organisatie voor sociale voorzieningen is van plan een nieuwe database te ontwerpen waarin staat wie hun klanten zijn en welke zorg zij nodig hebben.

Wat is een van de eerste belangrijke stappen die genomen moet worden om goedkeuring van de toezichthoudende autoriteit te krijgen?

A) Informatie verzamelen over de klanten en het type en de hoeveelheid zorg die ze nodig hebben en krijgen
B) Een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren om de risico's van de beoogde verwerking te beoordelen
C) Toestemming van de klanten verkrijgen voor de beoogde verwerking van hun persoonsgegevens

A) Incorrect. Het verzamelen van medische persoonsgegevens is per definitie ‘het verwerken van gevoelige gegevens’. Hiervoor is vooraf toestemming van de toezichthoudende autoriteit en de betrokkene nodig.
B) Correct. Wanneer de betrokkene om toestemming wordt gevraagd om gegevens te verwerken, ‘moeten bewust worden gemaakt van de risico's, regels, waarborgen en rechten...’. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation – Consent & AVG overweging 39.
C) Incorrect. Wanneer de betrokkene om toestemming wordt gevraagd om gegevens te verwerken, ‘moeten bewust worden gemaakt van de risico's, regels, waarborgen en rechten...’. Er is eerst een gegevensbeschermingseffectbeoordeling nodig om die risico's en waarborgen te evalueren.

18 / 40
In welk geval moeten de betrokkenen altijd op de hoogte worden gesteld van een inbreuk in verband met persoonsgegevens?

A) Als de persoonsgegevens zijn verwerkt bij een faciliteit van de verwerker die niet binnen de grenzen van de EU gelegen is.
B) Als de persoonsgegevens zijn verwerkt door een partij die wel heeft ingestemd met het contract dat de verwerkingsverantwoordelijke stuurde, maar het nog niet heeft getekend.
C) Als het systeem waarop de persoonsgegevens verwerkt zijn, is aangevallen en daarbij de opslagapparaten beschadigd zijn.
D) Als er een reële kans is dat de inbreuk nadelige gevolgen zal hebben voor de privacy van de betrokkenen.

A) Incorrect. De plaats waar de gegevens verwerkt worden is irrelevant voor de verplichting om betrokkenen op de hoogte te brengen van inbreuken in verband met persoonsgegevens.
B) Incorrect. Als persoonsgegevens worden verwerkt door een andere partij dan de verwerkingsverantwoordelijke, zonder schriftelijk contract, dan is sprake van een inbreuk in verband met persoonsgegevens. In de gegeven situatie zijn negatieve gevolgen voor de betrokkenen echter onwaarschijnlijk. Informeren van de betrokkenen is dan niet verplicht.
C) Incorrect. Schade aan opslagapparatuur maakt toegang tot gegevens moeilijk of zelfs onmogelijk, maar dat maakt niet dat er sprake is van illegale verwerking.
D) Correct. Als er een reële kans is dat de inbreuk schadelijke gevolgen zal hebben voor de betrokkenen, dan is de verwerkingsverantwoordelijke verplicht hen van de inbreuk op de hoogte te stellen. Bron: White Paper – Privacy, Personal Data and the GDPR - § 5.2 Procedures on how to act when a data breach occurs.

19 / 40
Een Nederlandse verwerkingsverantwoordelijke heeft de verwerking van gevoelige persoonsgegevens uitbesteed aan een verwerker in een Noord-Afrikaans land, zonder hierover de toezichthoudende autoriteit te raadplegen. Dit is ontdekt en hij is gestraft door de toezichthoudende autoriteit. Zes maanden later stelt de autoriteit vast dat de verwerkingsverantwoordelijke zich weer schuldig heeft gemaakt aan dezelfde overtreding bij een andere verwerking.

Wat is de maximale geldboete die de toezichthoudende autoriteit in dit geval kan opleggen?

A) € 750.000
B) €1.230.000
C) € 10.000.000, of 2% van de wereldwijde omzet van het bedrijf, indien dit cijfer hoger is.
D) € 20.000.000, of 4% van de wereldwijde omzet van het bedrijf, indien dit cijfer hoger is.

A) Incorrect. Volgens de AVG art. 83.3 is de maximale boete € 20.000.000 of 4% van de wereldwijde omzet van het bedrijf indien dit meer is.
B) Incorrect. Volgens de AVG art. 83.3 is de maximale boete € 20.000.000 of 4% van de wereldwijde omzet van het bedrijf indien dit meer is.
C) Incorrect. Volgens de AVG art. 83.3 is de maximale boete € 20.000.000 of 4% van de wereldwijde omzet van het bedrijf indien dit meer is.
D) Correct. Dit is het maximum voor een overtreding. Bron: White Paper – Privacy, Personal Data and the GDPR - §7.3.3 General conditions for imposing administrative fines.

20 / 40
Toezichthoudende autoriteiten krijgen een aantal verantwoordelijkheden toegewezen om ervoor te zorgen dat regelgeving over gegevensbescherming wordt nageleefd.

Wat is een van deze verantwoordelijkheden?

A) Beoordelen van gedragscodes voor specifieke sectoren over de verwerking van persoonsgegevens
B) Definiëren van een minimumpakket van maatregelen die moeten worden genomen om persoonsgegevens te beschermen
C) Onderzoeken van alle inbreuken in verband met persoonsgegevens waarvan ze op de hoogte zijn gesteld
D) Contracten en bindende bedrijfsvoorschriften controleren op conformiteit met de regelgeving

A) Correct. Een van de verantwoordelijkheden van de toezichthoudende autoriteiten is om organisaties van algemeen advies te voorzien over hoe ze aan de wettelijke regels kunnen voldoen. Bron: White Paper – Privacy, Personal Data and the GDPR - §7.1.4 To set standards.
B) Incorrect. Een toezichthoudende autoriteit verschaft algemeen advies over wat volgens hen een passend beveiligingsniveau is. Ze vertellen u echter niet welke specifieke maatregelen u moet nemen om dat niveau te realiseren. Zelfs als ze dat zouden willen zouden ze het niet kunnen, omdat er gewoonweg geen universele oplossing is.
C) Incorrect. Toezichthoudende autoriteiten zijn niet verplicht en hebben niet voldoende capaciteit om alle inbreuken in verband met persoonsgegevens waarvan ze op de hoogte zijn te onderzoeken. Maar ze onderzoeken die gevallen die zij belangrijk of opmerkelijk vinden.
D) Incorrect. Een toezichthoudende autoriteit is geen juridisch adviseur. Ze geven geen advies over contracten of bindende bedrijfsvoorschriften. Tijdens een onderzoek kunnen ze wel naar een specifiek contract of set bindende bedrijfsvoorschriften kijken.

21 / 40
Een religieuze organisatie wil persoonsgegevens delen met hun religieuze autoriteit in een niet-Europees land om te voldoen aan een wettelijk verzoek van de betreffende regering.

Welke bepaling uit de AVG is in dit geval van toepassing?

A) Bij wijze van uitzondering is de verwerking van gevoelige gegevens waaruit religieuze overtuigingen blijken toegestaan aan religieuze organisaties.
B) Het is niet geoorloofd om persoonsgegevens buiten de EER te brengen naar aanleiding van een wettelijk vereiste van een derde land.
C) Verwerking is rechtmatig mits specifieke en ondubbelzinnige toestemming van de betrokkene is verkregen.
D) Persoonsgegevens buiten de EER verwerken is toegestaan op basis van modelcontractclausules die door de Europese Commissie ontworpen zijn.

A) Incorrect. Religieuze verenigingen mogen persoonsgegevens met betrekking tot hun voormalige en huidige leden verwerken, *maar het is verboden om persoonsgegevens buiten de EU te brengen naar aanleiding van een wettelijk vereiste van een derde land.*
B) Correct. Bron: White Paper – Privacy, Personal Data and the GDPR - §7.5.2 Regulations applying to data transfer outside the EEA & EU GDPR, A pocket guide - Chapter 3: The regulation – International transfers & AVG art. 48.
C) Incorrect. Het is niet geoorloofd om persoonsgegevens buiten de EU te brengen naar aanleiding van een wettelijk vereiste van een derde land, *zelfs niet met toestemming van de betrokkene.*
D) Incorrect. Het verwerken van gevoelige gegevens buiten de EU kan wettig zijn, maar niet naar aanleiding van een verzoek van de overheid van een derde land.

22 / 40
Op 12 juli 2016 heeft de Europese Commissie een uitspraak uitgevoerd met betrekking tot de doorgifte van persoonsgegevens aan of door de V.S. (EU-VS-privacyschild).

Wat voor uitspraak is dit in termen van de AVG?

A) Een adequaatheidsbesluit
B) Een vrijstellingsbesluit
C) Een standaard bindend contract
D) Een verdrag dat voorrang heeft op de AVG

A) Correct. De uitspraak is een adequaatheidsbesluit in overeenstemming met de AVG met betrekking tot verwerking in derde landen. Bron: White Paper – Privacy, Personal Data and the GDPR - §7.5.4 Regulations applying to data transfer between the EEA and the USA & EU GDPR, A pocket guide - Chapter 3 The Regulation – International transfers & AVG overwegingen 104 en 106.
B) Incorrect. Een uitzondering heeft betrekking op doorgiften die noodzakelijk zijn om op terroristische delicten of ernstige misdrijven te reageren (art. 11).
C) Incorrect. De uitspraak is een adequaatheidsbesluit in overeenstemming met de AVG met betrekking tot verwerking in derde landen.
D) Incorrect. De uitspraak is een adequaatheidsbesluit in overeenstemming met de AVG met betrekking tot verwerking in derde landen.

23 / 40
Bindende bedrijfsvoorschriften zijn een manier waarop organisaties hun administratieve lasten om te voldoen aan de AVG kunnen verminderen.

Waarom zijn deze regels nuttig voor hen?

A) Ze stellen hen in staat om underpinning contracts (externe onderliggende contracten) met alle betrokken partijen in het buitenland af te sluiten.
B) Ze staan hen toe derden buiten de Europese Economische Ruimte persoonsgegevens te laten verwerken.
C) Ze voorkomen dat organisaties iedere toezichthoudende autoriteit in de EU apart moet benaderen.
D) Wanneer de bindende bedrijfsvoorschriften zijn geaccepteerd voorkomen deze dat ze een toezichthoudende autoriteit om toestemming moeten vragen om de gegevens te verwerken.

A) Incorrect. Bindende bedrijfsvoorschriften worden opgesteld zodat organisaties niet voor ieder filiaal schriftelijke underpinning contracts hoeven af te sluiten.
B) Incorrect. Bindende bedrijfsvoorschriften gelden alleen binnen een organisatie en al haar filialen. Ze gelden niet voor andere partijen.
C) Correct. Zodra bindende bedrijfsvoorschriften zijn goedgekeurd door een toezichthoudende autoriteit in de EU hoeft u de andere toezichthoudende autoriteiten in de EU niet meer om goedkeuring te vragen. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation – Binding corporate rules
D) Incorrect. Bindende bedrijfsvoorschriften moeten ook door een toezichthoudende autoriteit worden goedgekeurd.

24 / 40
Als een contractant verwerking van persoonsgegevens uitbesteedt, gaan de partijen een schriftelijke overeenkomst aan. In deze overeenkomst zijn het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het type persoonsgegevens en de categorieën van betrokkenen gedefinieerd.

Welk ander aspect moet door dit schriftelijke contract worden geregeld?

A) de aansprakelijkheid van de verwerker
B) de meldplicht inbreuk persoonsgegevens
C) de verplichting voor verwerkers om medewerking te verlenen aan de toezichthoudende autoriteit
D) de verplichtingen en rechten van de verwerkingsverantwoordelijke

A) Incorrect. Dit is een rechtstreekse verplichting van de AVG voor verwerkers.
B) Incorrect. Dit is een rechtstreekse verplichting van de AVG voor verwerkers.
C) Incorrect. Dit is een rechtstreekse verplichting van de AVG voor verwerkers.
D) Correct. Dit is een rechtstreekse verplichting van de AVG voor verwerkers. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation – Controller/processor contracts & AVG art. 28 (3).

25 / 40
Wat moet er worden gedaan om te zorgen dat een verwerkingsverantwoordelijke de verwerking van persoonsgegevens kan uitbesteden aan een verwerker?

A) De verwerkingsverantwoordelijke moet de toezichthoudende autoriteit om toestemming vragen om de gegevensverwerking uit te besteden.
B) De verwerkingsverantwoordelijke moet de toezichthoudende autoriteit vragen of het overeengekomen schriftelijke contract aan de regelgeving voldoet.
C) De verwerkingsverantwoordelijke en de verwerker moeten een schriftelijke overeenkomst opstellen en ondertekenen waarin ze de vertrouwelijkheid van de gegevens garanderen.
D) De verwerker moet de verwerkingsverantwoordelijke laten zien dat aan alle vereisten die zijn overeengekomen in de dienstenniveau-overeenkomst (ofwel SLA) wordt voldaan.

A) Incorrect. U hoeft de toezichthoudende autoriteit niet iedere keer dat u iets uitbesteedt om toestemming te vragen.
B) Incorrect. De toezichthoudende autoriteit is geen juridisch adviseur en controleert niet of contracten aan de AVG voldoen.
C) Correct. Er moet een schriftelijk contract zijn waarin de vertrouwelijkheid van de gegevens wordt gegarandeerd en waarin de verwerkingsverantwoordelijke de doelen en middelen van verwerking definieert. Beide partijen moeten dit contract ondertekenen. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation – Controller/processor contracts & AVG art. 28 (3).
D) Incorrect. Een dienstenniveau-overeenkomst (ofwel SLA) is niet toereikend, aangezien deze betrekking heeft op handelingen, niet per se op het bepalen van doelen.

26 / 40
Gegevensbescherming door ontwerp, zoals beschreven in artikel 25 van de AVG, is gebaseerd op zeven principes. Een hiervan wordt meestal *'Functionaliteit - positive sum in plaats van zero sum'* genoemd.

Wat is de kern van dit principe?

A) Toegepaste beveiligingsnormen moeten vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens waarborgen gedurende de volledige levenscyclus.
B) Als verschillende soorten legitieme doelstellingen tegenstrijdig zijn dan moeten de privacydoelstellingen prioriteit krijgen boven andere beveiligingsdoelstellingen.
C) Wanneer privacy in een bepaalde technologie, proces of systeem wordt gebouwd, moet dit zo worden gedaan dat de volledige functionaliteit niet nadelig wordt beïnvloed.
D) Wanneer dat mogelijk is moeten er altijd gedetailleerde evaluaties van de privacy-effecten en risico's worden uitgevoerd en gepubliceerd, waarbij de privacyrisico's duidelijk worden gedocumenteerd.

A) Incorrect. Dit is een aspect van end-to-end beveiliging - Bescherming gedurende de hele levenscyclus, een van de zes andere basisprincipes.
B) Incorrect. Privacy door ontwerp verwerpt de benadering waarbij privacy moet strijden met andere rechtmatige belangen, ontwerpdoelen en technische mogelijkheden. Er moet aan alle objecten tegemoet worden gekomen op een positieve som 'win-win'-manier.
C) Correct, daar komt het op neer. Bron: White Paper – Privacy, Personal Data and the GDPR - § 8.1.1 The seven principles of data protection by design & AVG art. 25
D) Incorrect. Dit is een aspect van '*integreren* van privacy in het ontwerp', een van de zes andere basisprincipes.

27 / 40
Personeel dat met persoonsgegevens werkt beschouwt privacy en informatiebeveiliging vaak als twee los van elkaar staande kwesties.

Waarom klopt dit niet?

A) Het is niet mogelijk privacy te garanderen zonder passende informatiebeveiligingsmaatregelen te bepalen, implementeren en bewaken.
B) De toezichthoudende autoriteit verwacht dat de rollen van functionaris voor gegevensbescherming en informatiebeveiliger zijn geïntegreerd.
C) De regelgeving omschrijft specifieke informatiebeveiligingsmaatregelen die moeten worden genomen voordat persoonsgegevens mogen worden verwerkt.

A) Correct. Privacy en gegevensbescherming hebben betrekking op het garanderen van vertrouwelijkheid van persoonsgegevens e.a. Hiervoor is de implementatie van beveiligingsmaatregelen nodig. Bron: White Paper – Privacy, Personal Data and the GDPR - § 2.1.6 - integrity and confidentiality.
B) Incorrect. De toezichthoudende autoriteit verwacht helemaal niet dat deze rollen worden geïntegreerd.
C) Incorrect. In de regelgeving zijn doelen gespecificeerd die gerealiseerd moeten worden, maar geen specifieke maatregelen die moeten worden genomen.

28 / 40
Een van de doelen van een gegevensbeschermingseffectbeoordeling (DPIA) is om 'klanten of burgers meer vertrouwen te geven in de manier waarop persoonsgegevens verwerkt worden en privacy wordt gerespecteerd'.

Hoe kan een DPIA 'meer vertrouwen geven'?

A) De organisatie beperkt het risico op kostbare aanpassingen in processen of herontwerp van systemen in een later stadium tot een minimum.
B) De organisatie voorkomt niet-naleving van de AVG en beperkt het risico op boetes tot een minimum.
C) De organisatie bewijst dat ze privacy serieus neemt en ernaar streeft om aan de AVG te voldoen.

A) Incorrect. Dit aspect geeft misschien wel meer vertrouwen aan het management, maar niet aan klanten of burgers.
B) Incorrect. Boetes voorkomen geeft misschien wel meer vertrouwen aan het management, maar niet aan klanten of burgers.
C) Correct. Bron: EU GDPR, A pocket guide - Chapter 3 The Regulation - Data Protection Impact Assessments

29 / 40
Wat is het doel van een controle van gegevensbescherming door de toezichthoudende autoriteit?

A) Aan de verplichting van de AVG voldoen om passende technische en organisatorische maatregelen voor gegevensbescherming te implementeren.
B) De toepassing van de AVG bewaken en afdwingen door te beoordelen of verwerking wordt uitgevoerd in overeenstemming met de AVG.
C) De verwerkingsverantwoordelijke adviseren over de vermindering van privacyrisico's om hem/haar te beschermen tegen aansprakelijkheidsvorderingen voor niet-naleving van de AVG.

A) Incorrect. De controle is niet de implementatie van de maatregelen, maar een evaluatie van de effectiviteit ervan.
B) Correct. Volgens de AVG is dit een belangrijke taak van de toezichthoudende autoriteit als toezichthouder. Bron: AVG art 57.1(a)
C) Incorrect. De toezichthoudende autoriteit heeft de taak op naleving te controleren en te adviseren over verbeteringen, maar heeft niet als doel de verwerkingsverantwoordelijke te beschermen.

30 / 40
Wat is de **beste** beschrijving van het principe van minimale gegevensverwerking?

A) Om de privacy en de belangen van de betrokkenen te beschermen moet er zorg aan besteed worden om zo min mogelijk gegevens te verzamelen.
B) Gegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.
C) Om gegevens beheersbaar te houden, moeten ze zo worden opgeslagen dat ze zo min mogelijk opslagruimte vereisen.
D) Het aantal items dat per betrokkene wordt verzameld mag niet hoger zijn dan de bovengrens die de toezichthoudende autoriteit heeft gesteld.

A) Incorrect. Om precies te zijn staat in de AVG dat de verzamelde gegevens toereikend moeten zijn, wat impliceert dat het niet het absolute minimum hoeft te zijn.
B) Correct. Dit is de definitie van minimale gegevensverwerking. Dit principe is bedoeld om te zorgen dat alleen gegevens worden verzameld die nodig zijn om de gedefinieerde doelen te bereiken. Bron: White Paper – Privacy, Personal Data and the GDPR - §2.1 Data processing principles & AVG artikel 5.1.c.
C) Incorrect. Opslaggrootte heeft niets met dit principe te maken.
D) Incorrect. Toezichthoudende autoriteiten stellen geen bovengrens aan het aantal verzamelde eenheden, zo lang dit aantal beperkt is tot wat nodig is om de gedefinieerde doelen te realiseren.

31 / 40
Sessiecookies zijn een van de meest voorkomende soorten cookies.

Wat is de **beste** beschrijving van een sessiecookie?

A) Het bevat informatie over wat u aan het doen bent, bijvoorbeeld welke producten u in een webwinkel selecteert voordat u daadwerkelijk bestelt.
B) Het onthult uw browsergeschiedenis, zodat andere websites kunnen achterhalen welke websites u bezocht hebt voordat u daar aankwam.
C) Het slaat uw browsegeschiedenis op, zodat u kunt traceren waar u op het net was en deze site(s) opnieuw bezoeken als u dat wilt.
D) Het verzamelt uw persoonsgegevens, zodat de website u met uw naam kan aanspreken en uw instellingen kan hergebruiken wanneer u terugkeert.

A) Correct. Een sessiecookie wordt bewaard om informatie over de sessie te bewaren. Het wordt gewist wanneer u de sessie afsluit. Bron: White Paper – Privacy, Personal Data and the GDPR - § 8.6.3 Cookies
B) Incorrect. Een sessie-cookie wordt gewist wanneer u de sessie sluit, zodat het bij een volgende sessie niet opnieuw kan worden gebruikt.
C) Incorrect. Een sessie-cookie wordt gewist wanneer u de sessie sluit, zodat het bij een volgende sessie niet opnieuw kan worden gebruikt.
D) Incorrect. Een sessie-cookie wordt gewist wanneer u de sessie sluit, zodat het bij een volgende sessie niet opnieuw kan worden gebruikt.

32 / 40
Soms volgen websites bezoekers en slaan ze hun informatie op voor marketingdoeleinden.

Is de website verplicht de bezoeker op de hoogte te stellen dat zijn/haar gegevens voor marketingdoeleinden worden gebruikt?

A) Ja
B) Nee

A) Correct. De website is verplicht de bezoeker op de hoogte te stellen dat zijn/haar gegevens voor marketingdoeleinden worden gebruikt. Ze hebben het recht om bezwaar aan te tekenen tegen de verwerking van hun persoonsgegevens voor marketingdoeleinden. Bron: White Paper – Privacy, Personal Data and the GDPR - § 8.6.3 Cookies
B) Incorrect. De website is verplicht de bezoeker op de hoogte te stellen dat zijn/haar gegevens voor marketingdoeleinden worden gebruikt. Ze hebben het recht om bezwaar aan te tekenen tegen de verwerking van hun persoonsgegevens voor marketingdoeleinden.

33 / 40
Een bedrijf kan zichzelf presenteren als expert in een specifiek vakgebied waarbij het gebruikmaakt van sociale media.

Wat is de **beste** manier om expertise in een specifiek onderwerp aan te tonen?

A) Door informatie over het bedrijf op sociale media te plaatsen
B) Door actief vragen over hun product te beantwoorden op sociale media
C) Door berichten te plaatsen over de redenen waarom het product van de concurrent minderwaardig is aan dat van het bedrijf
D) Door over nieuwe producten te berichten die het bedrijf aan het ontwikkelen is

A) Incorrect. Informatie over een bedrijf plaatsen maakt je nog geen expert in een bepaald onderwerp.
B) Correct. Het op sociale media beantwoorden (en actief beantwoorden) van vragen over een bepaald product kan aantonen dat uw bedrijf een expert is. Bron: White Paper – Privacy, Personal Data and the GDPR - § 8.6. Practice related applications of the use of data, marketing and social media.
C) Incorrect. Dat is alleen opscheppen hoe goed uw product is (en misschien is het dat niet).
D) Incorrect. Hieruit blijkt alleen dat u als bedrijf nieuwe producten ontwikkelt en ja, dat kan de verkopen verhogen, maar daardoor is uw bedrijf nog geen expert.

34 / 40
Er is een inbreuk op de beveiliging opgetreden in een informatiesysteem dat ook persoonsgegevens bevat.

Wat moet de verwerkingsverantwoordelijke als **eerste** doen?

A) Controleren of de inbreuk verlies of onrechtmatige verwerking van persoonsgegevens tot gevolg kan hebben gehad
B) Het risico op nadelige effecten voor de betrokkenen beoordelen middels een gegevensbeschermingseffectbeoordeling (DPIA)
C) Beoordelen of er onrechtmatig persoonsgegevens van gevoelige aard verwerkt (kunnen) zijn
D) De inbreuk onmiddellijk rapporteren aan de relevante toezichthoudende autoriteit

A) Correct. Bron: White Paper – Privacy, Personal Data and the GDPR - § 5.2 Procedures on how to act when a data breach occurs.
B) Incorrect. Er wordt een gegevensbeschermingseffectbeoordeling uitgevoerd bij het ontwerp van verwerkingen van persoonsgegevens.
C) Incorrect. De verwerkingsverantwoordelijke moet eerst achterhalen of het incident een inbreuk in verband met persoonsgegevens is die gemeld moet worden.
D) Incorrect. De verwerkingsverantwoordelijke moet eerst achterhalen of het incident een inbreuk in verband met persoonsgegevens is die gemeld moet worden.

35 / 40
Het woord 'privacy' komt niet voor in de AVG.

Wat is het verband tussen 'privacy' en 'gegevensbescherming'?

A) Gegevensbescherming is een verzameling regels en bepalingen over het verwerken van persoonsgegevens. Privacy is het resultaat van gegevensbescherming.
B) Privacy is het recht om tegen inmenging in persoonlijke aangelegenheden beschermd te worden. Gegevensbescherming is het middel om die bescherming te realiseren.
C) Privacy is het recht om persoonlijke aangelegenheden geheim te houden. Gegevensbescherming is het recht om persoonsgegevens geheim te houden.
D) De termen 'privacy' en 'gegevensbescherming' zijn uitwisselbaar. Er is geen relevant betekenisverschil.

A) Incorrect. Privacy is een recht, gegevensbescherming is een manier om dit te garanderen.
B) Correct. Bron: White Paper – Privacy, Personal Data and the GDPR - § 1.3 Definitions.
C) Incorrect. Privacy is een recht, gegevensbescherming is een manier om dit te garanderen.
D) Incorrect. Privacy is een recht, gegevensbescherming is een manier om dit te garanderen.

36 / 40
Verordening (EU) 2016/679, ook wel bekend als de AVG, herroept een eerdere EU-verordening.

Welke verordening wordt ingetrokken (vervangen)?

A) Verordening 2002/58/EG van 12 juli 2002
B) Verordening 2006/24/EG van 15 maart 2006
C) Verordening 95/46/EG van 24 oktober 1995
D) Verordening 97/66/EG van 15 december 1997

A) Incorrect. Verordening 2002/58/EG wijzigt sommige delen van verordening 97/66/EG bij amendement.
B) Incorrect. Deze verordening heeft betrekking op het bewaren van gegevens die bijvoorbeeld door internetproviders worden verzameld.
C) Correct. Deze vervanging wordt genoemd in de (sub)titel van de verordening. Bron: AVG.
D) Incorrect. Deze richtlijn is een aanvulling op richtlijn 95/46/EG om voor een gelijkwaardig niveau van bescherming van grondrechten en vrijheden in de lidstaten te zorgen.

37 / 40
Welk recht van betrokkenen wordt expliciet gedefinieerd in de AVG?

A) Er moet een kopie van de persoonsgegevens worden verstrekt in de door de betrokkene verzochte vorm.
B) Kosteloze toegang tot persoonsgegevens voor de betrokkene.
C) Persoonsgegevens moeten bij een verzoek daartoe van de betrokkene altijd gewijzigd worden.
D) Persoonsgegevens moeten altijd worden gewist als de betrokkene daarom vraagt.

A) Incorrect. De kopie moet worden aangeleverd in een gestructureerd, veelgebruikt en door machines verwerkbaar formaat, maar niet noodzakelijkerwijs in een door de betrokkene gespecificeerd formaat.
B) Correct. Maar alleen de eerste kopie hoeft gratis te worden verstrekt. Bron: EU GDPR, A pocket guide – Chapter 3 The Regulation – Data subjects' rights.
C) Incorrect. Alleen foutieve gegevens moeten worden gecorrigeerd.
D) Incorrect. In artikel 17 staan enkele uitzonderingen, bijvoorbeeld wanneer de gegevens nodig zijn om rechtsvorderingen vast te stellen, uit te oefenen of te verdedigen.

38 / 40
De AVG kenmerkt 'gevoelige persoonsgegevens' als een bijzondere categorie persoonsgegevens.

Wat is een voorbeeld van dergelijke gegevens?

A) Een afspraak in het ziekenhuis met een medisch specialist
B) Een internationaal bankrekeningnummer (IBAN)
C) Aanmelding voor een wetenschappelijk tijdschrift over politiek
D) Het lidmaatschap van een brancheverenigingen

A) Correct. Een afspraak met een medisch specialist is "persoonsgegevens betreffende de gezondheid". Zie AVG art. 9.1.
B) Incorrect. IBANs zijn gegevens die uniek gerelateerd zijn aan een persoon, dus persoonsgegevens. Maar geen gevoelige persoonsgegevens volgens AVG art. 9.
C) Incorrect. Een wetenschappelijk tijdschrift over politiek is geen 'persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen... blijken' en behoort dus niet tot gevoelige gegevens zoals gedefinieerd in artikel 9 van de AVG.
D) Incorrect. Alleen lidmaatschap van een vakbond en andere persoonsgegevens 'waaruit ... politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen... blijken' zijn gevoelige gegevens volgens artikel 9 van de AVG.

39 / 40
Welke rol in de gegevensbescherming bepaalt de doelen en middelen voor het verwerken van persoonsgegevens?

A) Verwerkingsverantwoordelijke
B) Functionaris voor gegevensbescherming
C) Verwerker

A) Correct. Verwerkingsverantwoordelijke: de natuurlijke of rechtspersoon, openbare instantie, agentschap of andere instantie die, alleen of samen met anderen, de doelen en middelen voor het verwerken van persoonsgegevens bepaalt. Bron: White Paper – Privacy, Personal Data and the GDPR - §1.4 Roles, responsibilities, stakeholders.
B) Incorrect.
C) Incorrect.

40 / 40
Welke informatie wordt in de AVG als persoonsgegevens beschouwd?

A) Informatie over een persoon die de privacy van die persoon kan schenden, ook al is de betreffende informatie onjuist
B) Alle informatie met betrekking tot een identificeerbare natuurlijke persoon
C) Informatie, over een identificeerbare natuurlijke persoon, die is gedigitaliseerd

A) Incorrect. Iedere uiting over een identificeerbare natuurlijke persoon valt onder de definitie van persoonsgegevens volgens de AVG.
B) Correct. Bron: EU GDPR, A pocket guide – Chapter 2 Term and definitions - Personal data & AVG art.4 (1).
C) Incorrect. Iedere uiting over een identificeerbare natuurlijke persoon valt onder de definitie van persoonsgegevens volgens de AVG.

Evaluatie

De juiste antwoorden op de vragen in dit voorbeeldexamen staan in de onderstaande tabel.

Vraag	Antwoord	Vraag	Antwoord
1	D	**21**	B
2	D	**22**	A
3	D	**23**	C
4	A	**24**	D
5	B	**25**	C
6	A	**26**	C
7	C	**27**	A
8	A	**28**	C
9	D	**29**	B
10	D	**30**	B
11	A	**31**	A
12	B	**32**	A
13	B	**33**	B
14	A	**34**	A
15	A	**35**	B
16	A	**36**	C
17	B	**37**	B
18	D	**38**	A
19	D	**39**	A
20	A	**40**	B

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER