Voorbeeldexamen

Editie 202009

Inhoud

Inleiding

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

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

Het maximaal aantal te behalen punten is 40. Elke goed beantwoorde vraag levert u 1 punt op. U hebt 26 punten of meer nodig om te slagen.

De beschikbare tijd is 120 minuten.

U mag de tekst van de AVG gebruiken tijdens dit examen.

Veel succes!

Voorbeeldexamen

1 / 40
Een bedrijf implementeert een privacybeleid, waardoor naleving van de AVG beter kan worden aangetoond. Het is om meerdere redenen raadzaam om dit beleid openbaar toegankelijk te maken.

Wat is de **belangrijkste** reden om het privacybeleid openbaar toegankelijk te maken?

A) Om klanten en partners de mogelijkheid te bieden te controleren welke persoonsgegevens de organisatie moet verwerken
B) Om klanten, partners en de toezichthoudende autoriteit de mogelijkheid te bieden te beoordelen hoe er met persoonsgegevens wordt omgegaan
C) Om het resultaat van de in de organisatie uitgevoerde gegevensbeschermingseffectbeoordelingen (DPIA's) te communiceren
D) Om de toezichthoudende autoriteit te informeren over de manier waarop de organisatie zal reageren na inbreuken in verband met persoonsgegevens

2 / 40
Welke informatie is onder de AVG **geen** verplicht onderdeel van een privacybeleid?

A) Informatie over de internationale doorgifte van persoonsgegevens aan een derde land
B) Informatie over de identiteit en contactgegevens van de verwerkingsverantwoordelijke
C) Informatie over maatregelen op het gebied van gegevensbeveiliging binnen de organisatie
D) Informatie over bewaartermijnen en de rechten van betrokkenen

3 / 40
De AVG onderschrijft de principes van privacy door ontwerp en door standaardinstellingen. Deze principes worden onder andere toegepast door zowel technische als organisatorische maatregelen te implementeren.

Waarom zijn organisatorische maatregelen noodzakelijk?

A) Omdat de organisatie voor privacy door ontwerp en door standaardinstellingen de toegang tot persoonsgegevens moet beperken tot uitsluitend verwerkingsverantwoordelijken
B) Omdat voor de bescherming van de rechten van betrokkenen organisatorische processen vereist zijn die niet onder de technische maatregelen kunnen vallen
C) Omdat de aanwijzing van een functionaris voor gegevensbescherming (FG), indien vereist, wordt beschouwd als een organisatorische maatregel

4 / 40
Een bedrijf werkt aan een project waarbij een nieuwe, gratis dienst voor consumenten wordt ontwikkeld.

Wat is volgens privacy door ontwerp de **meest** wenselijke tijd om gegevensbescherming te bespreken?

A) Direct vanaf het begin van het project
B) Tijdens de implementatiefase
C) Wanneer het project bijna is voltooid

5 / 40
Het opzetten van een managementsysteem voor gegevensbescherming (DPMS) gebeurt in fasen. De eerste fase voor de bouw van een DPMS is 'Data Protection and Privacy Preparation'. Een van de stappen in deze fase is 'Perform Initial Data Audits and Assessments'.

Waarom moeten deze gegevensaudits en -beoordelingen worden uitgevoerd in de fase 'Data Protection and Privacy Preparation' voor de bouw van een DPMS?

A) Omdat tijdens de gegevensaudits en -beoordelingen een analyse plaatsvindt van het bewustzijn en de gereedheid van personeel met betrekking tot gegevensbescherming en privacy
B) Omdat tijdens de gegevensaudits en -beoordelingen risico's met betrekking tot de naleving, mensen en andere gerelateerde risico's voor de organisatie worden vastgesteld
C) Omdat de gegevensaudits en -beoordelingen een duidelijk overzicht bieden van de huidige stromen van persoonsgegevens binnen en buiten de organisatie
D) Omdat met de gegevensaudits en -beoordelingen kan worden geïnventariseerd waar verschillende soorten persoonsgegevens zich binnen de organisatie bevinden

6 / 40
Een organisatie wil voldoen aan de AVG en bouwt daarom een managementsysteem voor gegevensbescherming (DPMS). De bouw van het DPMS bevindt zich in de eerste fase: 'Data Protection and Privacy Preparation'.

De functionaris voor gegevensbescherming (FG) heeft een conceptversie van een governance-structuur opgesteld, gegevensstromen bepaald, een inventarisatie van de persoonsgegevens gemaakt en alle drie de elementen van het gegevensbeschermings- en privacyprogramma bepaald (stap 7).

Wat is de **laatste** stap van de eerste fase voor de bouw van een DPMS?

A) De communicatie- en trainingsaspecten analyseren die het personeel nodig heeft met betrekking tot gegevensbescherming en privacy
B) Duidelijke rollen en verantwoordelijkheden definiëren in functieomschrijvingen en hieraan gerelateerde documenten, zoals de arbeidsovereenkomsten van privacymanagers en van een FG
C) Voor alle medewerkers die verantwoordelijk zijn voor gegevensbescherming en privacy een uitgebreid naslagwerk opstellen, zodat zij kunnen voldoen aan relevante wetgeving
D) Een rapportage over de tot dusver uitgevoerde stappen opstellen en dit indienen bij het bestuur van de organisatie, inclusief aanbevelingen voor actieplannen en een budget

7 / 40
Een bedrijf wil een managementsysteem voor gegevensbescherming (DPMS) bouwen. De eerste fase voor het bouwen van een DPMS is 'Data Protection and Privacy Preparation'.

Welke stap behoort **niet** tot deze eerste fase?

A) Het ontwikkelen van Draft Implementation Action Plans
B) Het opzetten van een Data Government Organization
C) Het bijhouden van gegevens en privacy documentatie
D) Het uitvoeren van initiële gegevensaudits en -beoordelingen

8 / 40
Een bedrijf wil een managementsysteem voor gegevensbescherming (DPMS) opzetten. De tweede fase voor de bouw van een DPMS is 'Data Protection and Privacy Organization'. Een van de stappen in fase 2 heeft de volgende doelstelling:

een op gegevensbescherming en privacy gerichte denkwijze integreren in het hele bedrijf en alle functies

Welke stap in fase 2 heeft deze doelstelling?

A) Een audit uitvoeren op de (beheers)maatregelen voor privacy en gegevensbescherming om hiaten en fouten aan het licht te brengen
B) De geautomatiseerde systemen voor gegevensbescherming en privacy implementeren en gebruiken
C) Medewerkers informeren over de status van het privacy- en gegevensbeschermingsprogramma
D) Regelmatig onderling communiceren over kwesties op het gebied van gegevensbescherming en privacy

9 / 40
Een functionaris voor gegevensbescherming (FG) beseft hoe belangrijk het is om regelmatig te communiceren met alle andere personen die zich bezighouden met en verantwoordelijk of verantwoordingsplichtig zijn voor gegevensbescherming en privacy. Deze groep personen moet voor gegevensbescherming en privacy streven naar een resultaat binnen de hele organisatie.

Bij welk resultaat heeft een organisatie het **meeste** baat?

A) Bij de ontwikkeling van een systeem waarin alle kwesties inzake gegevensbescherming en privacy moeten worden doorverwezen naar en vervolgens opgelost door de FG
B) Bij de ontwikkeling van uiteenlopende standpunten over gegevensbescherming en privacy terwijl gegevens in de organisatie worden uitbesteed of doorgegeven
C) Bij het stimuleren van een gezamenlijke en proactieve aanpak om gegevensbescherming en privacy te integreren in alle onderdelen van de organisatie
D) Bij een vergroting van het bewustzijn dat bij uitbesteding van gegevensbescherming en privacy een gedeelde verantwoordelijkheid en verantwoordingsplicht op het gebied van naleving ontstaat

10 / 40
Als een organisatie een managementsysteem voor gegevensbescherming (DPMS) wil ontwikkelen, implementeren en beheren, gebeurt dit in diverse fasen. De implementatie van het DPMS omvat vijf fasen waarin de volgende aspecten worden beschreven: voorbereiding, organisatie, ontwikkeling & implementatie, governance, en evaluatie & verbetering.

Waarmee kunnen de implementatiefasen voor een DPMS worden vergeleken?

A) Een constant verbeteringsproces, vergelijkbaar met de PDCA-cyclus
B) Een handleiding voor de implementatie van privacy-governance
C) Een inventarisatie van de regelgeving omtrent gegevens als voorbereiding op het DPMS
D) De impact van privacywetgeving, -regels en -normen

11 / 40
Een belangrijk aspect van de AVG is dat een organisatie naleving van de verordening moet kunnen aantonen. De implementatie van een managementsysteem voor gegevensbescherming (DPMS) kan helpen dit aan te tonen.

Welke fase voor de implementatie van een DPMS toont het **beste** aan dat de organisatie voldoet aan de AVG?

A) Fase 1, de organisatie treft voorbereidingen voor de implementatie van privacy en gegevensbescherming
B) Fase 2, de organisatorische structuren en mechanismen voor privacy worden vastgesteld
C) Fase 3, maatregelen voor gegevensbescherming en privacy worden ontwikkeld en geïmplementeerd
D) Fase 4, governance-mechanismen voor privacy worden vastgesteld voor de organisatie

12 / 40
Een functionaris voor gegevensbescherming (FG) ontwikkelt en implementeert een managementsysteem voor gegevensbescherming (DPMS). De implementatie bevindt zich in fase 3: 'Data Protection and Privacy Development and Implementation'.

Wat moet als **eerste** gebeuren in fase 3?

A) De behoeften en vereisten op het gebied van gegevensbescherming en privacy analyseren en definiëren voor het bedrijf
B) Onderzoeken in welke mate medewerkers al beschikken over kennis van en inzicht in de concepten voor gegevensbescherming en privacy
C) Onderzoek doen naar de best practices binnen de sector en deze aanpassen aan de behoeften en vereisten van het bedrijf
D) Inzicht krijgen in wereldwijde wetgeving op het gebied van gegevensbescherming en privacy, en de relevantie van die informatie bepalen

13 / 40
In een reactieplan voor inbreuken in verband met persoonsgegevens worden de volgende acties beschreven:

- Een **externe dienstverlener** reageert op de inbreuk, verleent PR-diensten en helpt de schade zo veel mogelijk te beperken
- De functionaris voor gegevensbescherming (**FG**) vraagt de toezichthoudende autoriteit om steun
- De **verwerker** brengt de zakelijke partners en betrokkenen op de hoogte van de inbreuk in verband met gegevens en vraagt hen om steun

Wie zal **hoogst waarschijnlijk** de impact voor derde partijen en betrokkenen het meest beperken?

A) De externe dienstverlener
B) De FG
C) De verwerker

14 / 40
Drie gezondheidsinstellingen ontwikkelen samen een mobiele app om patiënten te observeren. Het medisch personeel voegt eigen persoonsgegevens en kwalificaties toe aan de app, en patiënten voegen hun persoonsgegevens toe, inclusief medische gegevens.

De gezondheidsinstellingen benoemen één functionaris voor gegevensbescherming (FG). Om een pilot te kunnen uitvoeren, moet de app worden toegevoegd aan app-stores. Zodra dit is gebeurd, testen de gezondheidsinstellingen de beveiliging van de nieuwe app. Als veiligheidsmaatregel wordt in de beschrijving vermeld dat de app zich nog in een pilotfase bevindt. Slechts enkele testbetrokkenen downloaden de app, maar zij voeren wel echte gegevens in.

Uit de test blijkt dat de app helemaal niet veilig is en gemakkelijk kan worden gehackt. Hackers kunnen de gezondheidsgegevens van patiënten wijzigen en gegevens op ongeoorloofde manieren verzamelen en gebruiken.

Wat moet de FG onder de AVG doen?

A) De FG hoeft geen actie te ondernemen, omdat de app zich in een pilotfase bevindt waaraan slechts een klein aantal patiënten meedoet.
B) De FG hoeft geen actie te ondernemen, omdat de impact van de kwetsbaarheden in een pilotfase niet kan worden gekwalificeerd als een hoog risico.
C) De FG moet de patiënten en toezichthoudende autoriteit informeren, omdat de app een hoog risico vormt voor de rechten en vrijheden van de patiënten.
D) De FG moet de toezichthoudende autoriteit informeren en zorgen dat de beveiligingsmaatregelen van de app worden aangepast conform de vereiste beveiligingsnormen.

15 / 40
Om te voldoen aan de AVG kan het nuttig zijn om een systematische aanpak voor incidentmanagement te implementeren.

Wat zijn de hoofdlijnen van een effectief proces voor incidentmanagement?

A) Erkennen dat er zich een incident heeft voorgedaan, reageren op onmiddellijke aandachtspunten en aandachtspunten op lange termijn, en het incident blijven volgen om te waarborgen dat er effectieve stappen zijn ondernomen
B) Erkennen dat er zich een incident heeft voorgedaan en het incident melden aan de functionaris voor gegevensbescherming (FG), zodat gegevensstromen kunnen worden geëvalueerd en het beveiligingsbeleid kan worden verbeterd
C) Alle incidenten volgen waarbij persoonsgegevens betrokken zijn, een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren om de risico's te analyseren en een verbeterplan op te stellen
D) Alle gevallen volgen waarin persoonsgegevens worden verwerkt, zodat gegevens na een incident makkelijker kunnen worden opgevraagd, en zorgen dat responsmaatregelen kunnen worden beperkt om kosten zo laag mogelijk te houden.

16 / 40
De CEO heeft zijn privacyteam gevraagd de gegevensbeschermings- en privacyprestaties van de organisatie te evalueren. Een benchmark zou een goede manier zijn om objectief te bepalen hoe goed de organisatie presteert.

Wat valt **niet** onder de benchmark voor privacy?

A) Een onderzoek naar de klanttevredenheid met betrekking tot de privacy binnen de organisatie
B) Vergelijkingen tussen business-units of afdelingen met betrekking tot de naleving van privacy
C) De huidige privacyprestaties van de organisatie vergeleken met de prestaties van één jaar geleden
D) De privacyprestaties van de organisatie gemeten ten opzichte van de prestaties van gelijksoortige entiteiten in de sector

17 / 40
Een organisatie wil op de HR-afdeling kunstmatige intelligentie (AI) en deep learning-algoritmen gebruiken om arbeidsverhoudingen te beoordelen, bekwaamheidsprofielen op te stellen en bonussen voor individuele targets te bepalen.

Wat moet er **eerst** gebeuren, nog voordat deze nieuwe verwerkingsvorm voor persoonsgegevens wordt geïmplementeerd?

A) Een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren
B) Een privacybeoordeling van de HR-afdeling uitvoeren
C) De verwerking melden aan de toezichthoudende autoriteit

18 / 40
Welke activiteit is onder de AVG altijd een verantwoordelijkheid van de verwerkingsverantwoordelijke?

A) Zorg dragen voor de uitvoering van een gegevensbeschermingseffectbeoordeling (DPIA)
B) Een beveiligingsbedrijf inhuren voor de bescherming van doorgegeven persoonsgegevens
C) Een nieuwe methode implementeren om persoonsgegevens van klanten te verzamelen
D) Een register bijhouden van de verwerkingsactiviteiten die door de verwerker worden uitgevoerd

19 / 40
Een ziekenhuis besteedt het afdrukken van facturen voor patiënten uit aan een drukkerij. De drukkerij drukt ook facturen af voor andere organisaties.

Door een fout zijn namen en adressen tijdens het sorteren bij de drukkerij door elkaar gehaald en zijn er diverse facturen naar de verkeerde patiënten verstuurd.

Het ziekenhuis heeft de eigen processen zorgvuldig geanalyseerd. Het ziekenhuis beschikt over een solide verificatieproces en heeft contractuele overeenkomsten gesloten met de drukkerij.

Waarom zal het ziekenhuis toch **verantwoordelijk** worden gehouden door de toezichthoudende autoriteit?

A) Omdat dit zo wordt bepaald in de overeenkomst
B) Omdat het ziekenhuis de verwerkingsverantwoordelijke is
C) Omdat de fout betrekking heeft op patiënten
D) Omdat de verificatie fout is gelopen

20 / 40
Wanneer een verwerkingsverantwoordelijke en een verwerker een overeenkomst sluiten voor de verwerking van persoonsgegevens, hebben zij beide specifieke verantwoordelijkheden. Sommige van deze verantwoordelijkheden worden voorgeschreven door de AVG en andere kunnen in de overeenkomst worden vastgelegd.

Wanneer heeft de verwerker volgens de AVG altijd schriftelijke toestemming van de verwerkingsverantwoordelijke nodig?

A) Wanneer de verwerker een bedrijf inhuurt om gegevens tijdens doorgifte te beschermen
B) Wanneer de verwerker een derde inhuurt om persoonsgegevens te verwerken
C) Wanneer de verwerker een nieuwe methode implementeert om persoonsgegevens te verzamelen
D) Wanneer de verwerker een nieuwe methode implementeert om persoonsgegevens te verwijderen

21 / 40
Wie is wettelijk verplicht om een register van verwerkingsactiviteiten bij te houden?

A) De chief information officer
B) De chief privacy officer
C) De verwerkingsverantwoordelijke en verwerker
D) De functionaris voor gegevensbescherming (FG)

22 / 40
Een Noord-Amerikaanse organisatie die is gevestigd in de Europese Economische Ruimte (EER) verwerkt persoonsgegevens van natuurlijke personen. Hierbij worden op grote schaal gegevens over de etnische afkomst verwerkt.

Onder de AVG is een organisatie in drie specifieke gevallen verplicht om een functionaris voor gegevensbescherming (FG) te benoemen.

Waarom is deze organisatie in dit geval verplicht om een FG te benoemen?

A) Omdat de persoonsgegevens van buitenlandse personen worden verwerkt
B) Omdat de persoonsgegevens worden verwerkt in een derde land
C) Omdat de persoonsgegevens van minderheden worden verwerkt
D) Omdat er op grote schaal bijzondere categorieën van persoonsgegevens worden verwerkt

23 / 40
Een functionaris voor gegevensbescherming (FG) werkt voor het ministerie van Transport, een nationale dienst.

Er wordt een nieuw project aangekondigd om het rijgedrag van mensen op nationale snelwegen te observeren. Het ministerie wil gebruikmaken van een intelligent systeem voor videoanalyse om afzonderlijke auto's uit te lichten en kentekenplaten automatisch te herkennen.

De staatssecretaris wil graag snel van start gaan met het project en vreest dat privacykwesties mogelijk ongewenste vertragingen veroorzaken.

Wat moet de FG doen?

A) De staatssecretaris vragen om contact op te nemen met de toezichthoudende autoriteit, omdat dit duidelijk buiten het toepassingsgebied van de FG valt
B) De staatsecretaris verzekeren dat een DPIA niet nodig is als de betrokkenen worden geïnformeerd over de gegevensverwerking
C) De staatssecretaris laten weten dat een DPIA verplicht is voor de grootschalige observatie van een openbare ruimte
D) Er bij de staatssecretaris op aandringen het project te heroverwegen, omdat massale verwerking van surveillancegegevens verboden is

24 / 40
Functionarissen voor gegevensbescherming (FG's) zijn gehouden tot geheimhouding of vertrouwelijkheid met betrekking tot de uitvoering van hun taken.

In relatie tot welke partij is een FG **vrijgesteld** van deze geheimhouding of vertrouwelijkheid om deze partij om advies te kunnen vragen?

A) De raad van bestuur van het bedrijf
B) De teamleden van het gegevensbeschermings- en privacynetwerk
C) De functionaris voor informatiebeveiliging
D) De toezichthoudende autoriteit

25 / 40
Een gegevensbeschermingseffectbeoordeling (DPIA) is een instrument om risico's op het gebied van gegevensbescherming te herkennen, met name die risico's die waarschijnlijk sterk afbreuk doen aan de rechten en vrijheden van natuurlijke personen.

Waarom kan de DPIA worden gezien als onderdeel van het bredere risicomanagement van een organisatie?

A) Omdat bij een DPIA alle beveiligingsrisico's van de organisatie worden beoordeeld en hiermee elke andere vorm van risicobeoordeling of risicomanagement wordt vervangen
B) Omdat bij een DPIA risico's worden beoordeeld op hun waarschijnlijkheid en ernst, vergelijkbaar met andere goed gedefinieerde onderdelen van risicomanagement
C) Omdat een DPIA onder de AVG verplicht is voor elk project, waardoor alle andere wettelijke vereisten voor risicomanagement worden afgezwakt

26 / 40
Wat moet onder de AVG altijd onderdeel zijn van een gegevensbeschermingseffectbeoordeling (DPIA)?

A) Het ontwikkelen van een procedure voor inzageverzoeken van betrokkenen om naleving van de rechten van betrokkenen te waarborgen
B) Bepalen welke persoonsgegevens worden verwerkt en wat het voorgenomen doel van die verwerking is
C) De betrokkenen informeren dat er een beoordeling zal plaatsvinden en hun uitdrukkelijke toestemming vragen
D) Een reactieplan voor inbreuken in verband met persoonsgegevens opstellen en passende waarborgen definiëren om inbreuken in verband met gegevens te vermijden

27 / 40
Een organisatie ontwikkelt een nieuw product om te bepalen welke medewerkers ondermaats presteren. Door middel van kunstmatige intelligentie (AI) wordt gezocht in de browsergeschiedenis en wordt het werkgedrag geanalyseerd.

Hoewel de software-engineers het algoritme niet volledig begrijpen, besluit het management de 10% laagst scorende medewerkers te ontslaan.

De functionaris voor gegevensbescherming (FG) maakt zich zorgen over de impact van dit product en laat het bestuur weten dat er een gegevensbeschermingseffectbeoordeling (DPIA) vereist is.

Wat is **geen** onderdeel van de reden waarom een DPIA verplicht is?

A) De automatisering van de verwerking van persoonsgegevens
B) De evaluatie die mogelijk vergaande gevolgen heeft voor de betrokkenen
C) De verwerking van een bijzondere categorie van persoonsgegevens
D) De stelselmatige evaluatie van persoonlijke aspecten van natuurlijke personen

28 / 40
Wat is **geen** resultaat van een gegevensbeschermingseffectbeoordeling (DPIA)?

A) Een logboek met alle inzage van vertrouwelijke gegevens, inclusief een automatische toestemmingscontrole
B) Een register met de standpunten van betrokkenen aangaande de beoogde verwerkingsactiviteiten
C) Een systematische beschrijving van de beoogde verwerkingsactiviteiten
D) Een risicobeoordeling met betrekking tot de rechten en vrijheden van betrokkenen

29 / 40
In de AVG wordt beschreven wat de uitkomst van een gegevensbeschermingseffectbeoordeling (DPIA) minimaal moet omvatten.

Wat is **niet** verplicht in een DPIA?

A) Een beschrijving van de verwerking en de verwerkingsdoeleinden
B) Een beoordeling van de noodzaak en de evenredigheid van de verwerkingsactiviteiten met betrekking tot de doeleinden
C) Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen
D) Het advies van de toezichthoudende autoriteit

30 / 40
Uit een gegevensbeschermingseffectbeoordeling (DPIA) blijkt dat bij een beoogde verwerking meer gegevens over individuele klanten worden verzameld dan noodzakelijk is voor het beoogde doeleinde.

Wat is onder de AVG de **meest** passende reactie?

A) De gegevens zo snel mogelijk anonimiseren
B) Een trainings- en bewustzijnsprogramma invoeren
C) De periode beperken gedurende welke de gegevens worden opgeslagen
D) Minder gegevens verzamelen

31 / 40
Wat kan het beste **eerst** worden gedaan voorafgaand aan een gegevensbeschermingseffectbeoordeling (DPIA)?

A) Maatregelen bepalen om de gevonden risico's aan te pakken
B) Bepalen of het noodzakelijk is om een DPIA uit te voeren
C) De risico's voor de rechten en vrijheden van betrokkenen bepalen

32 / 40
Een bedrijf voert een gegevensbeschermingseffectbeoordeling (DPIA) uit.

Waarom is het voor een DPIA nuttig om gegevensstromen in kaart te brengen?

A) Omdat hiermee alle organisatorische risico's voor privacy worden beoordeeld
B) Omdat hiermee een overzicht wordt verkregen van de gebruikte persoonsgegevens
C) Omdat hiermee alle relevante partijen worden geïnformeerd

33 / 40
Een organisatie huurt een privacy-expert in. De organisatie wil gegevensverwerkingsactiviteiten gedeeltelijk gaan uitbesteden. De expert voert een gegevensbeschermingseffectbeoordeling (DPIA) uit voor de verwerking, waarbij een verwerker betrokken is.

Voor een van de belangrijkste stappen van een DPIA moet de verwerkingsverantwoordelijke alle input verstrekken en is betrokkenheid van de verwerker niet nodig.

Welke stap is dat?

A) Beoordeling van de noodzaak en evenredigheid van de verwerking
B) Beoordeling van de risico's voor de rechten en vrijheden van betrokkenen
C) Beperkende maatregelen om de risico's aan te pakken, inclusief waarborgen
D) Systematische beschrijvingen van de beoogde verwerkingsactiviteiten

34 / 40
Een groot bedrijf heeft het financieel moeilijk. Het bestuur wil dat medewerkers efficiënter gaan werken.

Het bestuur start een experiment waarbij de internetactiviteiten van medewerkers worden geobserveerd. De gegevens uit dit experiment worden geanalyseerd om na te gaan waar meer efficiëntie haalbaar is. Medewerkers die worden gecategoriseerd als *inefficiënt*, worden mogelijk ontslagen.

Waarom moet er een gegevensbeschermingseffectbeoordeling (DPIA) worden uitgevoerd voordat de nieuwe procedure wordt toegepast?

A) Omdat een groot bedrijf veel medewerkers heeft. De verwerking vindt daarom op grote schaal plaats.
B) Omdat dit een experiment is. Een DPIA is vereist voor nieuwe en experimentele verwerkingsactiviteiten.
C) Omdat dit stelselmatige monitoring is. De beslissingen hebben mogelijk vergaande gevolgen voor de medewerkers.

35 / 40
Een organisatie is van plan om geautomatiseerde besluitvorming toe te passen op klanten, waarbij gebruik wordt gemaakt van profilering.

Voor welk onderdeel van de gegevensbeschermingseffectbeoordeling (DPIA) is extra aandacht vereist?

A) De beoordeling van de noodzaak om een DPIA uit te voeren in verband met deze verwerkingsactiviteit
B) De maatregelen die worden geïmplementeerd om de rechten van betrokkenen te beschermen
C) De maatregelen om persoonsgegevens te beveiligen en zo te voorkomen dat ze door betrokkenen worden opgevraagd
D) De procedures om gegevens te wissen nadat een betrokkene heeft gevraagd om verwijdering van diens gegevens

36 / 40
Onder de AVG moeten organisaties zoeken naar manieren om inbreuken in verband met persoonsgegevens te voorkomen. Daarom is het belangrijk om incidenten die kunnen worden geclassificeerd als inbreuken in verband met persoonsgegevens snel te herkennen.

Welk incident vormt onder de AVG **geen** inbreuk in verband met persoonsgegevens?

A) Een patiënt verwacht een pakketje met medische apparatuur, maar het pakketje wordt bezorgd op het verkeerde adres.
B) Een medewerker bij een geestelijke gezondheidsinstelling is een aantal patiëntendossiers kwijt en kan deze niet terugvinden.
C) Persoonsgegevens worden per ongeluk vernietigd door een brand of aardbeving in een datawarehouse
D) Vertrouwelijke financiële bedrijfsgegevens met betrekking tot een beoogde overname worden ongeoorloofd bekendgemaakt

37 / 40
In welke situatie is het verplicht om een inbreuk in verband met persoonsgegevens te melden aan de toezichthoudende autoriteit?

A) Als de organisatie het incident niet kan oplossen binnen 72 uur nadat het zich heeft voorgedaan
B) In elke situatie waarin sprake is van een beveiligingsbedreiging voor de rechten en vrijheden van natuurlijke personen
C) Alleen als het incident binnen 72 uur wordt erkend als een inbreuk in verband met persoonsgegevens
D) Altijd, behalve wanneer het onwaarschijnlijk is dat de inbreuk een risico vormt voor de rechten en vrijheden van natuurlijke personen

38 / 40
Het hoofd van een HR-afdeling is een geheugenstick kwijt waarop de persoonsgegevens van 35 medewerkers staan. De geheugenstick is beschermd met sterke versleuteling. De HR-afdeling heeft deze persoonsgegevens ook op een back-upapparaat staan.

Is het onder de AVG verplicht om deze inbreuk in verband met persoonsgegevens te melden aan de toezichthoudende autoriteit?

A) Ja, want alle beveiligingsincidenten moeten worden gemeld aan de toezichthoudende autoriteit.
B) Ja, want door de melding kan de toezichthoudende autoriteit de medewerkers informeren.
C) Nee, want het is geen gerechtvaardigd belang van het bedrijf om inbreuken in verband met gegevens te melden.
D) Nee, want deze inbreuk in verband met persoonsgegevens vormt geen risico voor de rechten van de betrokkenen.

39 / 40
In welke situatie moet onder de AVG een inbreuk in verband met persoonsgegevens worden gemeld aan de getroffen betrokkenen?

A) Wanneer een inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico vormt voor de rechten en vrijheden van de betrokkenen
B) Wanneer de toezichthoudende autoriteit heeft vastgesteld dat toestemming de enige rechtsgrond voor verwerking was
C) Wanneer er een beveiligingsincident plaatsvindt dat binnen 72 uur wordt geclassificeerd als een inbreuk in verband met persoonsgegevens
D) Wanneer persoonsgegevens in het gedrang komen door externe factoren zoals hackers of andere cybercriminelen

40 / 40
In het best practice reactieproces voor inbreuken in verband met persoonsgegevens worden de fasen Voorbereiding, Reactie en Follow-up gedefinieerd. Voor elke fase is documentatie van essentieel belang.

In de Reactie-fase is het belangrijk om bewijs te verzamelen en bewaren, zodat kan worden aangetoond waarom een incident zich voordeed en waarom de organisatie het incident niet kon voorkomen.

Wat moet er worden verzameld en bewaard?

A) Auditcontroleplannen
B) Gegevensbeschermingseffectbeoordelingen (DPIA's)
C) Bewijs om een duidelijk beeld te schetsen
D) Systeemherstelplannen

Antwoordsleutel

1 / 40
Een bedrijf implementeert een privacybeleid, waardoor naleving van de AVG beter kan worden aangetoond. Het is om meerdere redenen raadzaam om dit beleid openbaar toegankelijk te maken.

Wat is de **belangrijkste** reden om het privacybeleid openbaar toegankelijk te maken?

A) Om klanten en partners de mogelijkheid te bieden te controleren welke persoonsgegevens de organisatie moet verwerken
B) Om klanten, partners en de toezichthoudende autoriteit de mogelijkheid te bieden te beoordelen hoe er met persoonsgegevens wordt omgegaan
C) Om het resultaat van de in de organisatie uitgevoerde gegevensbeschermingseffectbeoordelingen (DPIA's) te communiceren
D) Om de toezichthoudende autoriteit te informeren over de manier waarop de organisatie zal reageren na inbreuken in verband met persoonsgegevens

A) Incorrect. Een openbaar toegankelijk privacybeleid bepaalt niet welke persoonsgegevens door de organisatie moet worden verwerkt. Het biedt transparantie over de verwerking van persoonsgegevens.
B) Correct. Een openbaar toegankelijk beleid ondersteunt de transparantie, biedt klanten en partners de mogelijkheid om het beleid te beoordelen, en vormt een duidelijke verklaring op basis waarvan toezichthoudende autoriteiten en andere regelgevingsinstanties de organisatie kunnen beoordelen. (Literatuur: A, Hoofdstuk 16)
C) Incorrect. De resultaten van DPIA's moeten worden gedocumenteerd voor interne raadpleging en hoeven niet te worden opgenomen in het privacybeleid.
D) Incorrect. De manier waarop de organisatie reageert op een inbreuk in verband met gegevens is onderdeel van het reactieplan voor inbreuken in verband met persoonsgegevens. Dat is een intern document dat niet openbaar beschikbaar hoeft te zijn.

2 / 40
Welke informatie is onder de AVG **geen** verplicht onderdeel van een privacybeleid?

A) Informatie over de internationale doorgifte van persoonsgegevens aan een derde land
B) Informatie over de identiteit en contactgegevens van de verwerkingsverantwoordelijke
C) Informatie over maatregelen op het gebied van gegevensbeveiliging binnen de organisatie
D) Informatie over bewaartermijnen en de rechten van betrokkenen

A) Incorrect. Dit is verplicht.
B) Incorrect. Dit is verplicht.
C) Correct. Dit is onderdeel van een beleid voor informatiebeveiliging. (Literatuur: A, Hoofdstuk 16; Artikel 13 van de AVG)
D) Incorrect. Dit is verplicht.

3 / 40
De AVG onderschrijft de principes van privacy door ontwerp en door standaardinstellingen. Deze principes worden onder andere toegepast door zowel technische als organisatorische maatregelen te implementeren.

Waarom zijn organisatorische maatregelen noodzakelijk?

A) Omdat de organisatie voor privacy door ontwerp en door standaardinstellingen de toegang tot persoonsgegevens moet beperken tot uitsluitend verwerkingsverantwoordelijken
B) Omdat voor de bescherming van de rechten van betrokkenen organisatorische processen vereist zijn die niet onder de technische maatregelen kunnen vallen
C) Omdat de aanwijzing van een functionaris voor gegevensbescherming (FG), indien vereist, wordt beschouwd als een organisatorische maatregel

A) Incorrect. Organisatorische maatregelen zijn bedoeld om de rechten van betrokkenen te beschermen en bestaan uit procedures voor behoorlijke en transparante verwerking.
B) Correct. Sommige interne processen en procedures moeten met organisatorische maatregelen worden aangepakt om te kunnen garanderen dat de rechten van betrokkenen volledig kunnen worden uitgeoefend conform de AVG. Technische tools en systemen vormen een aanvulling op de organisatorische maatregelen, maar zijn geen vervanging hiervan. (Literatuur: A, Hoofdstuk 9)
C) Incorrect. Organisatorische maatregelen zijn bedoeld om de rechten van betrokkenen te beschermen en bestaan uit procedures voor behoorlijke en transparante verwerking.

4 / 40
Een bedrijf werkt aan een project waarbij een nieuwe, gratis dienst voor consumenten wordt ontwikkeld.

Wat is volgens privacy door ontwerp de **meest** wenselijke tijd om gegevensbescherming te bespreken?

A) Direct vanaf het begin van het project
B) Tijdens de implementatiefase
C) Wanneer het project bijna is voltooid

A) Correct. Privacy- en gegevensbescherming moeten direct vanaf het begin van het project worden gepromoot, conform het principe van privacy door ontwerp. (Literatuur: A, Hoofdstuk 5; F)
B) Incorrect. Het is te laat om gegevensbescherming pas in de implementatiefase te bespreken.
C) Incorrect. Het is te laat om gegevensbescherming pas in de voltooiingsfase van het project te bespreken.

5 / 40
Het opzetten van een managementsysteem voor gegevensbescherming (DPMS) gebeurt in fasen. De eerste fase voor de bouw van een DPMS is 'Data Protection and Privacy Preparation'. Een van de stappen in deze fase is 'Perform Initial Data Audits and Assessments'.

Waarom moeten deze gegevensaudits en -beoordelingen worden uitgevoerd in de fase 'Data Protection and Privacy Preparation' voor de bouw van een DPMS?

A) Omdat tijdens de gegevensaudits en -beoordelingen een analyse plaatsvindt van het bewustzijn en de gereedheid van personeel met betrekking tot gegevensbescherming en privacy
B) Omdat tijdens de gegevensaudits en -beoordelingen risico's met betrekking tot de naleving, mensen en andere gerelateerde risico's voor de organisatie worden vastgesteld
C) Omdat de gegevensaudits en -beoordelingen een duidelijk overzicht bieden van de huidige stromen van persoonsgegevens binnen en buiten de organisatie
D) Omdat met de gegevensaudits en -beoordelingen kan worden geïnventariseerd waar verschillende soorten persoonsgegevens zich binnen de organisatie bevinden

A) Incorrect. Gegevensaudits en -beoordelingen zijn niet bedoeld om het bewustzijn en de gereedheid van personeel met betrekking tot gegevensbescherming en privacy te analyseren.
B) Correct. Met gegevensaudits en -beoordelingen in deze fase worden risico's met betrekking tot de naleving, personen en andere gerelateerde risico's vastgesteld. Het resultaat biedt een eerste inzicht in de zaken waar het DPMS aandacht aan moet besteden. (Literatuur: B, Hoofdstuk 2.2.1)
C) Incorrect. Gegevensaudits en -beoordelingen worden niet gebruikt om inzicht te krijgen in de gegevensstromen binnen en buiten de organisatie.
D) Incorrect. Gegevensaudits en -beoordelingen worden niet gebruikt om de locatie van soorten gegevens binnen de organisatie te inventariseren, maar om risico's vast te stellen.

6 / 40
Een organisatie wil voldoen aan de AVG en bouwt daarom een managementsysteem voor gegevensbescherming (DPMS). De bouw van het DPMS bevindt zich in de eerste fase: 'Data Protection and Privacy Preparation'.

De functionaris voor gegevensbescherming (FG) heeft een conceptversie van een governance-structuur opgesteld, gegevensstromen bepaald, een inventarisatie van de persoonsgegevens gemaakt en alle drie de elementen van het gegevensbeschermings- en privacyprogramma bepaald (stap 7).

Wat is de **laatste** stap van de eerste fase voor de bouw van een DPMS?

A) De communicatie- en trainingsaspecten analyseren die het personeel nodig heeft met betrekking tot gegevensbescherming en privacy
B) Duidelijke rollen en verantwoordelijkheden definiëren in functieomschrijvingen en hieraan gerelateerde documenten, zoals de arbeidsovereenkomsten van privacymanagers en van een FG
C) Voor alle medewerkers die verantwoordelijk zijn voor gegevensbescherming en privacy een uitgebreid naslagwerk opstellen, zodat zij kunnen voldoen aan relevante wetgeving
D) Een rapportage over de tot dusver uitgevoerde stappen opstellen en dit indienen bij het bestuur van de organisatie, inclusief aanbevelingen voor actieplannen en een budget

A) Incorrect. Dit is een van de drie elementen van het gegevensbeschermings- en privacyprogramma dat al in stap 7 aan bod kwam.
B) Incorrect. Deze stap wordt veel later gezet, namelijk in stap 4 van fase 2.
C) Incorrect. Dit is de eerste stap die in fase 2 moet worden gezet.
D) Correct. Dit is de laatste stap die in de eerste fase moet worden gezet. (Literatuur: B, Hoofdstuk 2.2.1)

7 / 40
Een bedrijf wil een managementsysteem voor gegevensbescherming (DPMS) bouwen. De eerste fase voor het bouwen van een DPMS is 'Data Protection and Privacy Preparation'.

Welke stap behoort **niet** tot deze eerste fase?

A) Het ontwikkelen van Draft Implementation Action Plans
B) Het opzetten van een Data Government Organization
C) Het bijhouden van gegevens en privacy documentatie
D) Het uitvoeren van initiële gegevensaudits en -beoordelingen

A) Incorrect. Deze stap is onderdeel van de eerste fase.
B) Incorrect. Deze stap is onderdeel van de eerste fase.
C) Correct. Deze stap hoort bij fase 4: Data Protection and Privacy Governance. De eerste fase bestaat uit de volgende stappen: conduct privacy analysis, collect privacy laws, analyze privacy impact, perform initial data audits and assessments, establish data governance organization, establish data flows and personal data inventory, establish data protection and privacy program, develop data protection and privacy implementation action plans. (Literatuur: B, Hoofdstuk 2.2)
D) Incorrect. Deze stap is onderdeel van de eerste fase.

8 / 40
Een bedrijf wil een managementsysteem voor gegevensbescherming (DPMS) opzetten. De tweede fase voor de bouw van een DPMS is 'Data Protection and Privacy Organization'. Een van de stappen in fase 2 heeft de volgende doelstelling:

een op gegevensbescherming en privacy gerichte denkwijze integreren in het hele bedrijf en alle functies

Welke stap in fase 2 heeft deze doelstelling?

A) Een audit uitvoeren op de (beheers)maatregelen voor privacy en gegevensbescherming om hiaten en fouten aan het licht te brengen
B) De geautomatiseerde systemen voor gegevensbescherming en privacy implementeren en gebruiken
C) Medewerkers informeren over de status van het privacy- en gegevensbeschermingsprogramma
D) Regelmatig onderling communiceren over kwesties op het gebied van gegevensbescherming en privacy

A) Incorrect. Deze audit kan pas plaatsvinden na de volledige implementatie en is het resultaat van fase 5.
B) Incorrect. Dit is een technische maatregel om de integriteit van gegevens te waarborgen, geen culturele maatregel om een op gegevensbescherming en privacy gerichte denkwijze te integreren in het hele bedrijf en alle functies.
C) Incorrect. Hoewel het belangrijk is dat medewerkers weten wat de status van het programma is, is dergelijke communicatie niet voldoende om iedereen erbij te betrekken en een op gegevensbescherming en privacy gerichte denkwijze effectief te integreren in het hele bedrijf en alle functies.
D) Correct. Constante, regelmatige communicatie is onmisbaar om de strategie voor gegevensbescherming en privacy effectief te implementeren in alle activiteiten van het bedrijf. (Literatuur: B, Hoofdstuk 2.2.2)

9 / 40
Een functionaris voor gegevensbescherming (FG) beseft hoe belangrijk het is om regelmatig te communiceren met alle andere personen die zich bezighouden met en verantwoordelijk of verantwoordingsplichtig zijn voor gegevensbescherming en privacy. Deze groep personen moet voor gegevensbescherming en privacy streven naar een resultaat binnen de hele organisatie.

Bij welk resultaat heeft een organisatie het **meeste** baat?

A) Bij de ontwikkeling van een systeem waarin alle kwesties inzake gegevensbescherming en privacy moeten worden doorverwezen naar en vervolgens opgelost door de FG
B) Bij de ontwikkeling van uiteenlopende standpunten over gegevensbescherming en privacy terwijl gegevens in de organisatie worden uitbesteed of doorgegeven
C) Bij het stimuleren van een gezamenlijke en proactieve aanpak om gegevensbescherming en privacy te integreren in alle onderdelen van de organisatie
D) Bij een vergroting van het bewustzijn dat bij uitbesteding van gegevensbescherming en privacy een gedeelde verantwoordelijkheid en verantwoordingsplicht op het gebied van naleving ontstaat

A) Incorrect. In plaats van alle problemen op het gebied van gegevensbescherming en privacy uitsluitend over te laten aan de FG, zou het bedrijf er meer baat bij hebben als de regelmatige communicatie onder alle werknemers een cultuurverandering rondom gegevensbescherming en privacy zou stimuleren.
B) Incorrect. In plaats van uiteenlopende standpunten inzake gegevensbescherming en privacy binnen het bedrijf, zou het bedrijf er meer baat bij hebben als de regelmatige communicatie zou leiden tot een gemeenschappelijk standpunt dat is afgestemd op de missieverklaring voor privacy.
C) Correct. Door regelmatig te communiceren met alle andere personen binnen de organisatie die verantwoordelijk en verantwoordingsplichtig zijn voor gegevensbescherming en privacy, krijgt iedereen meer inzicht in de scenario's en uitdagingen van elke afdeling. Ook kunnen zo beter ideeën en suggesties worden uitgewisseld om privacy en gegevensbescherming te integreren in alle systemen, diensten, producten en lopende projecten. (Literatuur: B, Hoofdstuk 2.2.2)
D) Incorrect. Zelfs als de activiteiten of taken worden uitbesteed, zou het bedrijf er meer baat bij hebben als de regelmatige communicatie ertoe zou leiden dat alle medewerkers begrijpen dat zij een verantwoordelijkheid en verantwoordingsplicht hebben als het gaat om de gegevensbescherming en privacy van informatie waarover zij beschikken.

10 / 40
Als een organisatie een managementsysteem voor gegevensbescherming (DPMS) wil ontwikkelen, implementeren en beheren, gebeurt dit in diverse fasen. De implementatie van het DPMS omvat vijf fasen waarin de volgende aspecten worden beschreven: voorbereiding, organisatie, ontwikkeling & implementatie, governance, en evaluatie & verbetering.

Waarmee kunnen de implementatiefasen voor een DPMS worden vergeleken?

A) Een constant verbeteringsproces, vergelijkbaar met de PDCA-cyclus
B) Een handleiding voor de implementatie van privacy-governance
C) Een inventarisatie van de regelgeving omtrent gegevens als voorbereiding op het DPMS
D) De impact van privacywetgeving, -regels en -normen

A) Correct. De implementatiefasen voor een DPMS beschrijven een continu verbeteringsproces, vergelijkbaar met de PDCA-cyclus. (Literatuur: A, Hoofdstuk 1; B, Hoofdstuk 2)
B) Incorrect. Dit verwijst naar fase 4 van het opzetten van een DPMS.
C) Incorrect. Dit is slechts een gedeeltelijke beschrijving van stap 2 van fase 1 (de voorbereidingsfase).
D) Incorrect. Dit is slechts een gedeeltelijke beschrijving van stap 3 van fase 1.

11 / 40
Een belangrijk aspect van de AVG is dat een organisatie naleving van de verordening moet kunnen aantonen. De implementatie van een managementsysteem voor gegevensbescherming (DPMS) kan helpen dit aan te tonen.

Welke fase voor de implementatie van een DPMS toont het **beste** aan dat de organisatie voldoet aan de AVG?

A) Fase 1, de organisatie treft voorbereidingen voor de implementatie van privacy en gegevensbescherming
B) Fase 2, de organisatorische structuren en mechanismen voor privacy worden vastgesteld
C) Fase 3, maatregelen voor gegevensbescherming en privacy worden ontwikkeld en geïmplementeerd
D) Fase 4, governance-mechanismen voor privacy worden vastgesteld voor de organisatie

A) Incorrect. In deze fase wordt de implementatie voorbereid, maar de fase omvat nog geen enkele vorm van naleving.
B) Incorrect. Deze fase vormt de basis voor de implementatie van privacyvereisten, maar toont op zich nog geen naleving aan.
C) Correct. Met de implementatie van procedures, beleid en beheersmaatregelen wordt naleving aangetoond. (Literatuur: B, Hoofdstuk 2.2; Artikel 24(1) van de AVG)
D) Incorrect. Deze fase is belangrijk om te blijven voldoen aan de AVG, maar hiervoor is eerst implementatie vereist.

12 / 40
Een functionaris voor gegevensbescherming (FG) ontwikkelt en implementeert een managementsysteem voor gegevensbescherming (DPMS). De implementatie bevindt zich in fase 3: 'Data Protection and Privacy Development and Implementation'.

Wat moet als **eerste** gebeuren in fase 3?

A) De behoeften en vereisten op het gebied van gegevensbescherming en privacy analyseren en definiëren voor het bedrijf
B) Onderzoeken in welke mate medewerkers al beschikken over kennis van en inzicht in de concepten voor gegevensbescherming en privacy
C) Onderzoek doen naar de best practices binnen de sector en deze aanpassen aan de behoeften en vereisten van het bedrijf
D) Inzicht krijgen in wereldwijde wetgeving op het gebied van gegevensbescherming en privacy, en de relevantie van die informatie bepalen

A) Correct. De functionaris moest als eerste actie de behoeften en vereisten van het bedrijf begrijpen en definiëren, zodat hij de doelen en doelstellingen kan bepalen voor de gegevensbeschermings- en privacystrategieën, -plannen en -beleid. (Literatuur: B, Hoofdstuk 2.2)
B) Incorrect. Dit onderzoek moet pas plaatsvinden nadat de behoeften en vereisten van het bedrijf zijn geanalyseerd en gedefinieerd.
C) Incorrect. Best practices binnen de sector kunnen pas worden aangepast aan het bedrijf nadat de behoeften en vereisten van het bedrijf zijn geanalyseerd en gedefinieerd.
D) Incorrect. De relevantie van informatie kan pas worden bepaald nadat de behoeften en vereisten van het bedrijf zijn geanalyseerd en gedefinieerd.

13 / 40
In een reactieplan voor inbreuken in verband met persoonsgegevens worden de volgende acties beschreven:

- Een **externe dienstverlener** reageert op de inbreuk, verleent PR-diensten en helpt de schade zo veel mogelijk te beperken
- De functionaris voor gegevensbescherming (**FG**) vraagt de toezichthoudende autoriteit om steun
- De **verwerker** brengt de zakelijke partners en betrokkenen op de hoogte van de inbreuk in verband met gegevens en vraagt hen om steun

Wie zal **hoogst waarschijnlijk** de impact voor derde partijen en betrokkenen het meest beperken?

A) De externe dienstverlener
B) De FG
C) De verwerker

A) Correct. De externe partij levert diensten die helpen om snel te reageren op een inbreuk in verband met persoonsgegevens en de impact voor derde partijen en betrokkenen te beperken. (Literatuur: B, Hoofdstuk 2)
B) Incorrect. De FG moet informatie verstrekken en de toezichthoudende autoriteit ondersteunen, niet andersom.
C) Incorrect. Verwerkers zijn niet wettelijk verplicht om zakelijke partners op de hoogte te brengen van een inbreuk in verband met gegevens. Bovendien moeten betrokkenen alleen op de hoogte worden gebracht (1) wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen, en (2) door de verwerkingsverantwoordelijke, niet door de verwerker.

14 / 40
Drie gezondheidsinstellingen ontwikkelen samen een mobiele app om patiënten te observeren. Het medisch personeel voegt eigen persoonsgegevens en kwalificaties toe aan de app, en patiënten voegen hun persoonsgegevens toe, inclusief medische gegevens.

De gezondheidsinstellingen benoemen één functionaris voor gegevensbescherming (FG). Om een pilot te kunnen uitvoeren, moet de app worden toegevoegd aan app-stores. Zodra dit is gebeurd, testen de gezondheidsinstellingen de beveiliging van de nieuwe app. Als veiligheidsmaatregel wordt in de beschrijving vermeld dat de app zich nog in een pilotfase bevindt. Slechts enkele testbetrokkenen downloaden de app, maar zij voeren wel echte gegevens in.

Uit de test blijkt dat de app helemaal niet veilig is en gemakkelijk kan worden gehackt. Hackers kunnen de gezondheidsgegevens van patiënten wijzigen en gegevens op ongeoorloofde manieren verzamelen en gebruiken.

Wat moet de FG onder de AVG doen?

A) De FG hoeft geen actie te ondernemen, omdat de app zich in een pilotfase bevindt waaraan slechts een klein aantal patiënten meedoet.
B) De FG hoeft geen actie te ondernemen, omdat de impact van de kwetsbaarheden in een pilotfase niet kan worden gekwalificeerd als een hoog risico.
C) De FG moet de patiënten en toezichthoudende autoriteit informeren, omdat de app een hoog risico vormt voor de rechten en vrijheden van de patiënten.
D) De FG moet de toezichthoudende autoriteit informeren en zorgen dat de beveiligingsmaatregelen van de app worden aangepast conform de vereiste beveiligingsnormen.

A) Incorrect. Het aantal betrokkenen is niet relevant. De kwalificatie als hoog risico voor de rechten en vrijheden van natuurlijke personen bepaalt welke acties er moeten worden genomen.
B) Incorrect. Een pilotfase is geen excuus om gegevens bloot te stellen aan risico's.
C) Correct. De verwerkingsverantwoordelijke heeft onvoldoende maatregelen genomen om de veiligheid van de gegevens te waarborgen. Het risico geldt voor een bijzondere categorie van persoonsgegevens. Daarom moeten zowel de toezichthoudende autoriteit als de betrokkenen op de hoogte worden gebracht. (Literatuur: A, Hoofdstuk 14; Artikel 33(1) en Artikel 34(1) van de AVG)
D) Incorrect. Dit zijn allebei verstandige acties. De AVG beschrijft echter wel de melding aan de betrokkenen maar niet dat de beveiligingsmaatregelen moeten worden aangepast.

15 / 40
Om te voldoen aan de AVG kan het nuttig zijn om een systematische aanpak voor incidentmanagement te implementeren.

Wat zijn de hoofdlijnen van een effectief proces voor incidentmanagement?

A) Erkennen dat er zich een incident heeft voorgedaan, reageren op onmiddellijke aandachtspunten en aandachtspunten op lange termijn, en het incident blijven volgen om te waarborgen dat er effectieve stappen zijn ondernomen
B) Erkennen dat er zich een incident heeft voorgedaan en het incident melden aan de functionaris voor gegevensbescherming (FG), zodat gegevensstromen kunnen worden geëvalueerd en het beveiligingsbeleid kan worden verbeterd
C) Alle incidenten volgen waarbij persoonsgegevens betrokken zijn, een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren om de risico's te analyseren en een verbeterplan op te stellen
D) Alle gevallen volgen waarin persoonsgegevens worden verwerkt, zodat gegevens na een incident makkelijker kunnen worden opgevraagd, en zorgen dat responsmaatregelen kunnen worden beperkt om kosten zo laag mogelijk te houden.

A) Correct. Dit is een globale omschrijving van het incidentmanagementproces. (Literatuur: A, Hoofdstuk 14)
B) Incorrect. Incidenten moeten worden gemeld aan het verantwoordelijke personeel. De FG hoeft niet na elk incident de gegevensstromen te evalueren.
C) Incorrect. Er hoeft niet na elk incident een DPIA te worden uitgevoerd.
D) Incorrect. Het is ineffectief om alle gevallen te volgen waarin persoonsgegevens worden verwerkt. Bovendien ontbreken in dit antwoord de stappen om te reageren op een incident en om te waarborgen dat die stappen effectief werden genomen.

16 / 40
De CEO heeft zijn privacyteam gevraagd de gegevensbeschermings- en privacyprestaties van de organisatie te evalueren. Een benchmark zou een goede manier zijn om objectief te bepalen hoe goed de organisatie presteert.

Wat valt **niet** onder de benchmark voor privacy?

A) Een onderzoek naar de klanttevredenheid met betrekking tot de privacy binnen de organisatie
B) Vergelijkingen tussen business-units of afdelingen met betrekking tot de naleving van privacy
C) De huidige privacyprestaties van de organisatie vergeleken met de prestaties van één jaar geleden
D) De privacyprestaties van de organisatie gemeten ten opzichte van de prestaties van gelijksoortige entiteiten in de sector

A) Correct. Bij een benchmark wordt de huidige situatie van het bedrijf vergeleken met de situatie in eerdere perioden of binnen de sector. In dit geval wordt er niets vergeleken. Bovendien zijn niet alle klanten op de hoogte van best practices op het gebied van privacy, of hebben zij niet te maken gehad met de diverse privacypraktijken van de organisatie. (Literatuur: B, Hoofdstuk 2.2.5)
B) Incorrect. De privacy-benchmark helpt wel om vergelijkingen te maken tussen verschillende business-units of afdelingen met betrekking tot de naleving van privacy.
C) Incorrect. Een privacy-benchmark kan ook worden gebruikt als een soort zelfbeoordeling om resultaten te vergelijken met eerdere beoordelingen en zo verbeteringen of mogelijke aandachtspunten te herkennen.
D) Incorrect. Benchmarking is een objectieve methode om de privacyprestaties van de organisatie te vergelijken met gelijksoortige entiteiten in de sector en met best practices.

17 / 40
Een organisatie wil op de HR-afdeling kunstmatige intelligentie (AI) en deep learning-algoritmen gebruiken om arbeidsverhoudingen te beoordelen, bekwaamheidsprofielen op te stellen en bonussen voor individuele targets te bepalen.

Wat moet er **eerst** gebeuren, nog voordat deze nieuwe verwerkingsvorm voor persoonsgegevens wordt geïmplementeerd?

A) Een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren
B) Een privacybeoordeling van de HR-afdeling uitvoeren
C) De verwerking melden aan de toezichthoudende autoriteit

A) Correct. Bij de verwerking wordt een nieuwe profileringstechnologie gebruikt die waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen, aangezien de technologie een significante invloed kan hebben op hun werkgedrag, -activiteiten en -beloningen. (Literatuur: A, Hoofdstuk 5; Artikel 35 van de AVG)
B) Incorrect. Beoordelingen of business-units voldoen aan het privacybeleid worden periodiek en onaangekondigd uitgevoerd, niet tijdens de implementatie van een nieuwe verwerkingsvorm.
C) Incorrect. Dit vindt plaats nadat er een DPIA is uitgevoerd, en alleen onder bepaalde omstandigheden.

18 / 40
Welke activiteit is onder de AVG altijd een verantwoordelijkheid van de verwerkingsverantwoordelijke?

A) Zorg dragen voor de uitvoering van een gegevensbeschermingseffectbeoordeling (DPIA)
B) Een beveiligingsbedrijf inhuren voor de bescherming van doorgegeven persoonsgegevens
C) Een nieuwe methode implementeren om persoonsgegevens van klanten te verzamelen
D) Een register bijhouden van de verwerkingsactiviteiten die door de verwerker worden uitgevoerd

A) Correct. De verantwoordelijkheid voor DPIA's ligt bij de verwerkingsverantwoordelijke en mag niet worden uitbesteed aan een verwerker. (Literatuur: A, Hoofdstuk 12; Artikel 35 van de AVG)
B) Incorrect. Dit kan ook een verantwoordelijkheid van de verwerker zijn, op voorwaarde dat hiervoor voorafgaande schriftelijke toestemming is gegeven.
C) Incorrect. Dit kan ook een verantwoordelijkheid van de verwerker zijn, op voorwaarde dat hiervoor voorafgaande schriftelijke toestemming is gegeven.
D) Incorrect. Dit is een verantwoordelijkheid van de verwerker. De verwerkingsverantwoordelijke houdt een register bij van de verwerkingsactiviteiten die de verwerkingsverantwoordelijke zelf beheerst.

19 / 40
Een ziekenhuis besteedt het afdrukken van facturen voor patiënten uit aan een drukkerij. De drukkerij drukt ook facturen af voor andere organisaties.

Door een fout zijn namen en adressen tijdens het sorteren bij de drukkerij door elkaar gehaald en zijn er diverse facturen naar de verkeerde patiënten verstuurd.

Het ziekenhuis heeft de eigen processen zorgvuldig geanalyseerd. Het ziekenhuis beschikt over een solide verificatieproces en heeft contractuele overeenkomsten gesloten met de drukkerij.

Waarom zal het ziekenhuis toch **verantwoordelijk** worden gehouden door de toezichthoudende autoriteit?

A) Omdat dit zo wordt bepaald in de overeenkomst
B) Omdat het ziekenhuis de verwerkingsverantwoordelijke is
C) Omdat de fout betrekking heeft op patiënten
D) Omdat de verificatie fout is gelopen

A) Incorrect. Het ziekenhuis is verantwoordelijk omdat het als verwerkingsverantwoordelijke gehouden is aan het verantwoordingsbeginsel, zoals vastgelegd in de AVG.
B) Correct. Uit de AVG: “De verwerkingsverantwoordelijke is verantwoordelijk […], lid 1 (‘verantwoordingsplicht’)” voor de rechtmatigheid van de verwerking. De verwerkingsverantwoordelijke wordt door de toezichthoudende autoriteit verantwoordelijk en verantwoordingsplichtig gehouden, ongeacht de overeenkomst die de verwerkingsverantwoordelijke en de verwerker met elkaar hebben gesloten. De verwerkingsverantwoordelijke mag uitsluitend gebruikmaken van verwerkers die voldoende garanties bieden dat zij passende technische en organisatorische maatregelen implementeren. (Literatuur: A, Hoofdstuk 12; Artikel 5(2) van de AVG)
C) Incorrect. Het maakt niet uit dat de betrokkenen allemaal tot dezelfde verwerkingsverantwoordelijke behoren. Hier is alleen relevant wie de verwerkingsverantwoordelijke is.
D) Incorrect. Niets wijst erop dat de verificatie fout is gelopen. De toezichthoudende autoriteit houdt altijd de verwerkingsverantwoordelijke verantwoordelijk.

20 / 40
Wanneer een verwerkingsverantwoordelijke en een verwerker een overeenkomst sluiten voor de verwerking van persoonsgegevens, hebben zij beide specifieke verantwoordelijkheden. Sommige van deze verantwoordelijkheden worden voorgeschreven door de AVG en andere kunnen in de overeenkomst worden vastgelegd.

Wanneer heeft de verwerker volgens de AVG altijd schriftelijke toestemming van de verwerkingsverantwoordelijke nodig?

A) Wanneer de verwerker een bedrijf inhuurt om gegevens tijdens doorgifte te beschermen
B) Wanneer de verwerker een derde inhuurt om persoonsgegevens te verwerken
C) Wanneer de verwerker een nieuwe methode implementeert om persoonsgegevens te verzamelen
D) Wanneer de verwerker een nieuwe methode implementeert om persoonsgegevens te verwijderen

A) Incorrect. Dit aspect wordt (mogelijk) door de verwerker bepaald conform de overeenkomst, aangezien dit niet duidelijk wordt gedefinieerd in de AVG.
B) Correct. Op deze manier een andere verwerker in dienst nemen is niet toegestaan zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. (Literatuur: A, Hoofdstuk 12; Artikel 28(2) van de AVG)
C) Incorrect. Dit aspect wordt (mogelijk) door de verwerker bepaald conform de overeenkomst, aangezien dit niet duidelijk wordt gedefinieerd in de AVG.
D) Incorrect. Dit aspect wordt (mogelijk) door de verwerker bepaald conform de overeenkomst, aangezien dit niet duidelijk wordt gedefinieerd in de AVG.

21 / 40
Wie is wettelijk verplicht om een register van verwerkingsactiviteiten bij te houden?

A) De chief information officer
B) De chief privacy officer
C) De verwerkingsverantwoordelijke en verwerker
D) De functionaris voor gegevensbescherming (FG)

A) Incorrect. De chief information officer draagt de algehele verantwoordelijkheid voor informatietechnologie en informatiemanagement.
B) Incorrect. De chief privacy officer moet binnen de organisatie betrokkenheid bij naleving van de AVG genereren.
C) Correct. Zowel de verwerkingsverantwoordelijke als de verwerker zijn verplicht om een register van alle verwerkingsactiviteiten bij te houden. (Literatuur: A, Hoofdstuk 12; Artikel 30 van de AVG)
D) Incorrect. Hoewel de FG in de praktijk vaak inventarisaties uitvoert, een register van verwerkingsactiviteiten bijhoudt en de verantwoordelijkheid krijgt om deze gegevens te onderhouden, gebeurt dit onder de wettelijke verplichting van de verwerkingsverantwoordelijke of de verwerker.

22 / 40
Een Noord-Amerikaanse organisatie die is gevestigd in de Europese Economische Ruimte (EER) verwerkt persoonsgegevens van natuurlijke personen. Hierbij worden op grote schaal gegevens over de etnische afkomst verwerkt.

Onder de AVG is een organisatie in drie specifieke gevallen verplicht om een functionaris voor gegevensbescherming (FG) te benoemen.

Waarom is deze organisatie in dit geval verplicht om een FG te benoemen?

A) Omdat de persoonsgegevens van buitenlandse personen worden verwerkt
B) Omdat de persoonsgegevens worden verwerkt in een derde land
C) Omdat de persoonsgegevens van minderheden worden verwerkt
D) Omdat er op grote schaal bijzondere categorieën van persoonsgegevens worden verwerkt

A) Incorrect. Dit is niet een van de drie basisvoorwaarden in de AVG.
B) Incorrect. Dit is niet een van de drie basisvoorwaarden in de AVG.
C) Incorrect. Dit is niet een van de drie basisvoorwaarden in de AVG.
D) Correct. Dit is een van de gevallen die in de AVG wordt beschreven, waarbij de kerntaak van de verwerkingsverantwoordelijke of de verwerker bestaat uit de grootschalige verwerking van bijzondere categorieën van gegevens overeenkomstig Artikel 9. Gegevens met betrekking tot ras of etnische afkomst worden nadrukkelijk genoemd in Artikel 9 van de AVG. De andere twee voorwaarden zijn: (1) de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken, (2) de verwerking vereist regelmatige en stelselmatige observatie op grote schaal van betrokkenen. Deze drie basisvoorwaarden gelden voor zowel verwerkingsverantwoordelijken als verwerkers. (Literatuur: A, Hoofdstuk 2; Artikel 9 en Artikel 37 van de AVG)

23 / 40
Een functionaris voor gegevensbescherming (FG) werkt voor het ministerie van Transport, een nationale dienst.

Er wordt een nieuw project aangekondigd om het rijgedrag van mensen op nationale snelwegen te observeren. Het ministerie wil gebruikmaken van een intelligent systeem voor videoanalyse om afzonderlijke auto's uit te lichten en kentekenplaten automatisch te herkennen.

De staatssecretaris wil graag snel van start gaan met het project en vreest dat privacykwesties mogelijk ongewenste vertragingen veroorzaken.

Wat moet de FG doen?

A) De staatssecretaris vragen om contact op te nemen met de toezichthoudende autoriteit, omdat dit duidelijk buiten het toepassingsgebied van de FG valt
B) De staatsecretaris verzekeren dat een DPIA niet nodig is als de betrokkenen worden geïnformeerd over de gegevensverwerking
C) De staatssecretaris laten weten dat een DPIA verplicht is voor de grootschalige observatie van een openbare ruimte
D) Er bij de staatssecretaris op aandringen het project te heroverwegen, omdat massale verwerking van surveillancegegevens verboden is

A) Incorrect. Een FG moet voldoende gekwalificeerd zijn om dit te bespreken.
B) Incorrect. Door betrokkenen te informeren wordt een organisatie niet vrijgesteld van de verantwoordelijkheid om een DPIA uit te voeren.
C) Correct. Dit project vraagt om systematische en grootschalige observatie van een openbaar toegankelijke ruimte, en dat is een van de drie verplichte scenario's voor het uitvoeren van een DPIA. (Literatuur: A, Hoofdstuk 5; Artikel 35(3)(c) van de AVG)
D) Incorrect. Observatie, surveillance en profilering zijn niet verboden, op voorwaarde dat de rechten en vrijheden van mensen voldoende worden beschermd.

24 / 40
Functionarissen voor gegevensbescherming (FG's) zijn gehouden tot geheimhouding of vertrouwelijkheid met betrekking tot de uitvoering van hun taken.

In relatie tot welke partij is een FG **vrijgesteld** van deze geheimhouding of vertrouwelijkheid om deze partij om advies te kunnen vragen?

A) De raad van bestuur van het bedrijf
B) De teamleden van het gegevensbeschermings- en privacynetwerk
C) De functionaris voor informatiebeveiliging
D) De toezichthoudende autoriteit

A) Incorrect. De bestuursleden zijn weliswaar gemakkelijk toegankelijk, maar dat wil nog niet zeggen dat de FG hun om advies moet vragen. De FG heeft een onafhankelijke rol.
B) Incorrect. De teamleden van het gegevensbeschermings- en privacynetwerk zijn weliswaar makkelijk toegankelijk, maar dat wil nog niet zeggen dat de FG hun om advies moet vragen.
C) Incorrect. De functionaris voor informatiebeveiliging is weliswaar gemakkelijk toegankelijk, maar dat wil nog niet zeggen dat de FG de functionaris om advies moet vragen.
D) Correct. De geheimhoudings- en/of vertrouwelijkheidsplicht belet de FG niet om contact op te nemen met de toezichthoudende autoriteit en deze om advies te vragen. (Literatuur: A, Hoofdstuk 2; Artikel 36 en Artikel 39(1)(e) van de AVG)

25 / 40
Een gegevensbeschermingseffectbeoordeling (DPIA) is een instrument om risico's op het gebied van gegevensbescherming te herkennen, met name die risico's die waarschijnlijk sterk afbreuk doen aan de rechten en vrijheden van natuurlijke personen.

Waarom kan de DPIA worden gezien als onderdeel van het bredere risicomanagement van een organisatie?

A) Omdat bij een DPIA alle beveiligingsrisico's van de organisatie worden beoordeeld en hiermee elke andere vorm van risicobeoordeling of risicomanagement wordt vervangen
B) Omdat bij een DPIA risico's worden beoordeeld op hun waarschijnlijkheid en ernst, vergelijkbaar met andere goed gedefinieerde onderdelen van risicomanagement
C) Omdat een DPIA onder de AVG verplicht is voor elk project, waardoor alle andere wettelijke vereisten voor risicomanagement worden afgezwakt

A) Incorrect. Bij een DPIA wordt uitsluitend gekeken naar de beschermings- en privacyrisico's van persoonsgegevens.
B) Correct. Dit is het juiste verband tussen een DPIA en risicomanagement. (Literatuur: A, Hoofdstuk 2; Overweging 90 voor de AVG)
C) Incorrect. Een DPIA is niet altijd vereist en maakt de noodzaak van andere vormen van risicomanagement niet minder groot.

26 / 40
Wat moet onder de AVG altijd onderdeel zijn van een gegevensbeschermingseffectbeoordeling (DPIA)?

A) Het ontwikkelen van een procedure voor inzageverzoeken van betrokkenen om naleving van de rechten van betrokkenen te waarborgen
B) Bepalen welke persoonsgegevens worden verwerkt en wat het voorgenomen doel van die verwerking is
C) De betrokkenen informeren dat er een beoordeling zal plaatsvinden en hun uitdrukkelijke toestemming vragen
D) Een reactieplan voor inbreuken in verband met persoonsgegevens opstellen en passende waarborgen definiëren om inbreuken in verband met gegevens te vermijden

A) Incorrect. Dit is een mogelijke maatregel op basis van het resultaat van een DPIA.
B) Correct. Elke DPIA moet beginnen met een beschrijving van de beoogde verwerking en de verwerkingsdoeleinden. (Literatuur: A, Hoofdstuk 8; Artikel 35(7)(a) van de AVG)
C) Incorrect. Om een DPIA uit te voeren is geen toestemming vereist.
D) Incorrect. Dit is een mogelijke maatregel op basis van het resultaat van een DPIA.

27 / 40
Een organisatie ontwikkelt een nieuw product om te bepalen welke medewerkers ondermaats presteren. Door middel van kunstmatige intelligentie (AI) wordt gezocht in de browsergeschiedenis en wordt het werkgedrag geanalyseerd.

Hoewel de software-engineers het algoritme niet volledig begrijpen, besluit het management de 10% laagst scorende medewerkers te ontslaan.

De functionaris voor gegevensbescherming (FG) maakt zich zorgen over de impact van dit product en laat het bestuur weten dat er een gegevensbeschermingseffectbeoordeling (DPIA) vereist is.

Wat is **geen** onderdeel van de reden waarom een DPIA verplicht is?

A) De automatisering van de verwerking van persoonsgegevens
B) De evaluatie die mogelijk vergaande gevolgen heeft voor de betrokkenen
C) De verwerking van een bijzondere categorie van persoonsgegevens
D) De stelselmatige evaluatie van persoonlijke aspecten van natuurlijke personen

A) Incorrect. Dit is een reden waarom een DPIA verplicht is.
B) Incorrect. Dit is een reden waarom een DPIA verplicht is.
C) Correct. Hoewel het systeem wel persoonsgegevens verzamelt, worden deze gegevens niet beschouwd als een bijzondere gegevenscategorie. (Literatuur: A, Hoofdstuk 8; Artikel 35 van de AVG)
D) Incorrect. Dit is een reden waarom een DPIA verplicht is.

28 / 40
Wat is **geen** resultaat van een gegevensbeschermingseffectbeoordeling (DPIA)?

A) Een logboek met alle inzage van vertrouwelijke gegevens, inclusief een automatische toestemmingscontrole
B) Een register met de standpunten van betrokkenen aangaande de beoogde verwerkingsactiviteiten
C) Een systematische beschrijving van de beoogde verwerkingsactiviteiten
D) Een risicobeoordeling met betrekking tot de rechten en vrijheden van betrokkenen

A) Correct. Dit is geen resultaat van een DPIA, maar een constante activiteit in het kader van de informatiebeveiliging. (Literatuur: A, Hoofdstuk 8 en 3; Artikel 35 van de AVG)
B) Incorrect. Dit is een mogelijk resultaat van de DPIA.
C) Incorrect. Dit is een mogelijk resultaat van de DPIA.
D) Incorrect. Dit is een mogelijk resultaat van de DPIA.

29 / 40
In de AVG wordt beschreven wat de uitkomst van een gegevensbeschermingseffectbeoordeling (DPIA) minimaal moet omvatten.

Wat is **niet** verplicht in een DPIA?

A) Een beschrijving van de verwerking en de verwerkingsdoeleinden
B) Een beoordeling van de noodzaak en de evenredigheid van de verwerkingsactiviteiten met betrekking tot de doeleinden
C) Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen
D) Het advies van de toezichthoudende autoriteit

A) Incorrect. Dit is een verplicht onderdeel van de DPIA.
B) Incorrect. Dit is een verplicht onderdeel van de DPIA.
C) Incorrect. Dit is een verplicht onderdeel van de DPIA.
D) Correct. Het is niet altijd verplicht om de toezichthoudende autoriteit te raadplegen, en het is ook niet verplicht om een verslag van het advies op te nemen in de DPIA. (Literatuur: A, Hoofdstuk 5; Artikel 35(7) en Artikel 36(1) van de AVG)

30 / 40
Uit een gegevensbeschermingseffectbeoordeling (DPIA) blijkt dat bij een beoogde verwerking meer gegevens over individuele klanten worden verzameld dan noodzakelijk is voor het beoogde doeleinde.

Wat is onder de AVG de **meest** passende reactie?

A) De gegevens zo snel mogelijk anonimiseren
B) Een trainings- en bewustzijnsprogramma invoeren
C) De periode beperken gedurende welke de gegevens worden opgeslagen
D) Minder gegevens verzamelen

A) Incorrect. Hiermee wordt het risico beperkt, maar dit neemt niet weg dat de onnodige gegevens niet mogen worden verwerkt.
B) Incorrect. Hiermee wordt het risico beperkt, maar dit neemt niet weg dat de onnodige gegevens niet mogen worden verwerkt.
C) Incorrect. Hiermee wordt het risico beperkt, maar dit neemt niet weg dat de onnodige gegevens niet mogen worden verwerkt.
D) Correct. Hiermee wordt het principe van minimale gegevensverwerking geïmplementeerd en nemen de risico's voor betrokkenen af. (Literatuur: A, Hoofdstuk 8; Artikel 5(1) van de AVG)

31 / 40
Wat kan het beste **eerst** worden gedaan voorafgaand aan een gegevensbeschermingseffectbeoordeling (DPIA)?

A) Maatregelen bepalen om de gevonden risico's aan te pakken
B) Bepalen of het noodzakelijk is om een DPIA uit te voeren
C) De risico's voor de rechten en vrijheden van betrokkenen bepalen

A) Incorrect. Dit is onderdeel van een DPIA en moet worden gedaan nadat de noodzaak van de DPIA is bepaald.
B) Correct. De organisatie moet bepalen of het wettelijk vereist is om een DPIA uit te voeren of dat de behoeften van de organisatie hierom vragen. (Literatuur: A, Hoofdstuk 5; Artikel 35(7) van de AVG)
C) Incorrect. Dit is onderdeel van een DPIA en moet worden gedaan nadat de noodzaak van de DPIA is bepaald.

32 / 40
Een bedrijf voert een gegevensbeschermingseffectbeoordeling (DPIA) uit.

Waarom is het voor een DPIA nuttig om gegevensstromen in kaart te brengen?

A) Omdat hiermee alle organisatorische risico's voor privacy worden beoordeeld
B) Omdat hiermee een overzicht wordt verkregen van de gebruikte persoonsgegevens
C) Omdat hiermee alle relevante partijen worden geïnformeerd

A) Incorrect. Bij het in kaart brengen van gegevensstromen worden geen risico's beoordeeld.
B) Correct. Bij het in kaart brengen van gegevensstromen worden de gebruikte gegevens bepaald. Met vastgestelde gegevensstromen kan beter worden bepaald welke potentiële risico's moeten worden beoordeeld. (Literatuur: A, Hoofdstuk 7)
C) Incorrect. Het in kaart brengen van gegevensstromen wordt niet gebruikt om partijen te informeren.

33 / 40
Een organisatie huurt een privacy-expert in. De organisatie wil gegevensverwerkingsactiviteiten gedeeltelijk gaan uitbesteden. De expert voert een gegevensbeschermingseffectbeoordeling (DPIA) uit voor de verwerking, waarbij een verwerker betrokken is.

Voor een van de belangrijkste stappen van een DPIA moet de verwerkingsverantwoordelijke alle input verstrekken en is betrokkenheid van de verwerker niet nodig.

Welke stap is dat?

A) Beoordeling van de noodzaak en evenredigheid van de verwerking
B) Beoordeling van de risico's voor de rechten en vrijheden van betrokkenen
C) Beperkende maatregelen om de risico's aan te pakken, inclusief waarborgen
D) Systematische beschrijvingen van de beoogde verwerkingsactiviteiten

A) Correct. Dit is de verantwoordelijkheid van de verwerkingsverantwoordelijke en hierbij hoeft de verwerker niet te worden betrokken. (Literatuur: A, Hoofdstuk 12)
B) Incorrect. Input van de verwerker met betrekking tot mogelijke risico's is vereist.
C) Incorrect. Input met betrekking tot de genomen beperkende maatregelen door de verwerker is vereist.
D) Incorrect. Voor een volledige beschrijving is input van de verwerker nodig.

34 / 40
Een groot bedrijf heeft het financieel moeilijk. Het bestuur wil dat medewerkers efficiënter gaan werken.

Het bestuur start een experiment waarbij de internetactiviteiten van medewerkers worden geobserveerd. De gegevens uit dit experiment worden geanalyseerd om na te gaan waar meer efficiëntie haalbaar is. Medewerkers die worden gecategoriseerd als *inefficiënt*, worden mogelijk ontslagen.

Waarom moet er een gegevensbeschermingseffectbeoordeling (DPIA) worden uitgevoerd voordat de nieuwe procedure wordt toegepast?

A) Omdat een groot bedrijf veel medewerkers heeft. De verwerking vindt daarom op grote schaal plaats.
B) Omdat dit een experiment is. Een DPIA is vereist voor nieuwe en experimentele verwerkingsactiviteiten.
C) Omdat dit stelselmatige monitoring is. De beslissingen hebben mogelijk vergaande gevolgen voor de medewerkers.

A) Incorrect. De grote schaal is mogelijk wel van invloed, maar is op zich geen criterium. Observatie op grote schaal in een openbare ruimte zou wel een criterium zijn. Het bedrijf is echter geen openbare ruimte.
B) Incorrect. Het maakt niet uit of het gaat om een experiment of een gewone verwerkingsactiviteit.
C) Correct. Dit wordt gedefinieerd als een van de drie gevallen waarin een DPIA verplicht is. (Literatuur: A, Hoofdstuk 5; Artikel 35(3)(b) van de AVG)

35 / 40
Een organisatie is van plan om geautomatiseerde besluitvorming toe te passen op klanten, waarbij gebruik wordt gemaakt van profilering.

Voor welk onderdeel van de gegevensbeschermingseffectbeoordeling (DPIA) is extra aandacht vereist?

A) De beoordeling van de noodzaak om een DPIA uit te voeren in verband met deze verwerkingsactiviteit
B) De maatregelen die worden geïmplementeerd om de rechten van betrokkenen te beschermen
C) De maatregelen om persoonsgegevens te beveiligen en zo te voorkomen dat ze door betrokkenen worden opgevraagd
D) De procedures om gegevens te wissen nadat een betrokkene heeft gevraagd om verwijdering van diens gegevens

A) Incorrect. Voor verwerkingsactiviteiten waarbij geautomatiseerde besluitvorming komt kijken (inclusief profilering), is altijd een DPIA vereist.
B) Correct. De risico's die geautomatiseerde besluitvorming met zich meebrengt, vragen om speciale aandacht. Er moet zorgvuldig worden beschreven hoe het risico kan worden beperkt. Dit kan bijvoorbeeld door menselijke tussenkomst toe te staan. (Literatuur: A, Hoofdstuk 5; Artikel 35 van de AVG)
C) Incorrect. Gegevens moeten in het algemeen worden beveiligd, maar betrokkenen hebben wel recht van inzage.
D) Incorrect. Dit is wel een onderdeel van een DPIA, maar vraagt op zich niet om specifieke aandacht in het geval van geautomatiseerde besluitvorming.

36 / 40
Onder de AVG moeten organisaties zoeken naar manieren om inbreuken in verband met persoonsgegevens te voorkomen. Daarom is het belangrijk om incidenten die kunnen worden geclassificeerd als inbreuken in verband met persoonsgegevens snel te herkennen.

Welk incident vormt onder de AVG **geen** inbreuk in verband met persoonsgegevens?

A) Een patiënt verwacht een pakketje met medische apparatuur, maar het pakketje wordt bezorgd op het verkeerde adres.
B) Een medewerker bij een geestelijke gezondheidsinstelling is een aantal patiëntendossiers kwijt en kan deze niet terugvinden.
C) Persoonsgegevens worden per ongeluk vernietigd door een brand of aardbeving in een datawarehouse
D) Vertrouwelijke financiële bedrijfsgegevens met betrekking tot een beoogde overname worden ongeoorloofd bekendgemaakt

A) Incorrect. Dit is een inbreuk in verband met persoonsgegevens waarbij het gaat om een bijzondere categorie van persoonsgegevens.
B) Incorrect. Onopzettelijk verlies van alle persoonsgegevens (en vooral van een bijzondere categorie van persoonsgegevens) wordt ook beschouwd als een inbreuk in verband met persoonsgegevens.
C) Incorrect. Zelfs als het incident wordt veroorzaakt door een natuurramp of overmacht, moet dit worden beschouwd als een inbreuk in verband met persoonsgegevens.
D) Correct. Dit is wel een inbreuk in verband met gegevens, maar er zijn geen persoonsgegevens in het gedrang gekomen. Het gaat dus niet om een inbreuk in verband met persoonsgegevens. (Literatuur: A, Hoofdstuk 3; Artikel 4(12) van de AVG)

37 / 40
In welke situatie is het verplicht om een inbreuk in verband met persoonsgegevens te melden aan de toezichthoudende autoriteit?

A) Als de organisatie het incident niet kan oplossen binnen 72 uur nadat het zich heeft voorgedaan
B) In elke situatie waarin sprake is van een beveiligingsbedreiging voor de rechten en vrijheden van natuurlijke personen
C) Alleen als het incident binnen 72 uur wordt erkend als een inbreuk in verband met persoonsgegevens
D) Altijd, behalve wanneer het onwaarschijnlijk is dat de inbreuk een risico vormt voor de rechten en vrijheden van natuurlijke personen

A) Incorrect. De periode waarbinnen het incident wordt opgelost, is niet van belang.
B) Incorrect. Een dreiging is niet genoeg. Melding is alleen verplicht wanneer er zich een inbreuk in verband met persoonsgegevens heeft voorgedaan die waarschijnlijk een risico vormt voor de rechten en vrijheden van natuurlijke personen.
C) Incorrect. Binnen het incidentmanagementproces wordt het incident mogelijk niet binnen 72 uur herkend. In de AVG staat dat inbreuken in verband met persoonsgegevens "onverwijld en waar mogelijk niet meer dan 72 uur nadat er kennis van is genomen" moeten worden gemeld.
D) Correct. De toezichthoudende autoriteit moet op de hoogte worden gebracht van incidenten met persoonsgegevens, tenzij het onwaarschijnlijk is dat deze een risico vormen voor de rechten en vrijheden van natuurlijke personen. (Literatuur: A, Hoofdstuk 14; Artikel 33(1) van de AVG)

38 / 40
Het hoofd van een HR-afdeling is een geheugenstick kwijt waarop de persoonsgegevens van 35 medewerkers staan. De geheugenstick is beschermd met sterke versleuteling. De HR-afdeling heeft deze persoonsgegevens ook op een back-upapparaat staan.

Is het onder de AVG verplicht om deze inbreuk in verband met persoonsgegevens te melden aan de toezichthoudende autoriteit?

A) Ja, want alle beveiligingsincidenten moeten worden gemeld aan de toezichthoudende autoriteit.
B) Ja, want door de melding kan de toezichthoudende autoriteit de medewerkers informeren.
C) Nee, want het is geen gerechtvaardigd belang van het bedrijf om inbreuken in verband met gegevens te melden.
D) Nee, want deze inbreuk in verband met persoonsgegevens vormt geen risico voor de rechten van de betrokkenen.

A) Incorrect. Alleen inbreuken in verband met persoonsgegevens die een hoog risico vormen voor de rechten van de betrokkenen, moeten worden gemeld. Hoewel het een goede gewoonte kan zijn om alle inbreuken in verband met persoonsgegevens te melden en zo te voorkomen dat de wet wordt overtreden, is dit niet verplicht.
B) Incorrect. De rechten van de betrokkenen lopen geen risico, dus hoeven de betrokkenen niet te worden geïnformeerd. Het is ook niet de taak van de toezichthoudende autoriteit om betrokkenen te informeren.
C) Incorrect. Het gerechtvaardigde belang van het bedrijf is een geldige rechtsgrond voor verwerking. Het heeft niets te maken met inbreuken in verband met persoonsgegevens en de manier waarop deze moeten worden gemeld.
D) Correct. De krachtige versleuteling en back-up zijn voldoende om de vertrouwelijkheid en beschikbaarheid van de persoonsgegevens te waarborgen. Daarom vormt deze inbreuk in verband met gegevens waarschijnlijk geen risico voor de rechten en vrijheden van natuurlijke personen. Het is niet verplicht om deze inbreuk te melden bij de toezichthoudende autoriteit. (Literatuur: A, Hoofdstuk 14; Artikel 33(1) van de AVG)

39 / 40
In welke situatie moet onder de AVG een inbreuk in verband met persoonsgegevens worden gemeld aan de getroffen betrokkenen?

A) Wanneer een inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico vormt voor de rechten en vrijheden van de betrokkenen
B) Wanneer de toezichthoudende autoriteit heeft vastgesteld dat toestemming de enige rechtsgrond voor verwerking was
C) Wanneer er een beveiligingsincident plaatsvindt dat binnen 72 uur wordt geclassificeerd als een inbreuk in verband met persoonsgegevens
D) Wanneer persoonsgegevens in het gedrang komen door externe factoren zoals hackers of andere cybercriminelen

A) Correct. Betrokkenen moeten op de hoogte worden gebracht als de inbreuk in verband met persoonsgegevens een hoog risico vormt voor hun rechten en vrijheden. (Literatuur: A, Hoofdstuk 14; Artikel 34(1) van de AVG)
B) Incorrect. Alleen inbreuken in verband met persoonsgegevens die een hoog risico vormen, moeten ook worden gemeld aan de betrokkenen.
C) Incorrect. Die 72 uur zijn het tijdsbestek waarbinnen de inbreuk in verband met persoonsgegevens moet worden gemeld aan de toezichthoudende autoriteit. Niet alle inbreuken in verband met persoonsgegevens moeten aan de betrokkenen worden gemeld.
D) Incorrect. De melding is niet afhankelijk van de onderliggende oorzaak voor de inbreuk in verband met persoonsgegevens.

40 / 40
In het best practice reactieproces voor inbreuken in verband met persoonsgegevens worden de fasen Voorbereiding, Reactie en Follow-up gedefinieerd. Voor elke fase is documentatie van essentieel belang.

In de Reactie-fase is het belangrijk om bewijs te verzamelen en bewaren, zodat kan worden aangetoond waarom een incident zich voordeed en waarom de organisatie het incident niet kon voorkomen.

Wat moet er worden verzameld en bewaard?

A) Auditcontroleplannen
B) Gegevensbeschermingseffectbeoordelingen (DPIA's)
C) Bewijs om een duidelijk beeld te schetsen
D) Systeemherstelplannen

A) Incorrect. Er wordt geen auditcontroleplan gedocumenteerd in het reactieproces voor inbreuken in verband met persoonsgegevens.
B) Incorrect. Er wordt geen DPIA gedocumenteerd in het reactieproces voor inbreuken in verband met persoonsgegevens.
C) Correct. Gedurende het hele reactieproces voor inbreuken in verband met persoonsgegevens moet er bewijs worden verzameld en bewaard om een duidelijk beeld te schetsen van wat er is gebeurd en waarom de organisatie het incident niet kon voorkomen. (Literatuur: A, Hoofdstuk 14)
D) Incorrect. Er wordt geen systeemherstelplan gedocumenteerd in het reactieproces voor inbreuken in verband met persoonsgegevens.

Evaluatie

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

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

Contact EXIN

www.exin.com