

Voorbeeldexamen

Editie 202512

Copyright © EXIN Holding B.V. 2025. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

Inhoud

Inleiding	4
Voorbeeldexamen	5
Antwoordsleutel	17
Evaluatie	39

Inleiding

Dit is het EXIN Privacy & Data Protection Foundation (PDPF.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 minimaal 26 punten nodig om te slagen.

De beschikbare tijd is 60 minuten.

Veel succes!

Voorbeeldexamen

1 / 40
Wat is de relatie tussen gegevensbescherming en privacy?

A) Gegevensbescherming en privacy zijn synoniemen en betekenen hetzelfde.
B) Gegevensbescherming is het onderdeel van privacy waaronder de fysieke integriteit van personen wordt beschermd.
C) Gegevensbescherming verwijst naar de benodigde maatregelen om iemands privacy te beschermen.

2 / 40
In het rechtssysteem van de Europese Unie (EU) worden een aantal instrumenten gebruikt om verschillende doelen te bereiken. Sommige van deze instrumenten zijn bindend, terwijl andere instrumenten de EU-lidstaten zelf laten beslissen hoe ze ze gebruiken, wat flexibiliteit biedt.

Staat de AVG dit soort flexibiliteit toe?

A) Ja, want de AVG is een richtlijn die doelen stelt voor EU-lidstaten en nationale maatregelen voorstelt.
B) Ja, omdat het een aanbeveling is die advies geeft zonder verdere specifieke wettelijke verplichtingen.
C) Nee, want het is een besluit dat alleen bindend is voor specifieke partijen en niet voor alle EU-lidstaten.
D) Nee, want het is een verordening die voor alle EU-lidstaten geldt en rechtstreeks van toepassing is.

3 / 40
Hoe definieert de AVG persoonsgegevens?

A) Alle informatie die betrekking heeft op een inwoner van de Europese Economische Ruimte (EER)
B) Alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon
C) Gegevens die rechtstreeks betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon
D) Gegevens waaruit iemands ras of etnische afkomst, religieuze overtuigingen, gezondheid, seksueel gedrag of seksuele gerichtheid blijken

4 / 40
Wat is volgens de AVG de definitie van de verwerking van persoonsgegevens?

A) Elke bewerking die kan worden uitgevoerd op persoonsgegevens
B) Elke bewerking met betrekking tot persoonsgegevens, met uitzondering van wissen en vernietigen
C) Alleen bewerkingen waarbij persoonsgegevens op enige wijze worden gedeeld of overgedragen
D) Alleen bewerkingen waarbij de persoonsgegevens worden gebruikt voor de doeleinden waarvoor ze zijn verzameld

5 / 40
De AVG definieert sommige persoonsgegevens als gegevens uit een van de bijzondere categorieën van persoonsgegevens, ook wel 'gevoelige gegevens' genoemd.

Wat is een voorbeeld van dit soort gegevens?

A) Een overzicht van de zakelijke e-mailadressen van werknemers
B) Een stamboomuittreksel van iemands voorouders
C) Een lijst van betalingen die met een creditcard zijn gedaan
D) Een adressenlijst van de leden van een politieke partij

6 / 40
Een van de rollen die worden beschreven in de AVG, is als volgt gedefinieerd:

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Welke rol wordt hier gedefinieerd?

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

7 / 40
Het verwerken van persoonsgegevens dient rechtmatig te zijn. Een bedrijf verzamelt persoonsgegevens van zijn klanten.

Wat is **altijd** een vereiste voor rechtmatige verwerking bij het verzamelen van persoonsgegevens?

A) Toestemming voor de verwerking aanvragen bij de toezichthoudende autoriteit
B) Documentatie van de gerechtvaardigde grond voor het verwerken van de persoonsgegevens
C) Implementatie van een gedragscode die de aard van de verwerking beschrijft

8 / 40
Volgens de AVG moet de verwerkingsverantwoordelijke een register bijhouden van alle verwerkingsactiviteiten.

Welk register is **niet** verplicht volgens de AVG?

A) Een register van alle geïmplementeerde technische en organisatorische maatregelen van alle verwerkers
B) Een register van alle voorgenomen verwerkingsacties plus het verwerkingsdoel en de wettelijke rechtvaardiging hiervoor
C) Een register van inbreuken in verband met gegevens met alle relevante kenmerken, inclusief kennisgevingen

9 / 40
Een van de zeven beginselen van gegevensbescherming door ontwerp is *volledige functionaliteit – win-win zonder compromissen*.

Wat is de essentie van dit beginsel?

A) Gegevensbescherming werkt samen met beveiliging om een evenwichtssituatie te creëren, waarin zowel gerechtvaardigde belangen als privacy gewaarborgd worden.
B) Gegevensbescherming omvat ook het informeren van betrokkenen over de manier waarop hun gegevens worden verwerkt, waardoor betrokkenen de controle behouden.
C) Gegevensbescherming is ingebouwd in de architectuur en het ontwerp van de systemen, wat gegevensbescherming een kernfunctionaliteit maakt.

10 / 40
Wat is een beschrijving van gegevensbescherming door ontwerp en door standaardinstellingen?

A) Een aanpak waarmee gegevensbescherming vanaf de ontwikkeling wordt geïmplementeerd
B) Een indicatie van tijdsbestekken als de verwerking betrekking heeft op het wissen van gegevens
C) Gegevens mogen alleen worden verzameld voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden
D) Het niet bewaren van meer gegevens dan strikt noodzakelijk is voor het verwerken van gegevens

11 / 40
Om aantal benodigde parkeerplekken te plannen, worden door een lokale overheid de kentekens geregistreerd en bewaard van alle auto's die het centrum binnenrijden en verlaten. De overheid heeft toestemming verkregen om gegevens te verzamelen over het aantal aanwezige auto's in het centrum. Door de in- en uitrijdtijd voor elk kenteken te vergelijken, wordt op elk moment van de dag het aantal aanwezige auto's berekend.

Elke maand wordt er een verslag opgesteld met informatie over het gemiddelde aantal auto's in het centrum op specifieke momenten gedurende elke dag van de week. Bij elke toegangsweg tot het centrum staat een informatiebord waarop duidelijk wordt vermeld wie welke gegevens verzamelt, wat het doel van de verwerking is en dat de kentekens gedurende maximaal twee jaar veilig worden opgeslagen, omdat de metingen volgend jaar worden herhaald.

Welk basisbeginsel voor gerechtvaardigde verwerking van persoonsgegevens wordt in dit scenario **geschonden**?

A) Persoonsgegevens worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en verder niet verwerkt.
B) Persoonsgegevens worden niet langer dan noodzakelijk bewaard in een vorm die identificatie van betrokkenen toestaat.
C) Persoonsgegevens worden zodanig verwerkt dat passende persoonsgegevensbeveiliging wordt gewaarborgd.
D) Persoonsgegevens worden verwerkt op een wijze die transparant is ten aanzien van de betrokkene.

12 / 40
Volgens het beginsel van doelbinding mogen gegevens niet verder worden verwerkt, nadat het oorspronkelijke verwerkingsdoel is bereikt. In een aantal specifieke gevallen is verdere verwerking echter wel toegestaan, op voorwaarde dat er passende waarborgen worden genomen voor de rechten en vrijheden van de betrokkenen.

Voor welk doeleinde is verdere verwerking **niet** toegestaan?

A) Voor archiveringsdoeleinden in het algemeen belang
B) Voor direct marketing en commerciële doeleinden
C) Voor algemene statistische doeleinden
D) Voor wetenschappelijk of historisch onderzoek

13 / 40
Een organisatie biedt haar privacyverklaring aan in meerdere talen en formaten, waaronder een digitale, gedrukte en voorgelezen versie. Dit zorgt ervoor dat alle betrokkenen de verklaring kunnen inzien en begrijpen.

Welk AVG-recht wordt door deze praktijk het **meest** direct ondersteund?

A) Het recht op gegevenswissing, omdat betrokkenen duidelijk wordt gemaakt dat zij het recht hebben om hun gegevens te allen tijde te laten wissen.
B) Het recht van bezwaar, omdat betrokkenen beter bezwaar kunnen maken tegen verwerking als ze de privacyverklaring volledig begrijpen.
C) Het recht op beperking van de verwerking, omdat betrokkenen worden geïnformeerd over de doelstellingen van het bedrijf en de gerechtvaardigde gronden voor verwerking.
D) Het recht op transparante informatie, communicatie en mogelijkheden voor de uitoefening, omdat betrokkenen geholpen worden om de privacyverklaring te begrijpen.

14 / 40
Welk recht van de betrokkene is expliciet vastgelegd in de AVG?

A) Een kopie van de persoonsgegevens moet worden verstrekt in het door de betrokkene gevraagde formaat.
B) De betrokkene moet kosteloos inzage krijgen in de eigen persoonsgegevens.
C) Persoonsgegevens moeten altijd worden gewijzigd op verzoek van de betrokkene.
D) Persoonsgegevens moeten altijd gewist worden als de betrokkene daarom vraagt.

15 / 40
Iemand koopt een pak en geeft de winkel toestemming om zijn e-mailadres te gebruiken voor reclamedoeleinden. Bij thuiskomst vraagt de klant aan de winkel om al zijn persoonsgegevens weer te wissen en het sturen van e-mails stop te zetten.

Wat moet de winkel volgens de AVG doen?

A) De winkel mag geen van zijn persoonsgegevens verwijderen, aangezien de verkoopinformatie moet worden bijgehouden.
B) De winkel moet alle persoonsgegevens over deze persoon verwijderen waarvoor toestemming de gerechtvaardigde grond is.
C) De winkel moet zijn andere persoonsgegevens verwijderen, maar mag hem e-mails blijven toesturen.

16 / 40
Iemand ontvangt regelmatig aanbiedingen van een winkel waar hij vijf jaar geleden iets heeft gekocht. Hij wil dat het bedrijf stopt met het toesturen van deze aanbiedingen en zijn persoonsgegevens verwijdert.

Welk recht van de betrokkenen oefent hij uit?

A) Het recht van inzage
B) Het recht van bezwaar
C) Het recht op rectificatie
D) Het recht op beperking van de verwerking

17 / 40
Een bedrijf gebruikt kunstmatige intelligentie (AI) om sollicitatiebrieven te analyseren en automatisch te beslissen of sollicitanten uitgenodigd worden voor een gesprek.

Welk AVG-recht is **meest** relevant voor dit scenario?

A) Het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit
B) Het recht om een klacht in te dienen bij een toezichthoudende autoriteit
C) Het recht op beperking van de verwerking
D) Het recht op transparante informatie, communicatie en mogelijkheden voor de uitoefening

18 / 40
Persoonsgegevens moeten voor welbepaalde, uitdrukkelijke omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.

Welk beginsel inzake verwerking van persoonsgegevens wordt hier beschreven?

A) Juistheid
B) Minimale gegevensverwerking
C) Rechtmatigheid, behoorlijkheid en transparantie
D) Doelbinding

19 / 40
In de AVG wordt het beginsel van minimale gegevensverwerking beschreven.

Hoe kunnen organisaties voldoen aan dit beginsel?

A) Door het 'least privilege'-beginsel toe te passen op de verzamelde, opgeslagen of anderszins verwerkte persoonsgegevens
B) Door toegangsrechten te beperken tot personeel dat de persoonsgegevens nodig heeft voor de voorgenomen verwerkingsactiviteiten
C) Door de bestandsgrootte te beperken door alle persoonsgegevens die worden verwerkt, in een zo compact mogelijke indeling op te slaan
D) Door de persoonsgegevens te beperken tot dat wat toereikend, relevant en noodzakelijk is voor de verwerkingsdoeleinden

20 / 40
De AVG verwijst naar de principes van evenredigheid en subsidiariteit.

Wat betekent **subsidiariteit**?

A) Persoonsgegevens moeten worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder worden verwerkt.
B) Persoonsgegevens mogen niet langer dan noodzakelijk worden bewaard in een vorm die identificatie van betrokkenen toestaat.
C) Bij de verwerking van persoonsgegevens verzamelt een verwerkingsverantwoordelijke alleen gegevens die noodzakelijk zijn voor het doeleinde.
D) Bij de verwerking van persoonsgegevens moeten de gebruikte middelen zo min mogelijk inbreuk maken op de privacy.

21 / 40
Wat is het doel van data lifecycle management (DLM)?

A) Beoordelen of gegevens als persoonsgegevens of als normale gegevens moeten worden behandeld
B) Waarborgen dat persoonsgegevens worden verwijderd zodra er geen rechtsgrond meer is om ze te bewaren
C) Beheren van de gegevensstroom in een bedrijf in overeenstemming met de AVG

22 / 40
Wat is de **voornaamste** reden voor het gebruik een permanente cookie?

A) Waarborgen dat de persoonsgegevens van de gebruiker veilig worden opgeslagen op de server
B) De ervaring van de gebruiker op de website personaliseren bij een volgend bezoek
C) Elke toetsaanslag van een gebruiker registreren om wachtwoorden te achterhalen
D) Pagina's waaraan de gebruiker een bladwijzer heeft toegevoegd, opslaan in de browsergeschiedenis van de gebruiker

23 / 40
Een stichting voor kattenbescherming heeft vele donateurs. De stichting verwerkt persoonsgegevens van hun donateurs, zowel om gegevens bij te houden voor belastingdoeleinden als voor terugkerende donateurs. De donateurs hebben allemaal toestemming gegeven voor deze verwerking.

De kattenbescherming wil kunstmatige intelligentie (AI) in een AI-systeem gebruiken om terugkerende donateurs automatisch te bedanken, door hun kattenvideo's van hun favoriete katten toe te sturen. Ook zal het AI-systeem eenmalige donateurs e-mailen dat er meer hulpbehoevende katten zijn en maandelijkse donaties voorstellen.

Welk AVG-principe is **vooral** belangrijk voor dit AI-systeem?

A) Juistheid, omdat de kattenbescherming ervoor moet zorgen dat het AI-systeem de kattenvideo's goed afstemt op de donateurs om de beste resultaten te krijgen en op de lange termijn de donaties te verhogen.
B) Anonimisering, omdat de kattenbescherming ervoor moet zorgen dat het AI-systeem geen toegang heeft tot persoonsgegevens in een vorm die donateurs herkenbaar maakt.
C) Rechtmatigheid, omdat de kattenbescherming geen bedrijf is, waardoor het moeilijker is om een gerechtvaardigd belang te vinden dat de verwerking noodzakelijk en rechtmatig is.
D) Transparantie, omdat de kattenbescherming de donateurs duidelijk moet informeren over hoe hun gegevens worden gebruikt en hun een kans moet geven om bezwaar te maken als het oorspronkelijke doel verandert.

24 / 40
Een bedrijf gebruikt kunstmatige intelligentie (AI) om het goedkeuringsproces van leningen te stroomlijnen. Kredietaanvragers vullen een online formulier in. Het AI-systeem analyseert deze informatie en beslist automatisch of iemand in aanmerking komt voor een lening en hoe hoog de lening mag zijn. Dit proces is sneller en efficiënter dan traditionele methoden, waardoor het bedrijf een groter aantal aanvragen snel kan verwerken zonder menselijke tussenkomst.

Wat moet dit bedrijf volgens de AVG doen?

A) De persoonsgegevens die de AI gebruikt anonimiseren om ervoor te zorgen dat de kredietaanvragers niet kunnen worden geïdentificeerd
B) Kredietaanvragers informeren over de geautomatiseerde besluiten en hun een gemakkelijke manier bieden om een menselijke beoordeling aan te vragen
C) Een duidelijke melding geven dat kredietaanvragers ermee moeten instemmen dat de AI geautomatiseerde besluiten neemt zonder menselijke tussenkomst
D) Het gebruik van geautomatiseerde besluiten stoppen en terugvallen op menselijke besluitvorming om de rechten van de kredietaanvragers te waarborgen

25 / 40
Wanneer zijn er volgens de AVG **geen** aanvullende contracten nodig voor de doorgifte van persoonsgegevens?

A) Wanneer zowel de verzender als de ontvanger zich in de Europese Economische Ruimte (EER) bevinden
B) Wanneer de verzender de gegevens versleutelt voordat deze naar een ander bedrijf worden verstuurd
C) Wanneer de gegevens niet tot een van de bijzondere categorieën van persoonsgegevens behoren
D) Wanneer de gegevens worden doorgegeven voor journalistieke of artistieke doeleinden

26 / 40
Een bedrijf, dat het hoofdkantoor binnen de Europese Economische Ruimte (EER) heeft, heeft bindende bedrijfsvoorschriften (BCR) nodig.

Wat is volgens de AVG een beschrijving van BCR?

A) Een besluit over de veiligheid van de doorgifte van persoonsgegevens naar een niet-EER land
B) Een maatregel ter compensatie van het gebrek aan gegevensbescherming in een derde land
C) Een reeks overeenkomsten met betrekking tot de doorgifte van persoonsgegevens tussen niet-EER-landen
D) Een set goedgekeurde regels voor gegevensbescherming die door een groep ondernemingen wordt gebruikt

27 / 40
Een verwerkingsverantwoordelijke wil de verwerking van persoonsgegevens uitbesteden aan een verwerker.

Wat moet er **altijd** gebeuren voorafgaand aan de uitbesteding?

A) De verwerkingsverantwoordelijke en de verwerker moeten een schriftelijke overeenkomst, die de vertrouwelijkheid van de gegevens garandeert, opstellen en ondertekenen.
B) De verwerkingsverantwoordelijke of de verwerker moet de toezichthoudende autoriteit om toestemming vragen om de verwerking van de gegevens uit te besteden.
C) De verwerkingsverantwoordelijke moet bij de toezichthouder nagaan of de schriftelijke overeenkomst in overeenstemming is met de regelgeving.
D) De verwerker moet aan de verwerkingsverantwoordelijke laten zien dat hij aan alle eisen voldoet, die in de service level agreement (SLA) gesteld zijn.

28 / 40
Een multinational is van plan om persoonsgegevens over te dragen tussen vestigingen in verschillende landen, waaronder vestigingen buiten de Europese Economische Ruimte (EER). Het bedrijf besluit om bindende bedrijfsvoorschriften (BCR) te implementeren, om deze overdrachten te vergemakkelijken.

Wat is een noodzakelijk onderdeel van deze BCR?

A) De BCR moeten financiële compensatie aan betrokkenen gegaranderen in geval van inbreuk in verband met persoonsgegevens, en het bedrag specificeren.
B) De BCR moeten een mechanisme bevatten om naleving van de regels door alle werknemers, die betrokken zijn bij gegevensverwerking, te waarborgen.
C) De BCR moeten de exacte organisatorische en technische maatregelen voor de bescherming van de persoonsgegevens tijdens de overdracht beschrijven.
D) De BCR moeten specificeren dat alle betrokkenen op een toegankelijke manier op de hoogte moeten worden gesteld van elke overdracht van persoonsgegevens.

29 / 40
Een bedrijf wil persoonsgegevens doorgeven naar een land buiten de Europese Economische Ruimte (EER).

Welke doorgiftes **buiten** de EER zijn volgens de AVG altijd rechtmatig?

A) Doorgiften gebaseerd op de wetgeving van het betreffende niet-EER-land
B) Doorgiften die vallen onder de regels van de Wereldhandelsorganisatie (WTO)
C) Doorgiften waarop goedgekeurde bindende bedrijfsvoorschriften (BCR) van toepassing zijn
D) Doorgiften binnen een internationale onderneming of organisatie

30 / 40
Een bedrijf in Frankrijk heeft bindende bedrijfsvoorschriften (BCR) voor zijn wereldwijde activiteiten. Het bedrijf wil klantgegevens doorgeven aan een derde provider in de Verenigde Staten (VS), waarmee het geen gezamenlijke bedrijfsvoering heeft.

De Amerikaanse provider is niet gecertificeerd in het EU-U.S. Data Privacy Framework (DPF), maar heeft standaard contractuele clausules (SCCs) ondertekend, die zijn goedgekeurd door de Europese Commissie (EC). Deze SCCs maken deel uit van een ondertekend contract met het Franse bedrijf.

Is deze doorgifte van persoonsgegevens aan de Amerikaanse leverancier rechtmatig volgens de AVG?

A) Ja, omdat de DPF ongeldig is verklaard.
B) Ja, omdat de Amerikaanse provider SCCs heeft ondertekend.
C) Nee, omdat de doorgifte van persoonsgegevens naar de VS verboden is.
D) Nee, want de Amerikaanse provider moet de BCR ondertekenen.

31 / 40
Een koffiebar wil kunstmatige intelligentie (AI) en videobewaking gebruiken om bij te houden hoeveel kopjes koffie de werknemers inschenken. Het doel is om te begrijpen welke uren van de week het drukst zijn, door de productiviteit te monitoren.

Is een gegevensbeschermingseffectbeoordeling (DPIA) hier **verplicht**, volgens de AVG?

A) Ja, omdat de verwerking waarschijnlijk resulteert in een hoog risico voor de rechten van de betrokkenen.
B) Ja, omdat het project AI-technologieën of -processen omvat waarbij persoonsgegevens worden gebruikt.
C) Nee, omdat er met de monitoring geen persoonsgegevens uit een van de bijzondere categorieën worden verzameld.
D) Nee, omdat het geen direct doeleinde is om de productiviteit van de werknemers te beoordelen.

32 / 40
Tijdens de gegevensbeschermingseffectbeoordeling (DPIA) onderzoekt een team, dat werkt aan een online platform voor kinderen, of het gebruik van avatars in plaats van echte namen voldoet aan de functionaliteitsbehoeften.

Welke DPIA-doelstelling wordt **het meest** ondersteund door deze activiteit?

A) Het beoordelen van de noodzaak en evenredigheid van verwerking
B) Het beschrijven van de verwerking
C) Het betrekken van de relevante belanghebbenden
D) Het identificeren en beoordelen van de risico's voor betrokkenen

33 / 40
De AVG beschrijft de minimale onderdelen van een gegevensbeschermingseffectbeoordeling (DPIA).

Wat is een van deze minimale onderdelen?

A) Een gedetailleerd rapport over de taken en verantwoordelijkheden van de functionaris voor gegevensbescherming (FG)
B) Een beoordeling van de overeenkomsten aangaande gegevensuitwisseling tussen de organisatie en derde partijen
C) Een evaluatie van de beveiligingsmaatregelen die zijn genomen om gegevensdoorgiften te beschermen
D) Maatregelen om de geïdentificeerde risico's voor de rechten en vrijheden van de betrokkenen aan te pakken

34 / 40
Tijdens het maken van een back-up crasht een schijf van een dataserver. Zowel de gegevens als de back-up gaan hierbij verloren. De schijf bevatte persoonsgegevens, maar geen bijzondere categorie van persoonsgegevens.

De verwerker zegt dat dit volgens de AVG een inbreuk in verband met persoonsgegevens is.

Heeft de verwerker gelijk?

A) Ja, want de persoonsgegevens op de schijf werden onrechtmatig verwerkt.
B) Ja, want er werd geen bijzondere categorie van persoonsgegevens bewaard op de schijf.
C) Nee, want de persoonsgegevens op de schijf werden niet verwerkt, alleen vernietigd.
D) Nee, want dit is alleen een inbreuk in verband met reguliere gegevens en geen inbreuk in verband met persoonsgegevens.

35 / 40
Een bedrijf is van plan om persoonsgegevens te verwerken. De onlangs aangestelde functionaris voor gegevensbescherming (FG) voert een gegevensbeschermingseffectbeoordeling (DPIA) uit. De FG ontdekt dat alle computers een instelling hebben waardoor er na vijf seconden inactiviteit een schermbeveiliging wordt weergegeven op het beeldscherm. De computers worden echter niet automatisch vergrendeld. Wanneer medewerkers hun bureau verlaten, vergrendelen ze doorgaans hun computer ook niet.

Waar is dit een voorbeeld van?

A) Toegang tot gegevens
B) Inbreuk in verband met persoonsgegevens
C) Beveiligingsincident
D) Kwetsbaarheid in de beveiliging

36 / 40
Een architect verlaat een bouwplaats. Hij legt zijn laptop neer om zijn telefoon te beantwoorden. Dan rijdt er een vrachtwagen over de laptop heen. Al zijn bestanden voor het ontwerp van het gebouw en de berekeningen waaraan hij heeft gewerkt, gaan hierbij verloren. De architect heeft een back-up van een eerdere versie van de bestanden opgeslagen in de cloud.

Is dit volgens de AVG een inbreuk in verband met persoonsgegevens?

A) Ja, want door de vernietiging van de laatste kopie van bestanden zijn die bestanden niet meer beschikbaar.
B) Ja, want de vernietigde bestanden waren de persoonlijke bestanden van de architect.
C) Nee, want de ontwerpbestanden en berekeningen zijn geen persoonsgegevens.
D) Nee, want de bestanden zijn nog steeds beschikbaar in de vorm van een back-up.

37 / 40
Na een inbreuk in verband met persoonsgegevens moet een verwerkingsverantwoordelijke binnen de Europese Economische Ruimte (EER) bepalen wie moet worden geïnformeerd:

- Niemand
- Alleen de toezichthoudende autoriteit
- De toezichthoudende autoriteit en alle betrokkenen

In welke situatie moeten **betrokkenen** volgens de AVG op de hoogte worden gesteld van een inbreuk in verband met persoonsgegevens?

A) Wanneer persoonsgegevens worden verwerkt op een locatie van de verwerker die niet binnen de grenzen van de EER ligt
B) Wanneer persoonsgegevens worden verwerkt door een partij die akkoord is gegaan met het concept van de verwerkingsovereenkomst, maar deze nog niet heeft ondertekend
C) Wanneer het systeem waarin de persoonsgegevens worden verwerkt, wordt aangevallen en hierdoor schade aan de opslagapparatuur ontstaat
D) Wanneer de kans aanzienlijk is dat de inbreuk leidt tot een hoog risico voor de privacy van de betrokkenen

38 / 40
Een systeem dat persoonsgegevens bevat, is gehackt. Nu blijkt dat onbevoegde personen toegang hebben gekregen tot de persoonsgegevens.

Wat moet de verwerkingsverantwoordelijke volgens de AVG doen **voordat** hij de toezichthoudende autoriteit op de hoogte brengt?

A) Beoordelen of er toegang is of kan zijn verkregen tot gevoelige gegevens
B) Een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren om het risico voor natuurlijke personen te beoordelen
C) De getroffen betrokkenen op de hoogte brengen van de inbreuk in verband met persoonsgegevens en de mogelijke gevolgen hiervan
D) De politie op de hoogte brengen en aangifte doen van de onbevoegde toegang tot het systeem

39 / 40
Toezichthoudende autoriteiten hebben bepaalde taken die gericht zijn op het waarborgen van naleving van de AVG.

Wat is een van die taken?

A) Het beoordelen van gedragscodes voor specifieke sectoren in verband met de verwerking van persoonsgegevens
B) Het definiëren van een minimale set maatregelen die moeten worden genomen om persoonsgegevens en privacy te beschermen
C) Het opstellen van standaard contractbepalingen (SCC) en bindende bedrijfsvoorschriften (BCR)
D) Het onderzoeken van alle inbreuken in verband met gegevens waarvan de toezichthoudende autoriteit op de hoogte is gebracht

40 / 40
Het hoofdkantoor van een verwerkingsverantwoordelijke is gevestigd binnen de Europese Economische Ruimte (EER). De verwerking van gevoelige persoonsgegevens is uitbesteed aan een verwerker buiten de EER, zonder eerst de toezichthoudende autoriteit te raadplegen. Deze overtreding werd ontdekt en het bedrijf kreeg een geldboete van de toezichthoudende autoriteit.

Zes maanden later ontdekt de toezichthoudende autoriteit dat de verwerkingsverantwoordelijke nogmaals dezelfde overtreding heeft begaan, maar voor een andere verwerkingsactiviteit en met een andere verwerker.

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

A) Niets, omdat het bedrijf al een boete heeft gekregen voor deze overtreding
B) Niets, maar er kan een formele waarschuwing zonder financiële sancties worden gegeven
C) Een boete van maximaal €10 miljoen of 2% van de omzet, afhankelijk van wat hoger is
D) Een boete van maximaal €20 miljoen of 4% van de omzet, afhankelijk van wat hoger is

Antwoordsleutel

1 / 40
Wat is de relatie tussen gegevensbescherming en privacy?

A) Gegevensbescherming en privacy zijn synoniemen en betekenen hetzelfde.
B) Gegevensbescherming is het onderdeel van privacy waaronder de fysieke integriteit van personen wordt beschermd.
C) Gegevensbescherming verwijst naar de benodigde maatregelen om iemands privacy te beschermen.

A) Incorrect. Gegevensbescherming draagt bij aan de bescherming van iemands privacy, maar de termen zijn geen synoniemen.
B) Incorrect. Er bestaat geen verband tussen gegevensbescherming en fysieke integriteit of fysieke privacy.
C) Correct. Gegevensbescherming omvat enkele van de benodigde maatregelen om iemands privacy te beschermen. (Literatuur: A, Hoofdstuk 1)

2 / 40
In het rechtssysteem van de Europese Unie (EU) worden een aantal instrumenten gebruikt om verschillende doelen te bereiken. Sommige van deze instrumenten zijn bindend, terwijl andere instrumenten de EU-lidstaten zelf laten beslissen hoe ze ze gebruiken, wat flexibiliteit biedt.

Staat de AVG dit soort flexibiliteit toe?

A) Ja, want de AVG is een richtlijn die doelen stelt voor EU-lidstaten en nationale maatregelen voorstelt.
B) Ja, omdat het een aanbeveling is die advies geeft zonder verdere specifieke wettelijke verplichtingen.
C) Nee, want het is een besluit dat alleen bindend is voor specifieke partijen en niet voor alle EU-lidstaten.
D) Nee, want het is een verordening die voor alle EU-lidstaten geldt en rechtstreeks van toepassing is.

A) Incorrect. Een richtlijn stelt doelen voor de EU-lidstaten, die vervolgens zelf beslissen hoe ze deze in hun nationale wetgeving opnemen. De AVG is echter een verordening.
B) Incorrect. Een aanbeveling is niet-bindend en vereist geen wettelijke maatregelen van de EU-lidstaten. De AVG is echter een verordening.
C) Incorrect. Een besluit is alleen bindend voor de specifieke partijen waarop het betrekking heeft, niet voor alle EU-lidstaten, en het besluit is niet op iedereen van toepassing. De AVG is echter een verordening.
D) Correct. De AVG is een verordening die volledig bindend en rechtstreeks van toepassing is in de gehele EU, zonder dat er nationale maatregelen nodig zijn. (Literatuur: A, Hoofdstuk 1)

3 / 40
Hoe definieert de AVG persoonsgegevens?

A) Alle informatie die betrekking heeft op een inwoner van de Europese Economische Ruimte (EER)
B) Alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon
C) Gegevens die rechtstreeks betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon
D) Gegevens waaruit iemands ras of etnische afkomst, religieuze overtuigingen, gezondheid, seksueel gedrag of seksuele gerichtheid blijken

A) Incorrect. Gegevens zijn alleen persoonsgegevens als ze betrekking hebben op een identificeerbare of geïdentificeerde natuurlijke persoon. De woonplaats is niet relevant om te bepalen of gegevens persoonsgegevens zijn.
B) Correct. Dit is de officiële definitie in de AVG. (Literatuur: A, Hoofdstuk 1; Artikel 4(1) van de AVG)
C) Incorrect. Gegevens zijn ook persoonsgegevens als ze indirect betrekking hebben op een identificeerbare of geïdentificeerde natuurlijke persoon.
D) Incorrect. Dit is de definitie van persoonsgegevens uit een van de bijzondere categoriën van persoonsgegevens, niet van persoonsgegevens.

4 / 40
Wat is volgens de AVG de definitie van de verwerking van persoonsgegevens?

A) Elke bewerking die kan worden uitgevoerd op persoonsgegevens
B) Elke bewerking met betrekking tot persoonsgegevens, met uitzondering van wissen en vernietigen
C) Alleen bewerkingen waarbij persoonsgegevens op enige wijze worden gedeeld of overgedragen
D) Alleen bewerkingen waarbij de persoonsgegevens worden gebruikt voor de doeleinden waarvoor ze zijn verzameld

A) Correct. Onder verwerken valt elke bewerking die op persoonsgegevens kan worden uitgevoerd. (Literatuur: A, Hoofdstuk 1; Artikel 4(2) van de AVG)
B) Incorrect. Wissen en vernietigen vallen ook onder het verwerken van persoonsgegevens.
C) Incorrect. Elke bewerking, waaronder verspreiden, valt onder het verwerken van persoonsgegevens.
D) Incorrect. Elke bewerking wordt gezien als verwerking.

5 / 40
De AVG definieert sommige persoonsgegevens als gegevens uit een van de bijzondere categorieën van persoonsgegevens, ook wel 'gevoelige gegevens' genoemd.

Wat is een voorbeeld van dit soort gegevens?

A) Een overzicht van de zakelijke e-mailadressen van werknemers
B) Een stamboomuittreksel van iemands voorouders
C) Een lijst van betalingen die met een creditcard zijn gedaan
D) Een adressenlijst van de leden van een politieke partij

A) Incorrect. Zakelijke e-mailadressen vallen wel onder persoonsgegevens, maar niet onder een van de bijzondere categorieën van persoonsgegevens.
B) Incorrect. Genealogische informatie, zoals stambomen, over levende personen valt onder persoonsgegevens, maar niet onder een van de bijzondere categorieën van persoonsgegevens. De AVG is niet van toepassing op de gegevens van overleden personen.
C) Incorrect. Creditcardgegevens zijn persoonsgegevens, maar vallen niet onder een van de bijzondere categorieën van persoonsgegevens.
D) Correct. Persoonsgegevens waaruit politieke opvattingen blijken vallen onder een van de bijzondere categorieën van persoonsgegevens. (Literatuur: A, Hoofdstuk 4; Artikel 9(1) van de AVG)

6 / 40
Een van de rollen die worden beschreven in de AVG, is als volgt gedefinieerd:

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Welke rol wordt hier gedefinieerd?

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

A) Correct. De verwerkingsverantwoordelijke stelt het doel van en de middelen voor de verwerking vast. (Literatuur: A, Hoofdstuk 2; Artikel 4(7) van de AVG)
B) Incorrect. De verwerkingsverantwoordelijke stelt het doel van verwerking vast, de verwerker werkt op basis van de instructies van de verwerkingsverantwoordelijke.
C) Incorrect. De toezichthoudende autoriteit ziet toe op en handhaaft naleving van de AVG-vereisten.
D) Incorrect. Een derde speelt geen rol bij het bepalen van het verwerkingsdoel. Elke partij die het doel bepaalt, wordt automatisch een nieuwe verwerkingsverantwoordelijke.

7 / 40
Het verwerken van persoonsgegevens dient rechtmatig te zijn. Een bedrijf verzamelt persoonsgegevens van zijn klanten.

Wat is **altijd** een vereiste voor rechtmatige verwerking bij het verzamelen van persoonsgegevens?

A) Toestemming voor de verwerking aanvragen bij de toezichthoudende autoriteit
B) Documentatie van de gerechtvaardigde grond voor het verwerken van de persoonsgegevens
C) Implementatie van een gedragscode die de aard van de verwerking beschrijft

A) Incorrect. Voorafgaande raadpleging is alleen verplicht wanneer een gegevensbeschermingseffectbeoordeling (DPIA) wijst op een hoog risico. (Artikel 36 van de AVG)
B) Correct. Verwerking is alleen rechtmatig als er een gerechtvaardigde grond bestaat. (Literatuur: A, Hoofdstuk 4; Artikel 6 van de AVG)
C) Incorrect. Gedragscodes kunnen een middel zijn om overeenkomsten tussen verwerkingsverantwoordelijken en verwerkers te harmoniseren.

8 / 40
Volgens de AVG moet de verwerkingsverantwoordelijke een register bijhouden van alle verwerkingsactiviteiten.

Welk register is **niet** verplicht volgens de AVG?

A) Een register van alle geïmplementeerde technische en organisatorische maatregelen van alle verwerkers
B) Een register van alle voorgenomen verwerkingsacties plus het verwerkingsdoel en de wettelijke rechtvaardiging hiervoor
C) Een register van inbreuken in verband met gegevens met alle relevante kenmerken, inclusief kennisgevingen

A) Correct. Hoewel de verwerkingsverantwoordelijke moet controleren of verwerkers passende technische en organisatorische maatregelen gebruiken, hoeven deze maatregelen niet te worden geregistreerd. (Literatuur: A, Hoofdstuk 2; Artikel 28(1) van de AVG)
B) Incorrect. Een register van alle voorgenomen verwerkingsacties plus het verwerkingsdoel en de wettelijke rechtvaardiging hiervoor moet wel worden bijgehouden.
C) Incorrect. Een register van inbreuken in verband met gegevens moet wel worden bijgehouden.

9 / 40
Een van de zeven beginselen van gegevensbescherming door ontwerp is *volledige functionaliteit – win-win zonder compromissen*.

Wat is de essentie van dit beginsel?

A) Gegevensbescherming werkt samen met beveiliging om een evenwichtssituatie te creëren, waarin zowel gerechtvaardigde belangen als privacy gewaarborgd worden.
B) Gegevensbescherming omvat ook het informeren van betrokkenen over de manier waarop hun gegevens worden verwerkt, waardoor betrokkenen de controle behouden.
C) Gegevensbescherming is ingebouwd in de architectuur en het ontwerp van de systemen, wat gegevensbescherming een kernfunctionaliteit maakt.

A) Correct. Dit is de essentie van *volledige functionaliteit – win-win zonder compromissen*. (Literatuur: A, Hoofdstuk 2)
B) Incorrect. Dit is de essentie van *zichtbaarheid en transparantie - houd het open*.
C) Incorrect. Dit is de essentie van *gegevensbescherming geïntegreerd in het ontwerp*.

10 / 40
Wat is een beschrijving van gegevensbescherming door ontwerp en door standaardinstellingen?

A) Een aanpak waarmee gegevensbescherming vanaf de ontwikkeling wordt geïmplementeerd
B) Een indicatie van tijdsbestekken als de verwerking betrekking heeft op het wissen van gegevens
C) Gegevens mogen alleen worden verzameld voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden
D) Het niet bewaren van meer gegevens dan strikt noodzakelijk is voor het verwerken van gegevens

A) Correct. Dit is een juiste beschrijving. (Literatuur: A, Hoofdstuk 2; Artikel 25(1) van de AVG)
B) Incorrect. Dit is een beschrijving van een gegevensbeschermingseffectbeoordeling (DPIA).
C) Incorrect. Dit is een beschrijving van maatregelen die worden genomen om te voldoen aan het beginsel van doelbinding.
D) Incorrect. Dit is een beschrijving van procedures om te voldoen aan het beginsel van minimale gegevensverwerking.

11 / 40
Om aantal benodigde parkeerplekken te plannen, worden door een lokale overheid de kentekens geregistreerd en bewaard van alle auto's die het centrum binnenrijden en verlaten. De overheid heeft toestemming verkregen om gegevens te verzamelen over het aantal aanwezige auto's in het centrum. Door de in- en uitrijdtijd voor elk kenteken te vergelijken, wordt op elk moment van de dag het aantal aanwezige auto's berekend.

Elke maand wordt er een verslag opgesteld met informatie over het gemiddelde aantal auto's in het centrum op specifieke momenten gedurende elke dag van de week. Bij elke toegangsweg tot het centrum staat een informatiebord waarop duidelijk wordt vermeld wie welke gegevens verzamelt, wat het doel van de verwerking is en dat de kentekens gedurende maximaal twee jaar veilig worden opgeslagen, omdat de metingen volgend jaar worden herhaald.

Welk basisbeginsel voor gerechtvaardigde verwerking van persoonsgegevens wordt in dit scenario **geschonden**?

A) Persoonsgegevens worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en verder niet verwerkt.
B) Persoonsgegevens worden niet langer dan noodzakelijk bewaard in een vorm die identificatie van betrokkenen toestaat.
C) Persoonsgegevens worden zodanig verwerkt dat passende persoonsgegevensbeveiliging wordt gewaarborgd.
D) Persoonsgegevens worden verwerkt op een wijze die transparant is ten aanzien van de betrokkene.

A) Incorrect. De lokale overheid heeft een gerechtvaardigd doel aangegeven om gegevens over het aantal aanwezige auto's te verzamelen.
B) Correct. In dit scenario is het niet nodig om de gegevens van een specifieke auto waarmee de eigenaar wordt geïdentificeerd te bewaren nadat de auto het gebied heeft verlaten. (Literatuur: A, Hoofdstuk 3; Artikel 5 van de AVG)
C) Incorrect. Uit dit scenario blijkt geen ongeschikte beveiliging.
D) Incorrect. De verwerking gebeurt op transparante wijze, aangezien de betrokkenen naar behoren worden geïnformeerd.

12 / 40
Volgens het beginsel van doelbinding mogen gegevens niet verder worden verwerkt, nadat het oorspronkelijke verwerkingsdoel is bereikt. In een aantal specifieke gevallen is verdere verwerking echter wel toegestaan, op voorwaarde dat er passende waarborgen worden genomen voor de rechten en vrijheden van de betrokkenen.

Voor welk doeleinde is verdere verwerking **niet** toegestaan?

A) Voor archiveringsdoeleinden in het algemeen belang
B) Voor direct marketing en commerciële doeleinden
C) Voor algemene statistische doeleinden
D) Voor wetenschappelijk of historisch onderzoek

A) Incorrect. Met de juiste waarborgen is verdere verwerking voor archivering in het algemeen belang toegestaan.
B) Correct. Dit is geen toegestaan doeleinde als het niet het oorspronkelijke gerechtvaardigde doeleinde van de verwerking was. (Literatuur: A, Hoofdstuk 3)
C) Incorrect. Met de juiste waarborgen is verdere verwerking voor algemene statistische doeleinden toegestaan.
D) Incorrect. Met de juiste waarborgen is verdere verwerking voor onderzoek toegestaan.

13 / 40
Een organisatie biedt haar privacyverklaring aan in meerdere talen en formaten, waaronder een digitale, gedrukte en voorgelezen versie. Dit zorgt ervoor dat alle betrokkenen de verklaring kunnen inzien en begrijpen.

Welk AVG-recht wordt door deze praktijk het **meest** direct ondersteund?

A) Het recht op gegevenswissing, omdat betrokkenen duidelijk wordt gemaakt dat zij het recht hebben om hun gegevens te allen tijde te laten wissen.
B) Het recht van bezwaar, omdat betrokkenen beter bezwaar kunnen maken tegen verwerking als ze de privacyverklaring volledig begrijpen.
C) Het recht op beperking van de verwerking, omdat betrokkenen worden geïnformeerd over de doelstellingen van het bedrijf en de gerechtvaardigde gronden voor verwerking.
D) Het recht op transparante informatie, communicatie en mogelijkheden voor de uitoefening, omdat betrokkenen geholpen worden om de privacyverklaring te begrijpen.

A) Incorrect. Hoewel het belangrijk is om hun rechten te begrijpen, is de praktijk van het verstrekken van privacyverklaringen in verschillende formaten in de eerste plaats gericht op het ondersteunen van transparantie in plaats van op het direct faciliteren van het recht om gewist te worden.
B) Incorrect. Inzichtelijke privacyverklaringen kunnen betrokkenen helpen om hun rechten uit te oefenen, maar het hoofddoel van deze praktijk is het vergroten van transparantie in plaats van directe ondersteuning van het recht van bezwaar.
C) Incorrect. Hoewel het informeren van betrokkenen over de verwerking noodzakelijk is, is het belangrijkste doel van het verstrekken van toegankelijke privacyverklaringen het waarborgen van transparantie, niet specifiek het ondersteunen van het recht op beperkingen.
D) Correct. Het verstrekken van privacyverklaringen in meerdere talen en formaten zorgt ervoor dat alle betrokkenen duidelijke en toegankelijke informatie ontvangen, ter ondersteuning van hun recht op transparantie. (Literatuur: A, Hoofdstuk 5)

14 / 40
Welk recht van de betrokkene is expliciet vastgelegd in de AVG?

A) Een kopie van de persoonsgegevens moet worden verstrekt in het door de betrokkene gevraagde formaat.
B) De betrokkene moet kosteloos inzage krijgen in de eigen persoonsgegevens.
C) Persoonsgegevens moeten altijd worden gewijzigd op verzoek van de betrokkene.
D) Persoonsgegevens moeten altijd gewist worden als de betrokkene daarom vraagt.

A) Incorrect. De gegevens moeten worden verstrekt in een gestructureerd, algemeen gebruikt en machineleesbaar formaat. Dit hoeft niet noodzakelijkerwijs het formaat te zijn dat de betrokkene zelf aangeeft.
B) Correct. Betrokkenen hebben recht op een kopie van hun gegevens zonder dat ze daarvoor betalen. Echter, alleen de eerste kopie hoeft gratis zijn. (Literatuur: A, Hoofdstuk 5)
C) Incorrect. Alleen foutieve gegevens hoeven gecorrigeerd te worden.
D) Incorrect. Het recht om gegevens te wissen kent een aantal uitzonderingen, bijvoorbeeld als de gegevens nodig zijn voor de vaststelling, uitvoering of verdediging van rechtsvorderingen.

15 / 40
Iemand koopt een pak en geeft de winkel toestemming om zijn e-mailadres te gebruiken voor reclamedoeleinden. Bij thuiskomst vraagt de klant aan de winkel om al zijn persoonsgegevens weer te wissen en het sturen van e-mails stop te zetten.

Wat moet de winkel volgens de AVG doen?

A) De winkel mag geen van zijn persoonsgegevens verwijderen, aangezien de verkoopinformatie moet worden bijgehouden.
B) De winkel moet alle persoonsgegevens over deze persoon verwijderen waarvoor toestemming de gerechtvaardigde grond is.
C) De winkel moet zijn andere persoonsgegevens verwijderen, maar mag hem e-mails blijven toesturen.

A) Incorrect. De winkel is wettelijk verplicht om gegevens over de aankoop te bewaren. De toestemming van de betrokkene is ingetrokken, dus verwerking mag alleen doorgaan op basis van een andere rechtmatige grond dan toestemming, en de winkel moet stoppen met het versturen van reclamemails.
B) Correct. De winkel is wettelijk verplicht om gegevens over de aankoop (die ook persoonsgegevens zijn) te bewaren, maar andere gegevens moeten worden gewist. De toestemming van de betrokkene is ingetrokken, dus de winkel moet stoppen met het versturen van reclamemails. (Literatuur: A, Hoofdstuk 5; Artikel 17 van de AVG)
C) Incorrect. De toestemming van de betrokkene is ingetrokken, dus de winkel moet stoppen met het versturen van reclamemails.

16 / 40
Iemand ontvangt regelmatig aanbiedingen van een winkel waar hij vijf jaar geleden iets heeft gekocht. Hij wil dat het bedrijf stopt met het toesturen van deze aanbiedingen en zijn persoonsgegevens verwijdert.

Welk recht van de betrokkenen oefent hij uit?

A) Het recht van inzage
B) Het recht van bezwaar
C) Het recht op rectificatie
D) Het recht op beperking van de verwerking

A) Incorrect. Het recht van inzage omvat het verkrijgen van informatie over iemands persoonsgegevens en hoe deze worden verwerkt, niet het stoppen van communicatie of het verzoeken om verwijdering.
B) Correct. Met het recht van bezwaar kunnen individuen eisen dat het bedrijf stopt met het verwerken van gegevens voor marketingdoeleinden, waaronder het stoppen van aanbiedingen. (Literatuur: A, Hoofdstuk 5; Artikel 21 van de AVG)
C) Incorrect. Het recht op rectificatie geeft het recht om onjuiste of onvolledige gegevens rectificeren, maar niet het recht om communicatie te stoppen of gegevens te wissen.
D) Incorrect. De beperking in dit recht gaat over het blokkeren van gegevens die onjuist zijn of die in strijd met wettelijke verordeningen worden verwerkt.

17 / 40
Een bedrijf gebruikt kunstmatige intelligentie (AI) om sollicitatiebrieven te analyseren en automatisch te beslissen of sollicitanten uitgenodigd worden voor een gesprek.

Welk AVG-recht is **meest** relevant voor dit scenario?

A) Het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit
B) Het recht om een klacht in te dienen bij een toezichthoudende autoriteit
C) Het recht op beperking van de verwerking
D) Het recht op transparante informatie, communicatie en mogelijkheden voor de uitoefening

A) Correct. Dit recht is het meest relevant, omdat het specifiek betrekking heeft op besluiten die zonder menselijke tussenkomst worden genomen, zoals de besluiten die in dit scenario door de AI worden genomen. (Literatuur: A, Hoofdstuk 5; Artikel 22 van de AVG)
B) Incorrect. Het indienen van een klacht is een algemeen recht voor elke schending van de AVG, maar heeft niet specifiek betrekking op geautomatiseerde besluiten.
C) Incorrect. Beperking van de verwerking heeft betrekking op het beperken van het gebruik van persoonsgegevens, niet op besluiten die door AI worden genomen.
D) Incorrect. Hoewel transparantie belangrijk is, lost dat het probleem met geautomatiseerde besluiten in dit scenario niet op.

18 / 40
Persoonsgegevens moeten voor welbepaalde, uitdrukkelijke omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.

Welk beginsel inzake verwerking van persoonsgegevens wordt hier beschreven?

A) Juistheid
B) Minimale gegevensverwerking
C) Rechtmatigheid, behoorlijkheid en transparantie
D) Doelbinding

A) Incorrect. Juistheid verwijst naar het garanderen dat de gegevens juist en actueel worden gehouden, niet naar het specificeren van de doeleinden voor het verzamelen van gegevens.
B) Incorrect. Minimale gegevensverwerking verwijst naar het verzamelen van alleen die gegevens die nodig zijn voor een specifiek doel, niet naar het specificeren van de doeleinden zelf.
C) Incorrect. Rechtmatigheid, behoorlijkheid en transparantie vereisen een rechtsgrond en duidelijkheid over de verwerking, maar vereisen de doelspecificatie niet direct.
D) Correct. Doelbinding vereist dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. (Literatuur: A, Hoofdstuk 3; Artikel 5 van de AVG)

19 / 40
In de AVG wordt het beginsel van minimale gegevensverwerking beschreven.

Hoe kunnen organisaties voldoen aan dit beginsel?

A) Door het 'least privilege'-beginsel toe te passen op de verzamelde, opgeslagen of anderszins verwerkte persoonsgegevens
B) Door toegangsrechten te beperken tot personeel dat de persoonsgegevens nodig heeft voor de voorgenomen verwerkingsactiviteiten
C) Door de bestandsgrootte te beperken door alle persoonsgegevens die worden verwerkt, in een zo compact mogelijke indeling op te slaan
D) Door de persoonsgegevens te beperken tot dat wat toereikend, relevant en noodzakelijk is voor de verwerkingsdoeleinden

A) Incorrect. Minimale gegevensverwerking heeft niets te maken met het 'least privilege'-beginsel.
B) Incorrect. Hier wordt het concept beschreven waaronder toestemming wordt beperkt, bijvoorbeeld om te voldoen aan het beginsel van integriteit en vertrouwelijkheid.
C) Incorrect. Minimale gegevensverwerking draait volgens de AVG niet om de bestandsgrootte, maar om het beperken van persoonsgegevens tot wat strikt noodzakelijk is.
D) Correct. Dit is de essentie van de beschrijving van het principe van minimale gegevensverwerking in de AVG. (Literatuur: A, Hoofdstuk 3; Artikel 5(1)(c) van de AVG)

20 / 40
De AVG verwijst naar de principes van evenredigheid en subsidiariteit.

Wat betekent **subsidiariteit**?

A) Persoonsgegevens moeten worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder worden verwerkt.
B) Persoonsgegevens mogen niet langer dan noodzakelijk worden bewaard in een vorm die identificatie van betrokkenen toestaat.
C) Bij de verwerking van persoonsgegevens verzamelt een verwerkingsverantwoordelijke alleen gegevens die noodzakelijk zijn voor het doeleinde.
D) Bij de verwerking van persoonsgegevens moeten de gebruikte middelen zo min mogelijk inbreuk maken op de privacy.

A) Incorrect. Dit is een definitie van doelbinding.
B) Incorrect. Dit is een definitie van opslagbeperking.
C) Incorrect. Dit is een definitie van minimale gegevensverwerking.
D) Correct. Als subsidiariteit wordt toegepast op gegevensbescherming, betekent dit dat de minst ingrijpende manieren worden gebruikt om gegevens te verwerken, om de impact op de privacy te minimalizeren. (Literatuur: A, Hoofdstuk 3; Overweging 170 van de AVG)

21 / 40
Wat is het doel van data lifecycle management (DLM)?

A) Beoordelen of gegevens als persoonsgegevens of als normale gegevens moeten worden behandeld
B) Waarborgen dat persoonsgegevens worden verwijderd zodra er geen rechtsgrond meer is om ze te bewaren
C) Beheren van de gegevensstroom in een bedrijf in overeenstemming met de AVG

A) Incorrect. Het doel van DLM is om de stroom van alle gegevens in een bedrijf te beheren en te garanderen dat gegevens veilig en conform de AVG worden verwerkt. Dit geldt niet alleen voor persoonsgegevens, maar voor alle gegevens.
B) Incorrect. Dit is niet het doel van DLM, maar DLM helpt wel bij het opsporen van gegevens die verwijderd moeten worden als er geen rechtsgrond meer is om ze te bewaren.
C) Correct. DLM is een gestructureerde aanpak om de gegevensstroom te beheren, noodzakelijke beveiligingscontroles te bepalen en naleving van de AVG te garanderen. (Literatuur: A, Hoofdstuk 6; Artikel 5 van de AVG)

22 / 40
Wat is de **voornaamste** reden voor het gebruik een permanente cookie?

A) Waarborgen dat de persoonsgegevens van de gebruiker veilig worden opgeslagen op de server
B) De ervaring van de gebruiker op de website personaliseren bij een volgend bezoek
C) Elke toetsaanslag van een gebruiker registreren om wachtwoorden te achterhalen
D) Pagina's waaraan de gebruiker een bladwijzer heeft toegevoegd, opslaan in de browsergeschiedenis van de gebruiker

A) Incorrect. Cookies worden niet gebruikt om gegevens op de server op te slaan.
B) Correct. Dit is het voornaamste doel van een permanente cookie. (Literatuur: A, Hoofdstuk 7)
C) Incorrect. Cookies zijn op zich niet schadelijk, maar het mechanisme kan wel worden misbruikt voor schadelijke doeleinden.
D) Incorrect. Bladwijzers en de browsergeschiedenis worden inderdaad opgeslagen, maar niet in een cookie.

23 / 40
Een stichting voor kattenbescherming heeft vele donateurs. De stichting verwerkt persoonsgegevens van hun donateurs, zowel om gegevens bij te houden voor belastingdoeleinden als voor terugkerende donateurs. De donateurs hebben allemaal toestemming gegeven voor deze verwerking.

De kattenbescherming wil kunstmatige intelligentie (AI) in een AI-systeem gebruiken om terugkerende donateurs automatisch te bedanken, door hun kattenvideo's van hun favoriete katten toe te sturen. Ook zal het AI-systeem eenmalige donateurs e-mailen dat er meer hulpbehoevende katten zijn en maandelijkse donaties voorstellen.

Welk AVG-principe is **vooral** belangrijk voor dit AI-systeem?

A) Juistheid, omdat de kattenbescherming ervoor moet zorgen dat het AI-systeem de kattenvideo's goed afstemt op de donateurs om de beste resultaten te krijgen en op de lange termijn de donaties te verhogen.
B) Anonimisering, omdat de kattenbescherming ervoor moet zorgen dat het AI-systeem geen toegang heeft tot persoonsgegevens in een vorm die donateurs herkenbaar maakt.
C) Rechtmatigheid, omdat de kattenbescherming geen bedrijf is, waardoor het moeilijker is om een gerechtvaardigd belang te vinden dat de verwerking noodzakelijk en rechtmatig is.
D) Transparantie, omdat de kattenbescherming de donateurs duidelijk moet informeren over hoe hun gegevens worden gebruikt en hun een kans moet geven om bezwaar te maken als het oorspronkelijke doel verandert.

A) Incorrect. Binnen de AVG verwijst juistheid naar de juistheid van de gegevens zelf, niet naar de juistheid van het algoritme. Juistheid, behoorlijkheid en bias zijn verplichte vereisten in de AI-wet.
B) Incorrect. De organisatie moet identificeerbare persoonsgegevens gebruiken om gepersonaliseerde berichten te sturen, dus anonimiseren zou niet relevant zijn.
C) Incorrect. De kattenbescherming moet een rechtmatige grondslag of een gerechtvaardigd belang hebben. Het vinden van een dergelijke grondslag wordt echter niet bemoeilijkt doordat het een stichting is. Donateurs hebben al toestemming gegeven voor het verwerken van hun persoonsgegevens. Het enige wat ontbreekt is het informeren van donateurs en de mogelijkheid om bezwaar te kunnen maken tegen verdere verwerking.
D) Correct. Transparantie is het belangrijkst voor dit AI-systeem, omdat het gebruik van dit AI-systeem een nieuwe verwerkingsactiviteit is. Het is belangrijk om donateurs te informeren als het doel van de gegevensverwerking verandert. (Literatuur: A, Hoofdstuk 3 en 7.2)

24 / 40
Een bedrijf gebruikt kunstmatige intelligentie (AI) om het goedkeuringsproces van leningen te stroomlijnen. Kredietaanvragers vullen een online formulier in. Het AI-systeem analyseert deze informatie en beslist automatisch of iemand in aanmerking komt voor een lening en hoe hoog de lening mag zijn. Dit proces is sneller en efficiënter dan traditionele methoden, waardoor het bedrijf een groter aantal aanvragen snel kan verwerken zonder menselijke tussenkomst.

Wat moet dit bedrijf volgens de AVG doen?

A) De persoonsgegevens die de AI gebruikt anonimiseren om ervoor te zorgen dat de kredietaanvragers niet kunnen worden geïdentificeerd
B) Kredietaanvragers informeren over de geautomatiseerde besluiten en hun een gemakkelijke manier bieden om een menselijke beoordeling aan te vragen
C) Een duidelijke melding geven dat kredietaanvragers ermee moeten instemmen dat de AI geautomatiseerde besluiten neemt zonder menselijke tussenkomst
D) Het gebruik van geautomatiseerde besluiten stoppen en terugvallen op menselijke besluitvorming om de rechten van de kredietaanvragers te waarborgen

A) Incorrect. Door gegevens te anonimiseren kan de AI zijn werk niet goed doen. De AVG vereist geen anonimisering, maar wel de mogelijkheid voor een menselijke beoordeling.
B) Correct. Deze optie voldoet aan de AVG door ervoor te zorgen dat aanvragers worden geïnformeerd over AI-beslissingen en een menselijke beoordeling kunnen aanvragen als ze het niet eens zijn met een besluit. (Literatuur: A, Hoofdstuk 7.2)
C) Incorrect. Stellen dat aanvragers moeten instemmen met geautomatiseerde besluiten voldoet niet aan de vereisten van de AVG. Het bedrijf moet ook opties bieden voor een menselijke beoordeling.
D) Incorrect. De AVG vereist niet van bedrijven dat ze stoppen met het gebruik van AI voor besluiten. In plaats daarvan wordt de nadruk gelegd op transparantie en de mogelijkheid om een menselijke beoordeling aan te vragen.

25 / 40
Wanneer zijn er volgens de AVG **geen** aanvullende contracten nodig voor de doorgifte van persoonsgegevens?

A) Wanneer zowel de verzender als de ontvanger zich in de Europese Economische Ruimte (EER) bevinden
B) Wanneer de verzender de gegevens versleutelt voordat deze naar een ander bedrijf worden verstuurd
C) Wanneer de gegevens niet tot een van de bijzondere categorieën van persoonsgegevens behoren
D) Wanneer de gegevens worden doorgegeven voor journalistieke of artistieke doeleinden

A) Correct. Er zijn geen aanvullende contracten nodig voor het overdragen van persoonsgegevens binnen de EER, aangezien alle lidstaten zich moeten houden aan de normen voor gegevensbescherming van de AVG. (Literatuur: A, Hoofdstuk 8; Artikel 44 van de AVG)
B) Incorrect. Hoewel encryptie een goede beveiligingspraktijk is, kunnen er nog steeds aanvullende maatregelen nodig zijn als de gegevens naar buiten de EER worden overgedragen, afhankelijk van de gegevensbescherming in het land van bestemming.
C) Incorrect. De noodzaak voor aanvullende maatregelen hangt niet alleen af van of de gegevens tot een van de bijzondere categorieën van persoonsgegevens behoren, maar ook van de bestemming van de gegevensoverdracht.
D) Incorrect. Zelfs voor journalistieke of artistieke doeleinden zijn voor de overdracht van persoonsgegevens buiten de EER extra maatregelen nodig om naleving van de AVG te garanderen.

26 / 40
Een bedrijf, dat het hoofdkantoor binnen de Europese Economische Ruimte (EER) heeft, heeft bindende bedrijfsvoorschriften (BCR) nodig.

Wat is volgens de AVG een beschrijving van BCR?

A) Een besluit over de veiligheid van de doorgifte van persoonsgegevens naar een niet-EER land
B) Een maatregel ter compensatie van het gebrek aan gegevensbescherming in een derde land
C) Een reeks overeenkomsten met betrekking tot de doorgifte van persoonsgegevens tussen niet-EER-landen
D) Een set goedgekeurde regels voor gegevensbescherming die door een groep ondernemingen wordt gebruikt

A) Incorrect. Dit verwijst naar adequaatheidsbesluiten.
B) Incorrect. Dit verwijst naar passende waarborgen.
C) Incorrect. De AVG heeft geen betrekking op overeenkomsten tussen niet-EER landen.
D) Correct. BCR zijn een set regels die zijn goedgekeurd door de toezichthoudende autoriteiten. (Literatuur: A, Hoofdstuk 9; Artikel 47 van de AVG)

27 / 40
Een verwerkingsverantwoordelijke wil de verwerking van persoonsgegevens uitbesteden aan een verwerker.

Wat moet er **altijd** gebeuren voorafgaand aan de uitbesteding?

A) De verwerkingsverantwoordelijke en de verwerker moeten een schriftelijke overeenkomst, die de vertrouwelijkheid van de gegevens garandeert, opstellen en ondertekenen.
B) De verwerkingsverantwoordelijke of de verwerker moet de toezichthoudende autoriteit om toestemming vragen om de verwerking van de gegevens uit te besteden.
C) De verwerkingsverantwoordelijke moet bij de toezichthouder nagaan of de schriftelijke overeenkomst in overeenstemming is met de regelgeving.
D) De verwerker moet aan de verwerkingsverantwoordelijke laten zien dat hij aan alle eisen voldoet, die in de service level agreement (SLA) gesteld zijn.

A) Correct. Er moet een schriftelijke overeenkomst liggen waarin de vertrouwelijkheid van de gegevens wordt gegarandeerd, waarin de doeleinden en middelen van de verwerking, zoals gedefinieerd door de verwerkingsverantwoordelijke, worden beschreven en waarin wordt bepaald dat de verwerker alleen alleen gegevens verwerkt in opdracht van de verwerkingsverantwoordelijke. Beide partijen moeten deze overeenkomst ondertekenen. (Literatuur: A, Hoofdstuk 2; Artikel 28(3) van de AVG)
B) Incorrect. De verwerkingsverantwoordelijke hoeft de toezichthoudende autoriteit niet voor elke uitbesteding om toestemming te vragen. De verwerker hoeft nooit toestemming te vragen.
C) Incorrect. De toezichthoudende autoriteit is geen juridisch adviseur en controleert niet of schriftelijke overeenkomsten conform de regelgeving zijn.
D) Incorrect. Een SLA is niet voldoende, omdat deze gericht is op activiteiten, niet noodzakelijkerwijs op doeleinden.

28 / 40
Een multinational is van plan om persoonsgegevens over te dragen tussen vestigingen in verschillende landen, waaronder vestigingen buiten de Europese Economische Ruimte (EER). Het bedrijf besluit om bindende bedrijfsvoorschriften (BCR) te implementeren, om deze overdrachten te vergemakkelijken.

Wat is een noodzakelijk onderdeel van deze BCR?

A) De BCR moeten financiële compensatie aan betrokkenen gegaranderen in geval van inbreuk in verband met persoonsgegevens, en het bedrag specificeren.
B) De BCR moeten een mechanisme bevatten om naleving van de regels door alle werknemers, die betrokken zijn bij gegevensverwerking, te waarborgen.
C) De BCR moeten de exacte organisatorische en technische maatregelen voor de bescherming van de persoonsgegevens tijdens de overdracht beschrijven.
D) De BCR moeten specificeren dat alle betrokkenen op een toegankelijke manier op de hoogte moeten worden gesteld van elke overdracht van persoonsgegevens.

A) Incorrect. BCR garanderen geen financiële compensatie in geval van inbreuk in verband met persoonsgegevens. Ze zijn gericht op naleving van de standaarden voor gegevensbescherming.
B) Correct. De BCR moeten mechanismen bevatten om naleving door alle werknemers te garanderen, omdat de BCR bindend en afdwingbaar moeten zijn binnen de bedrijfsgroep. (Literatuur: A, Hoofdstuk 9)
C) Incorrect. Hoewel BCR gegevensbescherming moeten garanderen, hoeven ze de gebruikte technologieën niet nader te specificeren. BCR richten zich op naleving en afdwingbaarheid.
D) Incorrect. BCR zijn interne regels voor de overdracht van persoonsgegevens binnen een bedrijfsgroep. Betrokkenen moeten weten hoe hun persoonsgegevens worden verwerkt, maar het is niet nodig om hun een kennisgeving van elke overdracht te geven.

29 / 40
Een bedrijf wil persoonsgegevens doorgeven naar een land buiten de Europese Economische Ruimte (EER).

Welke doorgiftes **buiten** de EER zijn volgens de AVG altijd rechtmatig?

A) Doorgiften gebaseerd op de wetgeving van het betreffende niet-EER-land
B) Doorgiften die vallen onder de regels van de Wereldhandelsorganisatie (WTO)
C) Doorgiften waarop goedgekeurde bindende bedrijfsvoorschriften (BCR) van toepassing zijn
D) Doorgiften binnen een internationale onderneming of organisatie

A) Incorrect. Hiervoor is ook een adequaatheidsbesluit vereist waarmee wordt bevestigd dat die wetten toereikend zijn.
B) Incorrect. De WHO heeft alleen betrekking op de vrije handel van goederen en diensten.
C) Correct. BCR die zijn goedgekeurd door een toezichthoudende autoriteit, maken de doorgifte rechtmatig. (Literatuur: A, Hoofdstuk 9; Artikel 47 van de AVG)
D) Incorrect. Hiervoor is ook vereist dat er officieel bindende bedrijfsvoorschriften worden aangenomen.

30 / 40
Een bedrijf in Frankrijk heeft bindende bedrijfsvoorschriften (BCR) voor zijn wereldwijde activiteiten. Het bedrijf wil klantgegevens doorgeven aan een derde provider in de Verenigde Staten (VS), waarmee het geen gezamenlijke bedrijfsvoering heeft.

De Amerikaanse provider is niet gecertificeerd in het EU-U.S. Data Privacy Framework (DPF), maar heeft standaard contractuele clausules (SCCs) ondertekend, die zijn goedgekeurd door de Europese Commissie (EC). Deze SCCs maken deel uit van een ondertekend contract met het Franse bedrijf.

Is deze doorgifte van persoonsgegevens aan de Amerikaanse leverancier rechtmatig volgens de AVG?

A) Ja, omdat de DPF ongeldig is verklaard.
B) Ja, omdat de Amerikaanse provider SCCs heeft ondertekend.
C) Nee, omdat de doorgifte van persoonsgegevens naar de VS verboden is.
D) Nee, want de Amerikaanse provider moet de BCR ondertekenen.

A) Incorrect. Het DPF wordt adequaat geacht. De geldigheid van de DPF is hier echter niet relevant, aangezien de SCCs al een onafhankelijke rechtsgrond voor de doorgifte van persoonsgegevens bieden.
B) Correct. Het gebruik van door de EC goedgekeurde SCCs is een geldig juridisch mechanisme voor de doorgifte van persoonsgegevens onder de AVG, waardoor de overdracht rechtmatig is. (Literatuur: A, Hoofdstuk 9; Artikel 46(2)(c) van de AVG)
C) Incorrect. De doorgifte van persoonsgegevens naar de VS is niet absoluut verboden. Een overdracht kan rechtmatig zijn als passende waarborgen, zoals SCCs of de DPF, aanwezig zijn.
D) Incorrect. BCRs zijn bedoeld voor de doorgifte van persoonsgegevens binnen een groep en zijn niet van toepassing op derde providers, zoals de Amerikaanse cloudprovider. De SCCs zijn hier het passende mechanisme voor de doorgifte.

31 / 40
Een koffiebar wil kunstmatige intelligentie (AI) en videobewaking gebruiken om bij te houden hoeveel kopjes koffie de werknemers inschenken. Het doel is om te begrijpen welke uren van de week het drukst zijn, door de productiviteit te monitoren.

Is een gegevensbeschermingseffectbeoordeling (DPIA) hier **verplicht**, volgens de AVG?

A) Ja, omdat de verwerking waarschijnlijk resulteert in een hoog risico voor de rechten van de betrokkenen.
B) Ja, omdat het project AI-technologieën of -processen omvat waarbij persoonsgegevens worden gebruikt.
C) Nee, omdat er met de monitoring geen persoonsgegevens uit een van de bijzondere categorieën worden verzameld.
D) Nee, omdat het geen direct doeleinde is om de productiviteit van de werknemers te beoordelen.

A) Correct. Videobewaking kan een aanzienlijke impact hebben op de privacy en rechten van werknemers, waardoor een DPIA nodig is om mogelijke hoge risico's voor hun rechten en vrijheden te beoordelen en te beperken. (Literatuur: A, Hoofdstuk 10; Artikel 35 van de AVG)
B) Incorrect. Hoewel een DPIA vereist is, is dat niet vanwege het gebruik van persoonsgegevens of AI. Wat de DPIA verplicht maakt, is het hoge risico voor de privacy en rechten van de werknemers van de monitoring van de productiviteit.
C) Incorrect. Zelfs als er geen persoonsgegevens uit een van de bijzondere categorieën van persoonsgegevens worden verzameld, is er nog steeds een DPIA nodig als er een hoog risico is voor de rechten van mensen, zoals bij videobewaking.
D) Incorrect. De reden voor het verzamelen van gegevens verandert niets aan de noodzaak van een DPIA als er een hoog risico is voor de rechten van mensen.

32 / 40
Tijdens de gegevensbeschermingseffectbeoordeling (DPIA) onderzoekt een team, dat werkt aan een online platform voor kinderen, of het gebruik van avatars in plaats van echte namen voldoet aan de functionaliteitsbehoeften.

Welke DPIA-doelstelling wordt **het meest** ondersteund door deze activiteit?

A) Het beoordelen van de noodzaak en evenredigheid van verwerking
B) Het beschrijven van de verwerking
C) Het betrekken van de relevante belanghebbenden
D) Het identificeren en beoordelen van de risico's voor betrokkenen

A) Correct. Door te onderzoeken of het gebruik van avatars in plaats van echte namen voldoet aan de functionaliteitsbehoeften, beoordeelt het team of de gegevensverwerking strikt noodzakelijk is en in verhouding staat tot het bereiken van de doelen van het platform. (Literatuur: A, Hoofdstuk 10)
B) Incorrect. Bij de beoordeling over avatars worden de verwerkingsactiviteiten zelf niet beschreven. In plaats daarvan worden alternatieven geëvalueerd om aan de functionaliteitsbehoeften te voldoen.
C) Incorrect. Bij de beoordeling over avatars zijn de belanghebbenden niet betrokken. In plaats daarvan wordt geëvalueerd of er minder van hun persoonsgegevens gebruikt kunnen worden om aan de functionaliteitsbehoeften te voldoen.
D) Incorrect. De beoordeling over avatars identificeert of beoordeelt risico's niet rechtstreeks. De beoordeling is gericht op het evalueren van de noodzaak en evenredigheid van het gebruik van persoonsgegevens (echte namen) versus het weglaten ervan (avatars).

33 / 40
De AVG beschrijft de minimale onderdelen van een gegevensbeschermingseffectbeoordeling (DPIA).

Wat is een van deze minimale onderdelen?

A) Een gedetailleerd rapport over de taken en verantwoordelijkheden van de functionaris voor gegevensbescherming (FG)
B) Een beoordeling van de overeenkomsten aangaande gegevensuitwisseling tussen de organisatie en derde partijen
C) Een evaluatie van de beveiligingsmaatregelen die zijn genomen om gegevensdoorgiften te beschermen
D) Maatregelen om de geïdentificeerde risico's voor de rechten en vrijheden van de betrokkenen aan te pakken

A) Incorrect. Hoewel de rol van een FG belangrijk is onder de AVG, is een specifieke rapportage over hun taken en verantwoordelijkheden niet een van de minimale onderdelen van een DPIA.
B) Incorrect. Hoewel het beoordelen van overeenkomsten aangaande gegevensuitwisseling belangrijk is voor de algehele naleving van gegevensbescherming, wordt dit niet specifiek in de AVG genoemd als een van de minimale onderdelen van een DPIA.
C) Incorrect. Hoewel het evalueren van beveiligingsmaatregelen deel uitmaakt van het waarborgen van gegevensbescherming, richt een DPIA zich specifiek op het beoordelen van de risico's voor de rechten en vrijheden van de betrokkenen en de maatregelen om deze risico's te beperken, in plaats van alleen op het evalueren van beveiligingsmaatregelen die zijn genomen om gegevensoverdrachten te beschermen.
D) Correct. De AVG stelt de minimale onderdelen van een gegevensbeschermingseffectbeoordeling (DPIA) vast: een systematische beschrijving van de beoogde verwerkingen en de doeleinden van de verwerking; een beoordeling van de noodzaak en evenredigheid van de verwerking; een beoordeling van de risico’s voor de rechten en vrijheden van de betrokkenen; de beoogde maatregelen om deze risico’s aan te pakken en om naleving van de AVG aan te tonen. (Literatuur: A, Hoofdstuk 10; Artikel 35(7), Overweging 84 en Overweging 90 van de AVG)

34 / 40
Tijdens het maken van een back-up crasht een schijf van een dataserver. Zowel de gegevens als de back-up gaan hierbij verloren. De schijf bevatte persoonsgegevens, maar geen bijzondere categorie van persoonsgegevens.

De verwerker zegt dat dit volgens de AVG een inbreuk in verband met persoonsgegevens is.

Heeft de verwerker gelijk?

A) Ja, want de persoonsgegevens op de schijf werden onrechtmatig verwerkt.
B) Ja, want er werd geen bijzondere categorie van persoonsgegevens bewaard op de schijf.
C) Nee, want de persoonsgegevens op de schijf werden niet verwerkt, alleen vernietigd.
D) Nee, want dit is alleen een inbreuk in verband met reguliere gegevens en geen inbreuk in verband met persoonsgegevens.

A) Correct. Wanneer persoonsgegevens op onherstelbare wijze verloren gaan, beschouwen we dit als 'een inbreuk in de beveiliging die leidt tot onrechtmatige vernietiging van persoonsgegevens', wat het ook tot een inbreuk in verband met persoonsgegevens maakt. (Literatuur: A, Hoofdstuk 11; Artikel 4(12) van de AVG)
B) Incorrect. De gevoelige bedrijfsgegevens zijn niet van invloed bij het bepalen of er sprake is van een inbreuk in verband met persoonsgegevens.
C) Incorrect. De AVG ziet onopzettelijk verlies van persoonsgegevens als onrechtmatige verwerking, omdat het niet in opdracht van de verwerkingsverantwoordelijke of de verwerker gebeurt. Dit maakt het een inbreuk in verband met persoonsgegevens.
D) Incorrect. Het verlies van bedrijfsgegevens is een verlies van gegevens, geen inbreuk in verband met gegevens. Het verliezen van persoonsgegevens is het verwijderen van de toegang tot de persoonsgegevens, wat wordt beschouwd als een inbreuk in verband met persoonsgegevens (inbreuk met betrekking tot beschikbaarheid) onder de AVG.

35 / 40
Een bedrijf is van plan om persoonsgegevens te verwerken. De onlangs aangestelde functionaris voor gegevensbescherming (FG) voert een gegevensbeschermingseffectbeoordeling (DPIA) uit. De FG ontdekt dat alle computers een instelling hebben waardoor er na vijf seconden inactiviteit een schermbeveiliging wordt weergegeven op het beeldscherm. De computers worden echter niet automatisch vergrendeld. Wanneer medewerkers hun bureau verlaten, vergrendelen ze doorgaans hun computer ook niet.

Waar is dit een voorbeeld van?

A) Toegang tot gegevens
B) Inbreuk in verband met persoonsgegevens
C) Beveiligingsincident
D) Kwetsbaarheid in de beveiliging

A) Incorrect. Er is geen toegang verkregen tot de gegevens.
B) Incorrect. Er zijn nog geen persoonsgegevens verwerkt zonder dat hiervoor toestemming was, dus dit is geen inbreuk.
C) Incorrect. De verwerking moet nog beginnen, er is geen reden om aan te nemen dat er zich een incident heeft voorgedaan.
D) Correct. De vertrouwelijkheid van gegevens kan niet worden gegarandeerd als medewerkers hun werkplek verlaten zonder hun computer te vergrendelen. (Literatuur: A, Hoofdstuk 11; Artikel 5(1)(f) van de AVG)

36 / 40
Een architect verlaat een bouwplaats. Hij legt zijn laptop neer om zijn telefoon te beantwoorden. Dan rijdt er een vrachtwagen over de laptop heen. Al zijn bestanden voor het ontwerp van het gebouw en de berekeningen waaraan hij heeft gewerkt, gaan hierbij verloren. De architect heeft een back-up van een eerdere versie van de bestanden opgeslagen in de cloud.

Is dit volgens de AVG een inbreuk in verband met persoonsgegevens?

A) Ja, want door de vernietiging van de laatste kopie van bestanden zijn die bestanden niet meer beschikbaar.
B) Ja, want de vernietigde bestanden waren de persoonlijke bestanden van de architect.
C) Nee, want de ontwerpbestanden en berekeningen zijn geen persoonsgegevens.
D) Nee, want de bestanden zijn nog steeds beschikbaar in de vorm van een back-up.

A) Incorrect. Er zijn geen persoonsgegevens vernietigd.
B) Incorrect. Een persoonlijk bestand is geen synoniem voor persoonsgegevens.
C) Correct. Er zijn geen persoonsgegevens vernietigd, dus dit is geen inbreuk in verband met persoonsgegevens. (Literatuur: A, Hoofdstuk 11; Artikel 4(12) van de AVG)
D) Incorrect. Er was geen inbreuk in verband met persoonsgegevens, maar niet om deze reden. Er zijn geen persoonsgegevens vernietigd.

37 / 40
Na een inbreuk in verband met persoonsgegevens moet een verwerkingsverantwoordelijke binnen de Europese Economische Ruimte (EER) bepalen wie moet worden geïnformeerd:

- Niemand
- Alleen de toezichthoudende autoriteit
- De toezichthoudende autoriteit en alle betrokkenen

In welke situatie moeten **betrokkenen** volgens de AVG op de hoogte worden gesteld van een inbreuk in verband met persoonsgegevens?

A) Wanneer persoonsgegevens worden verwerkt op een locatie van de verwerker die niet binnen de grenzen van de EER ligt
B) Wanneer persoonsgegevens worden verwerkt door een partij die akkoord is gegaan met het concept van de verwerkingsovereenkomst, maar deze nog niet heeft ondertekend
C) Wanneer het systeem waarin de persoonsgegevens worden verwerkt, wordt aangevallen en hierdoor schade aan de opslagapparatuur ontstaat
D) Wanneer de kans aanzienlijk is dat de inbreuk leidt tot een hoog risico voor de privacy van de betrokkenen

A) Incorrect. De locatie waar de gegevens worden verwerkt, is niet relevant voor de verplichting om betrokkenen op de hoogte te brengen van inbreuken in verband met persoonsgegevens.
B) Incorrect. Wanneer persoonsgegevens worden verwerkt door een andere partij dan de verwerkingsverantwoordelijke zonder dat er een geldige schriftelijke overeenkomst is, wordt dit beschouwd als een inbreuk in verband met persoonsgegevens. In de geschetste situatie zijn negatieve gevolgen voor de betrokkenen echter zeer onwaarschijnlijk. In dat geval is het niet verplicht om de betrokkenen op de hoogte te brengen.
C) Incorrect. Schade aan opslagapparatuur maakt het lastig of zelfs onmogelijk om toegang te krijgen tot de gegevens, maar impliceert geen onrechtmatige verwerking.
D) Correct. Als de kans op negatieve gevolgen voor de betrokkenen aanzienlijk is, is de verwerkingsverantwoordelijke verplicht om hen op de hoogte te brengen van de inbreuk. (Literatuur: A, Hoofdstuk 11)

38 / 40
Een systeem dat persoonsgegevens bevat, is gehackt. Nu blijkt dat onbevoegde personen toegang hebben gekregen tot de persoonsgegevens.

Wat moet de verwerkingsverantwoordelijke volgens de AVG doen **voordat** hij de toezichthoudende autoriteit op de hoogte brengt?

A) Beoordelen of er toegang is of kan zijn verkregen tot gevoelige gegevens
B) Een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren om het risico voor natuurlijke personen te beoordelen
C) De getroffen betrokkenen op de hoogte brengen van de inbreuk in verband met persoonsgegevens en de mogelijke gevolgen hiervan
D) De politie op de hoogte brengen en aangifte doen van de onbevoegde toegang tot het systeem

A) Correct. Volgens Artikel 33(1) van de AVG, is kennisgeving niet vereist als "het onwaarschijnlijk is dat de inbreuk in verband met persoonsgegevens zal leiden tot een risico voor de rechten en vrijheden van natuurlijke personen". De verwerkingsverantwoordelijke moet dat controleren voordat hij rapporteert. (Literatuur: A, Hoofdstuk 11; Artikel 33(1) van de AVG)
B) Incorrect. Een DPIA wordt voorafgaand aan de daadwerkelijke verwerking uitgevoerd om te bepalen hoe de verwerking moet worden georganiseerd en welke risico's moeten worden beperkt.
C) Incorrect. Kennisgeving aan de betrokkene is alleen vereist als de inbreuk in verband met persoonsgegevens waarschijnlijk kan leiden tot een hoog risico voor de rechten en vrijheden van de betrokkenen.
D) Incorrect. Het informeren van de politie is niet verplicht volgens de AVG. Het kan wel verstandig zijn.

39 / 40
Toezichthoudende autoriteiten hebben bepaalde taken die gericht zijn op het waarborgen van naleving van de AVG.

Wat is een van die taken?

A) Het beoordelen van gedragscodes voor specifieke sectoren in verband met de verwerking van persoonsgegevens
B) Het definiëren van een minimale set maatregelen die moeten worden genomen om persoonsgegevens en privacy te beschermen
C) Het opstellen van standaard contractbepalingen (SCC) en bindende bedrijfsvoorschriften (BCR)
D) Het onderzoeken van alle inbreuken in verband met gegevens waarvan de toezichthoudende autoriteit op de hoogte is gebracht

A) Correct. Het is een van de verantwoordelijkheden van toezichthoudende autoriteiten om algemeen advies te geven over hoe een bedrijf kan voldoen aan de verordeningen. (Literatuur: A, Hoofdstuk 12)
B) Incorrect. Een toezichthoudende autoriteit geeft algemeen advies over passende beveiligingsniveaus. Zij schrijven geen specifieke maatregelen voor.
C) Incorrect. SCCs worden opgesteld door de Europese Commissie (EC). Toezichthoudende autoriteiten kunnen BCRs voor overdrachten van persoonsgegevens goedkeuren, maar bedrijven stellen ze zelf op.
D) Incorrect. Een toezichthoudende autoriteit heeft geen verplichting en ook geen capaciteit om alle inbreuken in verband met persoonsgegevens te onderzoeken waarvan zij in kennis is gesteld.

40 / 40
Het hoofdkantoor van een verwerkingsverantwoordelijke is gevestigd binnen de Europese Economische Ruimte (EER). De verwerking van gevoelige persoonsgegevens is uitbesteed aan een verwerker buiten de EER, zonder eerst de toezichthoudende autoriteit te raadplegen. Deze overtreding werd ontdekt en het bedrijf kreeg een geldboete van de toezichthoudende autoriteit.

Zes maanden later ontdekt de toezichthoudende autoriteit dat de verwerkingsverantwoordelijke nogmaals dezelfde overtreding heeft begaan, maar voor een andere verwerkingsactiviteit en met een andere verwerker.

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

A) Niets, omdat het bedrijf al een boete heeft gekregen voor deze overtreding
B) Niets, maar er kan een formele waarschuwing zonder financiële sancties worden gegeven
C) Een boete van maximaal €10 miljoen of 2% van de omzet, afhankelijk van wat hoger is
D) Een boete van maximaal €20 miljoen of 4% van de omzet, afhankelijk van wat hoger is

A) Incorrect. Elke overtreding van de AVG kan afzonderlijk worden beboet, vooral als er verschillende verwerkingen of verwerkers bij betrokken zijn. Eerdere boetes stellen het bedrijf dus niet vrij van nieuwe boetes.
B) Incorrect. Aangezien dit een herhaalde overtreding van de regels van de AVG is, is het onwaarschijnlijk dat er alleen een waarschuwing wordt gegeven, want gewoonlijk worden voor voortdurende niet-naleving zeker boetes opgelegd.
C) Incorrect. Het uitbesteden van de verwerking van gevoelige gegevens zonder goed overleg is een ernstige inbreuk, en herhaalde overtredingen kunnen leiden tot hogere boetes onder de AVG.
D) Correct. Dit is de maximale boete voor een herhaalde overtreding van deze aard. De doorgifte van persoonsgegevens aan een ontvanger in een derde land of een internationale organisatie mag worden bestraft met de hoogste boete. (Literatuur: A, Hoofdstuk 12; Artikel 33 van de AVG)

Evaluatie

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

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



Contact EXIN

www.exin.com