



Rendement

Algemene Verordening Gegevensbescherming

Jo Weerts



de laatste wet- en regelgeving boeiend en glashelder gebracht



Rendement

Programma AVG


- algemeen
- verplichtingen
- zorgvuldigheid 1
- rechten betrokkene
- datalekken
- zorgvuldigheid 2
- checklist

2 

Rendement

Volledige organisatie


<ul style="list-style-type: none"> ▪ juridisch <ul style="list-style-type: none"> - verwerkersovereenkomst - geheimhoudingverklaring - privacybeleid ▪ automatisering <ul style="list-style-type: none"> - software- en virusscanners - (veilige) back-ups om persoonsgegevens te beschermen tegen verlies of ransomware - cloud-oplossing binnen EU 	<ul style="list-style-type: none"> ▪ procedures <ul style="list-style-type: none"> - wie heeft waar toegang toe - welke procedure bij datalek - bewaartermijnen ▪ medewerkers <ul style="list-style-type: none"> - opleiding - bewustwording
--	---

3 

Rendement

Europese privacywetgeving

- Europa
 - Richtlijn 95/46/EG betreffende bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende vrije verkeer van die gegevens
 - 24 oktober 1995
- Nederland
 - Wet bescherming persoonsgegevens
 - 1 september 2001
- Europa
 - Algemene verordening gegevensbescherming (AVG)
 - 25 mei 2016 (2 jaar overgangsrecht)

4 

Rendement

Algemene verordening gegevensbescherming


- één Europese regeling
- verbetering van privacyrechten van personen en meer verantwoordelijkheden voor organisaties
 - met bijbehorende sancties
- meer nadruk op verantwoordelijkheid van organisaties zelf om te kunnen aantonen dat zij zich aan wet houden (accountability)
- dezelfde, stevige, bevoegdheden voor alle Europese privacytoezichthouders
- ...

5 

Rendement


Eén regeling

- doel van Verordening is één geharmoniseerd gegevensbeschermingsrecht
 - Verordening biedt lidstaten **op aantal punten ruimte** om specifieke bepalingen op te nemen of uitzonderingen te maken
 - regels omtrent verwerking van bijzondere categorieën van persoonsgegevens
 - invulling van (uitzonderingen op) rechten van betrokkenen
- in Nederland zijn deze specifieke bepalingen vastgelegd in Uitvoeringswet Algemene verordening gegevensbescherming / sectorale wetten die bepalingen bevatten over verwerking van persoonsgegevens op het terrein dat zij bestrijken

6 


**Algemene Verordening Gegevensbescherming
directe werking**

- nieuwe wetgeving betreft verordening
 - regels hebben **directe werking**
 - enkele regels ter uitvoering van AVG 2018 staan in uitvoeringswet AVG
- per **25 mei 2018** is Algemene verordening gegevensbescherming (AVG) definitief van toepassing
 - vanaf die datum dezelfde privacywetgeving in hele Europese Unie (EU)
- Wet bescherming persoonsgegevens (Wbp) / Wet meldplicht datalekken geldt dan niet meer

7 


Boete

- komt verantwoordelijke (een van de) **verplichtingen** niet na
 - maximaal € 10 miljoen
 - of 2% van wereldwijde jaaromzet (mocht dat bedrag hoger uitkomen)
- overtreedt verantwoordelijke beginselen of grondslagen van AVG / **privacyrechten** van betrokkenen
 - maximaal € 20 miljoen
 - of 4% van wereldwijde jaaromzet (mocht dat bedrag hoger uitkomen)

8 

**Persoonsgegevens
artikel 4 lid 1 AVG**


- alle informatie over geïdentificeerde of identificeerbare natuurlijke persoon (betrokkene)
 - als identificeerbaar wordt beschouwd natuurlijke persoon die direct of indirect kan worden geïdentificeerd
 - aan hand van identificator zoals naam / identificatienummer / locatiegegevens / online identificator
 - aan de hand van een of meer elementen die kenmerkend zijn voor fysieke / fysiologische / genetische / psychische / economische / culturele of sociale identiteit van die natuurlijke persoon

9 

Rendement

Persoonsgegevens

- naam
- adres
- woonplaats
- telefoonnummer
- postcode
- huisnummers
- e-mailadres
- ...


10 

Rendement

Verwerking

artikel 4 lid 2 AVG


- verzamelen / vastleggen / ordenen / structureren / opslaan / bijwerken of wijzigen / opvragen / raadplegen / gebruiken / verstrekken door middel van doorzending / verspreiden of op andere wijze ter beschikking stellen / aligneren of combineren / afschermen / wissen of vernietigen van gegevens

11 

Rendement

Geheel of gedeeltelijk geautomatiseerde verwerking / opname in een bestand

- geautomatiseerde verwerking
 - bewerkingen die worden uitgevoerd met behulp van computers / smartphones / tablets / servers / databases / ...
- persoonsgegevens in bestand worden opgenomen of bestemd zijn om daarin opgenomen te worden
 - gestructureerde verzameling persoonsgegevens die via bepaalde logica toegankelijk is
 - archiefkast / geordende verzameling naamkaartjes / ...
 - losse papieren op bureau met daarin namen van personen vormen geen bestand
- puur mondelinge overdracht van gegevens is geen verwerking van persoonsgegevens

12 

Verwerkingsverantwoordelijke - verwerker

- verwerkingsverantwoordelijke (natuurlijke persoon of rechtspersoon -bedrijf / stichting / overheidsorgaan / ...- die alleen of tezamen met anderen doel en middelen vaststelt voor verwerking)
 - verwerkt gegevens voor eigen doeleinden
- verwerker
 - gegevens mogen alleen in opdracht van verwerkingsverantwoordelijke worden verwerkt (niet voor eigen doeleinden)
 - uitbestede / gedelegeerde verwerkingsactiviteiten (die verwerkingsverantwoordelijke ook zelf had kunnen verrichten)
 - dienstverlening moet gericht zijn op verwerken van persoonsgegevens ten behoeve van verwerkingsverantwoordelijke



Verwerkersovereenkomst (data processing agreement)

artikel 28 lid 3 AVG

- verwerkingsverantwoordelijke en verwerker **verplicht** om aantal onderwerpen vast te leggen in schriftelijke overeenkomst
 - algemene beschrijving
 - onderwerp / duur / aard en doel van verwerking / soort persoonsgegevens / categorieën van betrokkenen / rechten en verplichtingen als verwerkingsverantwoordelijke
 - geheimhoudingsplicht
 - beveiliging
 - ...

inzien van gegevens door externe helpdesk is verwerking

14



Onderwerpen in verwerkersovereenkomst 1

- verwerking in overeenstemming met instructies verantwoordelijke
- verwerker mag persoonsgegevens niet voor eigen doeleinden gebruiken
 - alleen om uitvoering te geven aan instructies van verantwoordelijke
- geheimhouding
 - opzettelijke niet-naleving van geheimhoudingsplicht is strafbaar gesteld in Wetboek van Strafrecht
- beveiligingsmaatregelen
 - passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies e.d.


15



Rendement

Onderwerpen in verwerkersovereenkomst 2

- inschakelen derden / onderaannemers
 - of, en onder welke voorwaarden verwerker subbewerkers mag inschakelen
- locatie van data
 - verantwoordelijke moet weten in welke landen data worden opgeslagen
 - mede van belang met oog op verplichtingen die gelden bij doorgifte van persoonsgegevens naar buitenland / buiten EU
- audits
 - verantwoordelijke moet kunnen controleren of verwerker zich houdt aan gemaakte afspraken

16 

Rendement

Onderwerpen in verwerkersovereenkomst 3

- aansprakelijkheid
 - wet bepaalt dat **verantwoordelijke** kan worden aangesproken als iemand schade lijdt doordat AVG niet wordt nageleefd
 - geldt zelfs als schade gevolg is van nalatigheid van verwerker
 - verwerker ook zelfstandig aansprakelijk
 - » artikel 82 AVG

17 

Rendement

Gegevensverwerking grondslag

- noodzakelijk
- zo privacy-vriendelijk mogelijk
- proportioneel

18 

Beginnselen verwerking persoonsgegevens artikel 5 AVG

- rechtmatig / behoorlijk / transparant
- voor welbepaalde, **uitdrukkelijk omschreven** en gerechtvaardigde doeleinden verzameld (doelbinding)
- minimale gegevensverwerking
- juistheid
- opslagbeperking
- integriteit en verantwoordelijkheid

verantwoordingsplicht

Rechtmatigheid van de verwerking 1 aan ten minste één voorwaarde is voldaan - artikel 6 AVG

- noodzakelijk voor uitvoering van **overeenkomst** waarbij betrokkene partij is
 - arbeidsovereenkomst / leasecontract / ...
- noodzakelijk om te voldoen aan **wettelijke verplichting**
 - loonaangifte belastingdienst / ziekmelding bij arbodienstverlener / ...
- betrokkene heeft **toestemming** gegeven voor verwerking van persoonsgegevens voor een of meer specifieke doeleinden
 - cookies website / online boeken hotelkamer / ...

Rechtmatigheid van de verwerking 2 aan ten minste één voorwaarde is voldaan - artikel 6 AVG

- noodzakelijk om **vitale belangen** betrokkene / andere natuurlijke persoon te beschermen
 - naam bewusteloze werknemer doorgeven aan ambulancebroeder / ...
- noodzakelijk voor **algemeen belang**
 - gegevens doorgeven aan Kadaster / ...
- noodzakelijk voor **gerechtvaardigde belangen**
 - presentielijst / BKR-toets nieuwe klanten / ...

Rendement

Verwerking van bijzondere categorieën van persoonsgegevens - artikel 9 AVG

- verwerking van persoonsgegevens waaruit
 - ras of etnische afkomst / politieke opvattingen / religieuze of levensbeschouwelijke overtuigingen / lidmaatschap vakbond / ... / gegevens over gezondheid / gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid blijken is **verboden**

22 

Rendement

Verwerking van bijzondere categorieën van persoonsgegevens - uitzonderingen (artikel 9, lid 2)


- verwerking is **noodzakelijk** met oog op uitvoering van verplichtingen en uitoefening op gebied van arbeidsrecht en sociale zekerheidsrecht
- betrokkene heeft uitdrukkelijke **toestemming** gegeven voor verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden
- ...

23 

Rendement

Bijzondere persoonsgegevens
o.a.


- godsdienst of levensovertuiging
- ras
- salarisgegevens
- politieke voorkeur
- gezondheid
- seksuele leven
- lidmaatschap vakbond
- strafrechtelijk verleden
- Burgerservicenummer (?)

24 

Rendement

Burgerservicenummer (BSN)


- uniek tot persoon herleidbaar nummer
 - persoonsnummer dat in eerste plaats bedoeld is voor contact tussen burgers en overheid
- organisaties buiten overheid mogen BSN alleen gebruiken als dat **wettelijk** is bepaald (wet / amvb)
 - alleen voor doel dat in wet staat omschreven
 - zorgverlener (huisarts / tandarts) is bijvoorbeeld verplicht BSN te gebruiken (Wet gebruik burgerservicenummer in de zorg)
 - banken moeten BSN gebruiken voor uitwisseling van gegevens met Belastingdienst (Algemene Wet inzake Rijksbelastingen)

25 

Rendement

Voorwaarden voor toestemming artikel 7 AVG


- kunnen aantonen dat betrokkene toestemming heeft gegeven voor verwerking van zijn persoonsgegevens
 - duidelijke **actieve handeling**
 - schriftelijke verklaring (ook met elektronische middelen) / mondelinge verklaring, waaruit blijkt dat betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met verwerking van persoonsgegevens instemt
 - begrijpelijke en gemakkelijk toegankelijke vorm / in duidelijke en eenvoudige taal (niet 'verstopt' tussen andere zaken)
- betrokkene heeft recht toestemming te allen tijde in te trekken
 - net zo makkelijk om toestemming in te trekken als om die te geven

26 

Rendement

Toestemming

- in arbeidsverhouding, waarin werknemer financieel afhankelijk is van werkgever
 - over algemeen geen sprake van 'vrije' toestemming

27 

Mag school foto's van leerlingen op internet publiceren


- ja
 - van iedere leerling van wie foto wordt gepubliceerd toestemming nodig
 - leerlingen van 16 jaar of ouder mogen zelf toestemming geven
 - voor leerlingen die jonger zijn dan 16 jaar toestemming nodig van ouders of voogd
- specifiek doel
 - mag foto's niet voor ander doel gebruiken zonder daar apart toestemming voor te vragen

foto werknemer op website

28 


Transparantie

- persoonsgegevens moeten worden verwerkt op wijze die ten aanzien van betrokkene rechtmatig / behoorlijk / transparant is
 - voor betrokkene duidelijk dat zijn persoonsgegevens verzameld / gebruikt / geraadpleegd / op andere manier verwerkt worden / waarom en door wie
- bedrijf dat gegevens over iemand verzamelt neemt bepaalde verantwoordelijkheid op zich / kan daarover verantwoording afleggen
 - bijhouden van administratie waarin **privacy-beleid** en daarbij gemaakte keuzes neergelegd zijn
- informatie moet in duidelijke eenvoudige taal / op toegankelijke en begrijpelijke manier afgestemd zijn op doelgroep

29 

Transparantie 2

- informatie moet in duidelijke eenvoudige taal / op toegankelijke en begrijpelijke manier afgestemd zijn op doelgroep


30 

Rendement

Verplichtingen

programma

- register met alle verwerkingen
- gegevensbeschermingsbeleid (privacybeleid)
 - privacy statement / privacyverklaring
- (digitale) beveiliging


31 

Rendement

Documentatieplicht

artikel 30 AVG

- elke verwerkingsverantwoordelijke houdt schriftelijk en elektronisch **register van verwerkingsactiviteiten** die onder zijn verantwoordelijkheid plaatsvinden
 - moet op elk moment actueel / compleet inzicht geven
 - bijvoorbeeld EXCEL-spreadsheet
- register kan vanaf 25 mei 2018 door AP worden **opgevraagd** in kader van controles
- **verwerker** moet register bijhouden van verwerkingsactiviteiten die verwerker ten behoeve van verwerkingsverantwoordelijke (klant) heeft verricht

32 

Rendement

Register van de verwerkingsactiviteiten


niet van toepassing

- niet van toepassing op ondernemingen of organisaties die minder dan 250 personen in dienst hebben
 - jaaronzet van maximaal 50 miljoen of jaarlijks balanstotaal van maximaal 43 miljoen
- tenzij waarschijnlijk is dat
 - verwerking **risico** inhoudt voor rechten en vrijheden van betrokkenen *of*
 - verwerking **niet incidenteel** is *of*
 - verwerking **bijzondere** persoonsgegevens

33 

Hoog risico
voorgenomen verwerking aan 2 of meer criteria voldoet

- gevoelige gegevens of gegevens van zeer persoonlijke aard
- op grote schaal verwerkte gegevens
- gegevens met betrekking tot kwetsbare betrokkenen
- evaluatie van personen of scoretoekenning
- geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg
- stelselmatige monitoring
- matching of samenvoeging van datasets
- blokkering van recht, dienst of contract
- ...

34 

Niet-incidentele verwerking

- elke verwerking met zekere bestendigheid
 - bijvoorbeeld bijhouden van klantendatabase of personeelsadministratie

35 

Register van de verwerkingsactiviteiten - 1a
artikel 30 AVG

- naam en contactgegevens verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken / functionaris voor gegevensbescherming (wie)
- beschrijving van de categorieën van betrokkenen / categorieën van persoonsgegevens (wat)
- verwerkingsdoeleinden (waarom)
- categorieën van ontvangers aan wie persoonsgegevens zijn of zullen worden verstrekt
 - waar worden gegevens gelokaliseerd / doorgegeven

36 

Rendement

Register van de verwerkingsactiviteiten - 1b
artikel 30 AVG

- indien mogelijk, beoogde termijnen waarbinnen verschillende categorieën van gegevens moeten worden gewist
 - tot wanneer worden gegevens bewaard
- indien mogelijk, algemene beschrijving van technische en organisatorische beveiligingsmaatregelen
 - hoe worden gegevens beveiligd

37 

Rendement

Register van de verwerkingsactiviteiten
verwerker - artikel 30 lid 2 AVG


- ook **verwerker** is verplicht om register van de verwerkingsactiviteiten bij te houden
 - naam en contactgegevens van verwerkers, van verwerkingsverantwoordelijke(n) en functionaris voor gegevensbescherming
 - categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd
 - doorgiften van persoonsgegevens aan derde land of internationale organisatie (indien van toepassing)
 - indien mogelijk algemene beschrijving van technische en organisatorische maatregelen die genomen zijn om te beveiligen

38 

Rendement

Gegevensbeschermingbeleid (privacybeleid) 1


- wie bent u / hoe kan betrokkene contact opnemen met u en (indien van toepassing) uw Functionaris Gegevensbescherming
 - contactgegevens
- waarom verzamelt u persoonsgegevens en waarom mag dat
 - doelomschrijving / rechtsgrond / gerechtvaardigd belang
- aan wie gaat u persoonsgegevens verder nog verstrekken (buiten EU?)

39 

Rendement

Gegevensbeschermingbeleid (privacybeleid) 2

- waar / hoe kan betrokkene vragen om inzage / rectificatie / wissen van persoonsgegevens (right to be forgotten) / klachten indienen / bezwaar maken / gegevensoverdraagbaarheid
- hoe kan betrokkene verleende toestemming intrekken
- is verstrekking van persoonsgegevens wettelijke of contractuele verplichting / noodzakelijke voorwaarde om overeenkomst te sluiten

40 

Rendement

Gegevensbeschermingbeleid (privacybeleid) 3

- is betrokkene verplicht om gevraagde persoonsgegevens te verstrekken of niet
 - wat zijn gevolgen als hij/zij persoonsgegevens niet verstrekt
 - noodzaak
- hoe lang verwacht u persoonsgegevens te gaan bewaren
- bestaan van profiling of geautomatiseerde besluitvorming
- indien gegevens niet van betrokkene worden verkregen, bron waar persoonsgegevens vandaan komen ...

41 

Rendement

Privacy statement / privacyverklaring

- alle organisaties die persoonsgegevens verwerken, moeten mensen heldere informatie geven over persoonsgegevens die zij verwerken en voor welk(e) doel(en) zij deze gegevens verwerken
 - verkorte versie van gegevensbeschermingsbeleid op website
 - makkelijk te lezen / te begrijpen
 - makkelijk te vinden

zie bijvoorbeeld privacyverklaring op website consumentenbond / autoriteit persoonsgegevens

42 

Rendement

Beveiliging van persoonsgegevens

- bij verwerking van persoonsgegevens voldoende **technische** en **organisatorische** maatregelen treffen om gegevens te beveiligen
 - bijvoorbeeld: wie heeft toegang tot welke gegevens?


blijvend punt van aandacht

43 

Rendement

Zorgvuldigheid *programma*

- **privacy by design / privacy by default**
- functionaris voor de gegevensbescherming
- impact assesment

44 

Rendement

Privacy by design / Privacy by default ontwerp / standaardinstellingen

- bij **ontwerpen** van producten en diensten zorgen dat persoonsgegevens goed worden beschermd
 - afvragen of het écht nodig is persoonsgegevens te verwerken
 - kan bijvoorbeeld gewerkt worden met **geanonimiseerde** gegevens
 - toch persoonsgegevens verwerken
 - nadenken over beveiliging van deze gegevens
 - bijvoorbeeld door **pseudonimiseren**
- instellingen van programma / app / website / dienst zodanig dat maximale privacy wordt betracht
 - **standaardinstellingen** altijd zo privacy-vriendelijk mogelijk

45 

Rendement

Voorbeeld
online-bestelproces


- vragen naar adres zal mogelijk noodzakelijk zijn om product te kunnen afleveren
 - niet noodzakelijk bij e-tickets voor concert / voorstelling
 - telefoonnummer?
- geboortedatum is hoogstwaarschijnlijk niet noodzakelijk
 - tenzij bierpakket wordt besteld

46 

Rendement

Bewaren van persoonsgegevens

- niet langer bewaren dan **noodzakelijk** is voor **doel**
 - psychologische test / loonbeslag / ...
- geen concrete bewaartermijn in AVG
 - organisaties bepalen zelf hoe lang zij persoonsgegevens bewaren
- wel concrete bewaartermijnen in andere wetten
 - belastingwetgeving / ...
- richtlijn: bewaartermijn van (maximaal) 2 jaar nadat werknemer uit dienst is

47 

Rendement

Dossier digitaliseren


- originele papieren dossier pas vernietigen als organisatie zorgt voor goede beveiliging van digitale dossier

48 

Rendement

Rechten betrokkene
programma

- recht op informatie
- recht op inzage
- recht om te wijzigen
- recht om vergeten te worden
- recht op beperking van de verwerking
- recht om gegevens over te dragen

49 

Rendement

Recht op informatie
artikel 13 en 14 AVG


- betrokkene moet **op hoogte worden gesteld** van feit dat verwerking van zijn persoonsgegevens plaatsvindt of zal plaatsvinden en wat doeleinden hiervan zijn
 - informatie over periode / rechten van betrokkene / bron van gegevens / juridische grondslag voor verwerking / ...
 - verandert doel van verwerking, moet ook daarover informatie worden verstrekt

50 

Rendement

Te verstrekken informatie wanneer persoonsgegevens bij betrokkene worden verzameld (artikel 13 AVG) 1

- identiteit en contactgegevens van verwerkingsverantwoordelijke en, in voorkomend geval, van vertegenwoordiger van verwerkingsverantwoordelijke
 - in voorkomend geval, contactgegevens van functionaris voor gegevensbescherming
- bewaartermijn, of als dat niet mogelijk is criteria voor bepalen ervan
- rechten van betrokkene
 - recht op informatie / recht op inzage / recht om te wijzigen / recht om vergeten te worden / recht op beperking van de verwerking / recht om gegevens over te dragen

51 


Te verstrekken informatie wanneer persoonsgegevens bij betrokkene worden verzameld (artikel 13 AVG) 2

- verwerkingsdoeleinden waarvoor persoonsgegevens zijn bestemd, alsook rechtsgrond voor verwerking
 - of verwerken van persoonsgegevens wettelijke verplichting is / noodzakelijk is voor uitvoering of aangaan van overeenkomst
 - of betrokkene verplicht is die gegevens te verstrekken en wat gevolgen zijn van niet verstrekken van die gegevens voor betrokkene
 - wanneer u verwerking baseert op grondslag 'gerechtvaardigd belang' wat gerechtvaardigd belang is
- in geval van toestemming, dat betrokkene die toestemming altijd weer kan intrekken

52 


Te verstrekken informatie wanneer persoonsgegevens bij betrokkene worden verzameld (artikel 13 AVG) 3

- in voorkomend geval, ontvangers of categorieën van ontvangers van persoonsgegevens
- in geval van verstrekking aan derde landen
 - of er een adequaatheidsbesluit van de Commissie bestaat
 - of passende waarborgen zijn getroffen, welke dit zijn en of hier kopie van kan worden verkregen, dan wel waar die waarborgen kunnen worden geraadpleegd
- in geval van geautomatiseerde besluitvorming, nuttige informatie over onderliggende logica, belang van verwerking en verwachte gevolgen van die verwerking voor betrokkene

53 

Te verstrekken informatie wanneer persoonsgegevens bij betrokkene worden verzameld (artikel 13 AVG) 4


- alle andere informatie die noodzakelijk is om tegenover betrokkene behoorlijke en transparante verwerking te waarborgen
 - zelf bepalen welke aanvullende informatie (naast verplichte elementen) het eventueel zou betreffen
- als u persoonsgegevens voor andere doelen verder gaat verwerken, moet u betrokkene opnieuw worden geïnformeerd over dat nieuwe doel
 - opnieuw alle hierboven genoemde informatie verstrekken
 - behalve voor zover betrokkene al van die informatie op de hoogte is

54 

Rendement

Te verstrekken informatie wanneer persoonsgegevens NIET bij betrokkene worden verzameld (artikel 14 AVG)

- wanneer u gegevens verzamelt buiten betrokkene om moet u in beginsel dezelfde informatie verstrekken als wanneer u gegevens van betrokkene zelf heeft gekregen
 - enige dat u moet toevoegen is bron waaruit persoonsgegevens zijn verkregen
 - als bron van informatie niet kan worden vastgesteld dient u algemene informatie over herkomst te verstrekken

55 

Rendement

Inzagerecht
artikel 15 AVG


- recht op inzage in eigen persoonsgegevens
 - vragen of persoonsgegevens zijn vastgelegd en zo ja, welke
 - hoeft geen reden te geven voor inzageverzoek

56 

Rendement

Reikwijdte inzage recht

- betreft alleen inzage in iemands eigen gegevens
 - of organisatie zijn persoonsgegevens gebruikt
 - om welke gegevens het gaat
 - wat doel is van het gebruik
 - aan wie organisatie de gegevens eventueel heeft verstrekt
 - wat herkomst is van de gegevens (als deze bekend is)
- organisatie is verplicht binnen 4 weken schriftelijk of per e-mail te reageren op inzageverzoek
- volledig overzicht / kopieën-afdrukken / inzage ter plekke

57 

Recht van kopie
artikel 15 lid 3 AVG

- verwerkingsverantwoordelijke verstrekt betrokkene kopie van persoonsgegevens die worden verwerkt

Elektronische opgave loonbedrag
7:626 BW

- voor verstrekken van elektronische opgave is uitdrukkelijke instemming van werknemer vereist
- ...

Recht op correctie en verwijdering (rectificatie)
artikel 16 AVG

- persoonsgegevens te verbeteren / aan te vullen / te verwijderen / ...
 - feitelijk onjuist
 - onvolledig of niet ter zake doen voor doel waarvoor ze zijn verzameld
 - op andere manier in strijd met wet worden gebruikt
- eisen dat organisatie correctie / verwijdering **doorgeeft** aan alle andere organisaties die deze gegevens hebben gekregen

Rendement

Recht op vergetelheid
artikel 17 AVG

- organisaties moeten in aantal gevallen persoonsgegevens wissen als betrokkene erom vraagt

*Recht op gegevenswissing
Recht auf Vergessenwerden*

61 

Rendement

Recht op beperking van de verwerking
artikel 18 AVG

- betrokkene heeft recht van verwerkingsverantwoordelijke beperking van de verwerking te verkrijgen
 - verwerking is onrechtmatig en betrokkene verzet zich tegen het wissen van persoonsgegevens en verzoekt in plaats daarvan om beperking van het gebruik ervan
 - verwerkingsverantwoordelijke heeft persoonsgegevens niet meer nodig voor verwerkingsdoeleinden
 - betrokkene heeft deze nodig voor instelling / uitoefening / onderbouwing van een rechtsvordering
 - ...


62 

Rendement

Recht op dataportabiliteit - 1
artikel 20 AVG

- recht op overdraagbaarheid van persoonsgegevens
 - recht hebben om persoonsgegevens te ontvangen die organisatie van je heeft
- organisatie die gegevens verstrekt, mag betrokkenen hierin niet tegenwerken
 - moet ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen / doorgeven

digitale gegevens

63 

**Recht op dataportabiliteit - 2
artikel 20 AVG**

- gegevens zelf opslaan voor persoonlijk (her)gebruik
- gegevens makkelijk doorgeven aan andere leverancier van dezelfde soort dienst
 - uitschrijven bij ene sociale netwerksite en inschrijven bij andere
 - overstappen naar andere telecomprovider
 - ...
- kan eisen dat organisatie persoonsgegevens direct doorstuurt aan nieuwe dienstverlener
 - als dat (technisch) mogelijk is

**Trendonderzoek salarisprofessionals 2017 NIRPA
datalekken**

- 60% organisaties heeft procedure die voorschrijft hoe er omgegaan moet worden met datalekken
- 21% geeft aan dat er geen procedure is
- 19% geeft aan niet te weten of er procedure bestaat


Persoonsgegevens van gevoelige aard

- bijzondere persoonsgegevens
 - godsdienst / levensovertuiging / ras / gezondheid / ...
- gegevens over financiële of economische situatie van betrokkene
 - (problematische) schulden / salaris / ...
- gegevens die kunnen worden misbruikt voor (identiteits)fraude
 - kopieën van identiteitsbewijzen / Burgerservicenummer / ...
- ...

Rendement

Wanneer hoeft u datalek niet te melden

- hoeft niet aan getroffen personen gemeld te worden wanneer gelekte persoonsgegevens onleesbaar zijn
 - persoonsgegevens versleuteld zijn
 - wanneer gegevens op afstand verwijderd kunnen worden van bijvoorbeeld gestolen laptop
 - moet er dan wel zeker van zijn dat niemand gegevens heeft kunnen inzien
- beoordeling of datalek gemeld moet worden aan toezichthouder en/of getroffen personen ligt te allen tijde bij verwerkingsverantwoordelijke

67 

Rendement

Wanneer datalek melden aan toezichthouder
artikel 33 AVG

- ‘ernstige’ datalekken zonder onnodige vertraging
 - zo mogelijk niet later dan 72 uur na ontdekking bij toezichthouder melden
- kan ernstig zijn als het grote hoeveelheid data betreft (kwantitatief ernstig) / als het om gevoelige gegevens gaat (kwalitatief ernstig)

68 

Rendement

Wanneer datalek melden aan getroffen personen
artikel 34 AVG

- indien datalek waarschijnlijk ongunstige gevolgen heeft voor privéleven van personen van wie gegevens gelekt zijn
 - naast melding aan toezichthouder lek tevens onverwijld melden aan personen waarvan gegevens zijn gelekt
- ongunstige gevolgen
 - identiteitsfraude / discriminatie / reputatieschade / ...
- wanneer kwalitatief ernstige gegevens zijn gelekt is eigenlijk altijd sprake van ongunstig gevolg
 - moet dus ook altijd worden gemeld aan getroffen personen

69 

Inbreuken documenteren

artikel 33 lid 5 AVG

- verwerkingsverantwoordelijke documenteert **alle** inbreuken in verband met persoonsgegevens
 - dus ook niet-meldingsplichtige datalekken
 - feiten omtrent inbreuk in verband met persoonsgegevens / gevolgen daarvan / genomen corrigerende maatregelen

70 

Inbreuken melden - verwerker

artikel 33 lid 2 AVG

- **verwerker** informeert verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van inbreuk in verband met persoonsgegevens

71 

Data Privacy impact assessment (DPIA)

gegevensbeschermingseffectbeoordeling - artikel 35 AVG

- instrument om **vooraf** privacy-risico's van gegevensverwerking in kaart te brengen
 - vervolgens maatregelen te kunnen nemen om risico's te verkleinen
- verplicht als gegevensverwerking waarschijnlijk hoog privacy-risico oplevert voor betrokkenen (mensen van wie organisatie gegevens verwerkt)
 - systematisch en uitvoerig persoonlijke aspecten evalueert
 - waaronder profiling
 - op grote schaal bijzondere persoonsgegevens verwerkt
 - op grote schaal en systematisch mensen volgt in publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht)

72 

In welke gevallen moet u DPIA uitvoeren


- werkgroep van Europese privacytoezichhouders (WP29) heeft lijst van 10 criteria opgesteld
 - aan hoe meer criteria verwerking voldoet, hoe waarschijnlijker het is dat deze hoog risico oplevert

Autoriteit Persoonsgegevens (AP) werkt aan lijst met verwerkingen waarvoor u DPIA moet uitvoeren

73 

DPIA uitvoeren
voorbeelden

- ziekenhuis dat patiëntgegevens verwerkt
- vervoersmaatschappij die reisinformatie verwerkt
 - bijvoorbeeld door reizigers te volgen via vervoerskaarten
- verwerker die gespecialiseerd is in marktonderzoek en voor klant actuele locatiegegevens van hun klanten verwerkt voor statistische doeleinden
- verzekeringsmaatschappij of bank die klantgegevens verwerkt
- zoekmachine die persoonsgegevens verwerkt om advertenties te kunnen tonen op basis van internetgedrag

74 

Wanneer hoef ik geen DPIA uit te voeren?

- wanneer gegevensverwerking
 - waarschijnlijk geen hoog privacyrisico oplevert
 - sterk lijkt op een andere gegevensverwerking waarvoor al DPIA is uitgevoerd
 - wordt geregeld door andere Europese of nationale wet en er bij totstandkoming van deze wet al DPIA is uitgevoerd
 - tenzij privacytoezichhouder oordeelt dat er toch DPIA nodig is
- op lijst staat van verwerkingen waarvoor DPIA niet verplicht is

75 

Geen DPIA uitvoeren voorbeelden

- verwerking van persoonsgegevens van patiënten of cliënten door individuele arts / andere zorgprofessional / advocaat
- online tijdschrift dat mailinglist gebruikt om zijn abonnees algemene dagelijkse verzamelmail te sturen
- internetwinkel die op website advertenties voor oldtimeronderdelen toont
 - daarbij beperkte profielbepaling toepast op basis van items die op eigen website zijn bekeken of gekocht

Functionaris voor de gegevensbescherming (FG) Data Protection Officer (DPO) - artikel 37 AVG

- **natuurlijke persoon** die binnen organisatie toezicht houdt op toepassing en naleving van AVG
 - in 3 situaties verplicht
 - **overheidsinstanties** en publieke organisaties altijd verplicht om FG aan te stellen (ongeacht type gegevens dat ze verwerken)
 - organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen (observaties)
 - profilering van mensen voor maken van risico-inschattingen / cameratoezicht / ...
 - op grote schaal bijzondere persoonsgegevens verwerken en dit kernactiviteit is


Kernactiviteiten

- processen die essentieel zijn om doelen van organisatie te bereiken, of die tot hoofdtaken van organisatie horen
 - verwerking van gegevens over gezondheid is kernactiviteit van ziekenhuis
 - verwerking van persoonsgegevens die ondersteunend is aan bedrijfsvoering, zoals salarisadministratie, valt dan buiten kernactiviteiten

Rendement

Verwerking op grote schaal


- Verordening laat in het midden wat verwerking op grote schaal is
 - u moet dit zelf bepalen / beoordeling is afhankelijk van concrete situatie
 - aantal betrokkenen (hetzij als specifiek aantal, hetzij als deel van relevante populatie)
 - hoeveelheid gegevens die u verwerkt
 - duur of permanente karakter van gegevensverwerking
 - geografische omvang van verwerking
 - ...

79 

Rendement

Eén FG voor meerdere onderdelen / organisaties


- meerdere bedrijfsonderdelen kunnen samen één FG aanstellen
- ook groep organisaties kan gezamenlijke FG benoemen
- voorwaarde voor gezamenlijke FG is dat deze persoon goed bereikbaar is vanuit elke afdeling en vestiging

80 

Rendement

Plichten verwerkingsverantwoordelijke 1 checklist

- register van verwerkingsactiviteiten bijhouden
- informatievoorziening aan betrokkenen op schrift stellen
- privacybeleid opstellen
- vastleggen van wijze waarop toestemming wordt gevraagd
 - bewijs dat deze toestemming daadwerkelijk is gegeven documenteren
- gerechtvaardigd belang documenteren
- functionaris voor gegevensbescherming aanstellen
- gegevensbeschermingseffectbeoordeling uitvoeren

81 


Plichten verwerkingsverantwoordelijke 2 checklist

- privacy by design & default
- passende beveiligingsmaatregelen treffen
- in geval van datalek melding doen bij Autoriteit Persoonsgegevens / onder bepaalde omstandigheden betrokkenen daarover informeren
- afspraken maken met verwerkers
- Autoriteit Persoonsgegevens onder bepaalde omstandigheden **voorafgaand** aan nieuwe risicovolle verwerkingsactiviteit **raadplegen**

82 


Plichten verwerker 1 checklist

- verwerkt persoonsgegevens alleen onder schriftelijke instructies van verwerkingsverantwoordelijke
 - onder andere voor wat betreft doorgifte van persoonsgegevens aan derde land of internationale organisatie (tenzij deze daartoe wettelijk is verplicht)
- waarborgt dat toegang tot die gegevens is beperkt tot gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting

83 

Plichten verwerker 2 checklist

- houdt verplicht overzicht bij van alle categorieën persoonsgegevens die hij verwerkt in opdracht van verwerkingsverantwoordelijke (registerplicht)
- biedt verwerkingsverantwoordelijke alle mogelijke ondersteuning bij nakomen van diens verplichtingen met oog op beantwoording van verzoeken rondom rechten van betrokkenen
- staat verwerkingsverantwoordelijke bij bij nakomen van diens verplichtingen op gebied van beveiliging van persoonsgegevens / meldplicht datalekken
 - stelt verwerkingsverantwoordelijke onverwijld op hoogte stellen van datalek

84 

**Plichten verwerker 3
checklist**

- hanteert minimaal hetzelfde niveau van beveiliging van persoonsgegevens hanteert als verwerkingsverantwoordelijke
 - neemt passende technische en organisatorische beveiligingsmaatregelen die passend beschermingsniveau bieden met oog op risico van de gegevensverwerking voor betrokkenen
- geeft na beëindiging van overeenkomst in opdracht van verwerkingsverantwoordelijke verwerkte persoonsgegevens terug (of wist) verwijderd bestaande kopieën
- maakt afspraken met betrekking tot sub-verwerkers

**Plichten verwerker 4
checklist**

- stelt verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aantoonbaar te maken dat verplichtingen op grond van Verordening rondom inzetten van verwerker worden nageleefd en die nodig is om audits mogelijk te maken
- verleent medewerking bij verzoek van toezichthouder (Autoriteit Persoonsgegevens) in kader van uitoefening van diens taken
- stelt in bepaalde gevallen functionaris voor gegevensbescherming aan

Do's / don'ts

- laat documenten met persoonsgegevens nooit onbeheerd achter op bureau of bij printer
- kies nooit voor automatisch opslaan van inloggegevens op je computer
- beseft dat openbare netwerken niet veilig zijn
- let op wat je deelt via sociale media
- bedek altijd je webcam om 'meekijken' te voorkomen
- geef je inloggegevens niet door aan collega
- blokkeer altijd beeldscherm bij verlaten van werkplek
- ...

Onrechtmatig verwerken van persoonsgegevens

ECLI:NL:RBNNE:2017:1700

- Wettelijke schuldsaneringsregeling natuurlijke personen (Wsnp) is van toepassing verklaard op verzoekster
 - enkele persoonsgegevens van verzoekster gepubliceerd in Staatscourant
- bij brief van 12 mei 2016 heeft advocatenkantoor aan verzoekster aanbod tot rechtsbijstand gedaan (*direct marketing*)
- rechtbank van oordeel dat advocatenkantoor -alleen al door overtypen van gegevens uit Staatscourant, zelfs zonder deze gegevens op te slaan- persoonsgegevens heeft verwerkt
 - geen gerechtvaardigd belang van advocatenkantoor bij verwerking van persoonsgegevens (art. 8, sub f Wbp)

88 

Checklist AVG 1

- zorg dat u weet welke **regels** gelden voor type (bijzondere) gegevens dat u verwerkt en probeer gebruik ervan zoveel mogelijk te beperken
- stel **overzicht** verwerken persoonsgegevens op (artikel 13 + 14 AVG)
- begin op tijd met in kaart brengen van alle verwerkingsactiviteiten zodat alle informatie op tijd in **register** is opgenomen (artikel 30 AVG)
 - ook **verstandig** indien niet verplicht
- stel **privacy-beleid** op
 - zorg dat werknemers op de hoogte zijn van / handelen naar inhoud

89 

Checklist AVG 2

- stel **privacy-statement** op
- loop alle bestaande **verwerkersovereenkomsten** na en kijk of deze (nog) voldoen aan alle eisen
- denk tijdens ontwerp- en ontwikkelingsproces van systemen en processen al na over privacy (**privacy by design**)
- meldplicht datalekken
 - neem kennis van procedure (**draaiboek**) / stel procedure op
- tref bij verwerking van persoonsgegevens voldoende **technische** en **organisatorische** maatregelen om gegevens te beveiligen

90 

Checklist AVG 3

- ga na of er binnen organisatie verwerkingen plaatsvinden met hoog risico en bepaal of **DPIA** op z'n plaats is (artikel 35 AVG)
 - ook *verstandig* indien niet verplicht
- ga na of uw bedrijf functionaris voor de gegevensbescherming (FG) nodig heeft (artikel 37 AVG)
- bereid u voor op
 - recht beperking van de verwerking (artikel 18 AVG)
 - recht op dataportabiliteit (artikel 20 AVG)
- **begin op tijd!**



de taaieste wet- en regelgeving boeiend en glashelder gebracht

mobiel 06 50 683 960
info@jwinfotainment.nl
www.jwinfotainment.nl
facebook.com/jwinfotainment
