Algemene Verordening Gegevensbescherming

Jo Weerts

JWinfotainment

de taaiste wet- en regelgeving boeiend en glashelder gebracht

1

Volledige organisatie

- juridisch
  - verwerkersovereenkomst
  - geheimhoudingverklaring
  - privacybeleid
- automatisering
  - software- en virusscanners
  - (veilige) back-ups om persoonsgegevens te beschermen tegen verlies of ransomware
  - cloud-oplossing binnen EU
- procedures
  - wie heeft waar toegang toe
  - welke procedure bij datalek
  - bewaartermijnen
- medewerkers
  - opleiding
  - bewustwording

2

Instemmingsrecht ondernemingsraad
artikel 27 WOR

- regeling omtrent verwerken van alsmede bescherming van persoonsgegevens van in onderneming werkzame personen
- regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid / gedrag / prestaties van in onderneming werkzame personen

3

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

4

Algemene Verordening Gegevensbescherming
directe werking

- nieuwe wetgeving betreft verordening
  - regels hebben directe werking
    - enkele regels ter uitvoering van AVG 2018 staan in uitvoeringswet AVG
- sinds 25 mei 2018 is Algemene verordening gegevensbescherming (AVG) definitief van toepassing
- Wet bescherming persoonsgegevens (Wbp) / Wet meldplicht datalekken geldt niet meer

5

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)

6

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

7

Persoonsgegevens

- naam
- adres
- woonplaats
- telefoonnummer
- postcode
- huisnummers
- e-mailadres
- kenteken
- …

8

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

9

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

10

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

11

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)

12

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

13

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

14

Onderwerpen in verwerkersovereenkomst 2

- beveiligingsmaatregelen
  - passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies e.d.
- 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

15

Onderwerpen in verwerkersovereenkomst 3

- audits
  - verantwoordelijke moet kunnen controleren of verwerker zich houdt aan gemaakte afspraken
- 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

16

Verwerking
grondslag

- noodzakelijk
- zo klantvriendelijk mogelijk
- proportioneel

17

Beginselen verwerking persoonsgegevens
artikel 5 AVG

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

18

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 / …

19

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 vervulling van taak van algemeen belang / taak in kader van uitoefening van openbaar gezag
  - gegevens doorgeven aan Kadaster / …
- noodzakelijk voor gerechtvaardigde belangen
  - presentielijst / BKR-toets nieuwe klanten / …

20

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

21

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
- verwerking heeft betrekking op persoonsgegevens die kennelijk door betrokkene openbaar zijn gemaakt
- …

22

Bijzondere persoonsgegevens
o.a.

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

23

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)

24

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

25

Toestemming

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

26

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

27

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

28

Verplichtingen

programma

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

29

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

30

Register van de verwerkingsactiviteiten
niet van toepassing

- niet van toepassing op ondernemingen of organisaties die minder dan 250 personen in dienst hebben
  - jaaromzet 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

31

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
- …

32

Niet-incidentele verwerking

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

33

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

34

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

35

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

36

Gegevensbeschermingbeleid (privacy-beleid)

- verplicht om gegevensbeschermingsbeleid op te stellen als dat in verhouding staat tot verwerkingsactiviteiten
  - hangt af van concrete omstandigheden
    - aard / omvang / context /doel van gegevensverwerking
      - ziekenhuizen / gemeenten / social mediabedrijven / …
        - » ook kleine organisaties kunnen verplicht zijn privacy-beleid op te stellen
- vrijwillig opstellen van gegevensbeschermingsbeleid
  - helpt u om te zien of u voldoende maatregelen heeft genomen om persoonsgegevens van medewerkers / klanten / patiënten / cliënten e.d. te beschermen

37

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?)

38

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

39

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 …

40

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

41

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

42

Beveiliging
technische maatregelen

- betrouwbare informatiesystemen
  - toegangscontrole, gebruik vastleggen en back-ups maken
- voldoende beveiligingsschillen
  - firewall, actuele virusscanner, updates voor software
- veilige internetverbinding
- 'logfile'
  - kan worden nagegaan wie, wanneer dossier heeft geraadpleegd of verwerkt

43

Beveiliging
organisatorische maatregelen

- verantwoordelijkheden en bevoegdheden bij verwerken van persoonsgegevens zijn voor iedereen helder
  - wie mag welke gegevens inzien?
- werknemers zijn goed voorgelicht over omgang met privacygevoelige informatie
  - bij inloggen / opslaan / bewaren van gegevens

44

Zorgvuldigheid
programma

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

45

Data-minimalisatie

- technische en organisatorische maatregelen nemen om ervoor te zorgen dat alléén persoonsgegevens worden verwerkt die noodzakelijk zijn voor specifieke doel dat men wil bereiken
  - privacy by design / privacy by default

46

Privacy by design
ontwerp

- 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

47

Privacy by default
standaardinstellingen

- instellingen van programma / app / website / dienst zodanig dat maximale privacy wordt betracht
  - standaardinstellingen altijd zo privacy-vriendelijk mogelijk

48

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 / …
- bewaartermijn van (maximaal) 2 jaar nadat werknemer uit dienst is

49

Dossier digitaliseren

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

50

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

51

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

52

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

53

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

54

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

55

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

56

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

57

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

58

Reikwijdte inzagerecht

- 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

59

Recht van kopie
artikel 15 lid 3 AVG

- verwerkingsverantwoordelijke verstrekt betrokkene kopie van persoonsgegevens die worden verwerkt

60

Elektronische opgave loonbedrag
7:626 BW

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

61

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

62

Recht op correctie en verwijdering (rectificatie)
artikel 16 AVG

- niet bedoeld voor corrigeren van professionele indrukken / meningen / conclusies waarmee iemand het niet eens is (voor zover deze ter zake doen)
  - mag wel van organisatie verwachten dat deze in ieder geval schriftelijke mening toevoegt aan dossier

63

Recht op vergetelheid
artikel 17 AVG

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

Recht op gegevenswissing
Recht auf Vergessenwerden

64

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
  - …

65

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

66

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

67

Datalek
vrij brede definitie

- persoonsgegevens verloren raken ***of***
- onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten
  - aanpassen en/of veranderen van persoonsgegevens
  - onbevoegde toegang tot of afgifte daarvan

68

Datalek
voorbeelden

- hacker krijgt toegang tot persoonsgegevens
- verlies van USB-stick
- verloren of gestolen laptop
- gestolen geprinte klantenlijst
- verlies van gegevens
  - bijvoorbeeld: brand in datacentrum terwijl er geen back up beschikbaar is
- e-mail verzonden naar verkeerde adressen
- sturen van mailing met adressen in CC-veld (in plaats van BCC-veld)

69

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)

70

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

71

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

72

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

73

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

74

Meldplicht datalekken
checklist - 1

- ga na of databeveiliging up-to-date is
- richt goed incidentenbeheer in
  - hanteer intern procedure voor omgang met, en melding van, datalekken
- beslis wie in organisatie datalekken gaat beoordelen en melden bij AP
- denk na over hoe u betrokkenen gaat informeren bij datalek
- denk na over hoe u wilt omgaan met signalen uit buitenwereld over mogelijke datalekken

75

Meldplicht datalekken
checklist - 2

- inventariseer wie uw gegevens verwerken en of met deze partijen een verwerkersovereenkomst is gesloten
  - update verwerkersovereenkomsten met bepaling omtrent datalekken
- sluit met iedere partij waarmee u samenwerkt een NDA (Non Disclosure Agreement = geheimhoudingsverklaring) waarin u persoonsgegevens benoemt
- controleer hoe bedrijven die voor u persoonsgegevens verwerken persoonsgegevens opslaan
  - controleer dit uiteraard ook binnen eigen bedrijf

76

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)

77

Grootschalige gegevensverwerking

- aantal betrokkenen (mensen van wie u gegevens verwerkt)
- hoeveelheid gegevens die u verwerkt
- duur van de gegevensverwerking
- geografische reikwijdte van de verwerking

78

‘Systematisch’ / ‘stelselmatig’

- verwerking van persoonsgegevens die is opgenomen in de systemen of in het beleid van de organisatie moet worden beschouwd als een systematische of stelselmatige verwerking

gegevensverwerkingen die ad hoc of incidenteel plaatsvinden moeten niet beschouwd worden als systematische of stelselmatige verwerkingen

79

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

80

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 privacytoezichthouder oordeelt dat er toch DPIA nodig is
- op lijst staat van verwerkingen waarvoor DPIA niet verplicht is

81

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

82

AP-lijst van verwerkingen waarvoor DPIA verplicht is 1

- heimelijk onderzoek
  - grootschalige en/of systematische verwerkingen
    - waarbij informatie wordt verzameld door middel van onderzoek zonder betrokkene daarvan vooraf op de hoogte te stellen
      - particuliere rechercheburo's / heimelijk cameratoezicht
- zwarte lijsten
  - verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door organisaties of particulieren worden verwerkt en gedeeld met derden
    - bijvoorbeeld door verzekeraars / horecabedrijven / winkelbedrijven / telecomprovider / …

83

AP-lijst van verwerkingen waarvoor DPIA verplicht is 2

- fraudebestrijding
  - grootschalige en/of systematische verwerkingen
    - sociale diensten / fraudeafdelingen van verzekeraars / …
- creditscores
  - grootschalige en/of systematische verwerkingen
    - inschattingen van kredietwaardigheid van natuurlijke personen
- financiële situatie
  - grootschalige en/of systematische verwerkingen
    - financiële gegevens waaruit inkomens- of vermogenspositie of bestedingspatroon van mensen valt af te leiden

84

AP-lijst van verwerkingen waarvoor DPIA verplicht is 3

- genetische persoonsgegevens
  - grootschalige en/of systematische verwerkingen
    - DNA-analyses ten behoeve van het in kaart brengen van persoonlijke kenmerken / bio-databanken / …
- gezondheidsgegevens
  - grootschalige verwerkingen
    - instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening / arbodiensten / reïntegratiebedrijven / (speciaal)onderwijsinstellingen / verzekeraars / onderzoeksinstituten / …
      - waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid

85

AP-lijst van verwerkingen waarvoor DPIA verplicht is 4

- samenwerkingsverbanden
  - delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard (zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk) met elkaar uitwisselen
    - wijkteams / veiligheidshuizen / informatieknooppunten / …

86

AP-lijst van verwerkingen waarvoor DPIA verplicht is 5

- cameratoezicht
  - stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten met behulp van camera's / webcams / drones
- flexibel cameratoezicht
  - grootschalig en/of systematisch gebruik
    - camera's op kleding of helm van brandweer- of ambulancepersoneel / dashcams gebruikt door hulpdiensten

87

AP-lijst van verwerkingen waarvoor DPIA verplicht is 6

- controle werknemers
  - grootschalige en/of systematische verwerking van persoonsgegevens om activiteiten van werknemers te monitoren
    - controle van e-mail en internetgebruik / GPS-systemen in (vracht)auto's van werknemers / cameratoezicht ten behoeve van diefstal- en fraudebestrijding / …
- locatiegegevens
  - grootschalige en/of systematische verwerking van locatiegegevens van of herleidbaar tot natuurlijke personen
    - (scan)auto's / navigatiesystemen / telefoons / verwerking van locatiegegevens van reizigers in openbaar vervoer / …

88

AP-lijst van verwerkingen waarvoor DPIA verplicht is 7

- communicatiegegevens
  - grootschalige en /of systematische verwerking van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen
    - tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder / randapparaat van de eindgebruiker

89

AP-lijst van verwerkingen waarvoor DPIA verplicht is 8

- internet of things
  - grootschalige en/of systematische verwerkingen door verantwoordelijken van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen
    - slimme televisies / slimme huishoudelijke apparaten / connected toys / smart cities / slimme energiemeters / medische hulpmiddelen / …

90

AP-lijst van verwerkingen waarvoor DPIA verplicht is 9

- profilering
  - systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking
    - beoordeling van beroepsprestaties / prestaties van leerlingen / economische situatie / gezondheid / persoonlijke voorkeuren of interesses / betrouwbaarheid of gedrag / …
- observatie en beïnvloeding van gedrag
  - grootschalige verwerkingen waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd / verzameld / vastgelegd / beïnvloed wordt
    - inclusief gegevens die voor het doel online behavioural advertising worden verzameld

91

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

92

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

93

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
    - …

94

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

95

Deskundigheid en vaardigheden van functionaris voor gegevensbescherming

- "wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 bedoelde taken te vervullen“

artikel 37, lid 5 AVG

96

Niveau van deskundigheid

- vereiste niveau is niet strikt gedefinieerd, maar moet in verhouding zijn tot gevoeligheid en complexiteit van gegevens, alsook hoeveelheid gegevens die organisatie verwerkt
  - bij bijzonder complexe dataverwerkingsactiviteit of bij verwerking van groot aantal gevoelige gegevens kan van functionaris voor gegevensbescherming hoger niveau van deskundigheid en ondersteuning worden vereist

97

Professionele kwaliteiten

- enige ervaring met nationale en Europese wetten en praktijken op gebied van gegevensbescherming
- grondige kennis AVG
- kennis bedrijfstak / organisatie van verwerkingsverantwoordelijke
- voldoende inzicht hebben in uitgevoerde verwerkingsactiviteiten / informatiesystemen / behoeften van verwerkingsverantwoordelijke op vlak van gegevensbeveiliging en gegevensbescherming
- gedegen kennis van administratieve regels / procedures van organisatie

98

Positie van functionaris voor gegevensbescherming 1

- "naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens"

artikel 38 AVG

99

Positie van functionaris voor gegevensbescherming 2

- regelmatig uitnodigen om vergaderingen van hogere management en middenkader bij te wonen
- aanwezigheid wordt aanbevolen wanneer beslissingen worden genomen die gevolgen hebben voor de gegevensbescherming
  - alle relevante informatie moet tijdig aan FG worden bezorgd, zodat hij/zij passend advies kan verlenen
- mening van FG naar behoren in overweging wordt genomen
  - redenen voor het niet volgen van advies van functionaris voor gegevensbescherming documenteren
- meteen wordt geconsulteerd zodra zich gegevensinbreuk of ander incident voordoet

100

Waarborgen FG

- geen instructies door verwerkingsverantwoordelijken of verwerkers met betrekking tot uitoefening van taken van FG
- geen ontslag of sancties door verwerkingsverantwoordelijke voor de uitvoering van de taken van FG
- geen belangenconflict met andere mogelijke taken en verplichtingen
- FG moet zonder tussenkomst van anderen in organisatie toegang hebben tot hoogste bestuurders (verwerkingsverantwoordelijke in de zin van de wet) om adviezen te kunnen geven.

Taken van functionaris voor gegevensbescherming 1

- informeren / adviseren over verplichtingen uit hoofde van verordening
- toezien op naleving van verordening
- desgevraagd advies verstrekken met betrekking tot gegevensbeschermingseffectbeoordeling / toezien op uitvoering daarvan
- samenwerken met toezichthoudende autoriteit
- optreden als contactpunt voor toezichthoudende autoriteit inzake met verwerking verband houdende aangelegenheden

102

Taken van functionaris voor gegevensbescherming 2

- functionaris voor gegevensbescherming houdt bij uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met aard, omvang, context en verwerkingsdoeleinden

103

Plichten verwerkingsverantwoordelijke 1
checklist

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

104

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

105

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

106

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

107

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) verwijdert bestaande kopieën
- maakt afspraken met betrekking tot sub-verwerkers

108

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

109

Controle van e-mail en internet op het werk
Europese jurisprudentie (art. 8 EVRM)

- werknemer heeft ook op werkplek recht op privacy
- eventuele inbreuk moet kenbaar zijn gemaakt aan werknemer door middel van waarschuwing of geldende gedragscode binnen onderneming
  - duidelijk e-mail- en internetprotocol
- gerechtvaardigd doel
- proportionaliteitsvereiste

110

Gebruik van e-mail en internet controleren

- werkgever mag voorwaarden stellen aan gebruik van e-mail en internet op werk / bepaalde soorten gebruik verbieden
  - werkgever mag controles uitvoeren
    - moet daarbij voldoen aan voorwaarden uit onder meer Wbp/AVG
- kan bijvoorbeeld steekproefsgewijs monitoren of er verboden gebruik van e-mail of internet plaatsvindt

111

Openbare bronnen

- hoofdregel: organisatie mag persoonsgegevens uit openbare bronnen niet vrijelijk gebruiken
  - grondslag / doel / noodzaak

heimelijk waarnemen

112

Sociale media
sollicitant

- checken van sociale media in beginsel niet toegestaan
  - noodzakelijk / relevant met oog op vervullen van vacature
    - bepaalde risico's onderzoeken
  - sollicitant van tevoren informeren dat screening door middel van sociale media-onderzoek mogelijk is
  - alleen relevante informatie bekijken
  - afweging maken of profiel zakelijk of privé bedoeld is
    - LinkedIn wel / Facebook-Instagram niet

113

Sociale media
(ex-)werknemer

- in beginsel niet monitoren op sociale media
  - controle op overtreden van concurrentie- en/of relatiebeding door middel van LinkedIn / controle op nevenwerkzaamheden
    - betreffende (ex-)werknemer hierover geïnformeerd
    - geen controlemogelijkheid die minder vergaande inbreuk maakt op privacy

114

Ontslag op staande voet wegens stelselmatig internetten onder werktijd - ECLI:NL:RBAMS:2017:6700

- in memo van 18 oktober 2016 is medewerkers van kledingzaak meegedeeld dat het niet meer is toegestaan om mobiele telefoon, iPad, laptop of welk apparaat dan ook waarmee kan worden gebeld, gechat, getext, of voor welke vorm van internet dan ook gebruikt kan worden, tijdens werktijd bij zich te hebben
- 22 december 2016 schriftelijke waarschuwing: te laat komen / gebruik van privé telefoon tijdens werktijd / achterhouden van artikelen uit winkelvoorraad voor persoonlijk gewin
- 4 februari 2017 'laatste' waarschuwing
- 21 april 2017 incident - ontslag op staande voet

Tip

- internet- / e-mail- / sociaal mediaprotocol
  - instemmingsrecht medezeggenschap (artikel 27 WOR)

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
- besef 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)

118

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

119

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

120

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)

121

Regelhulp Algemene verordening gegevensbescherming

- in 10 stappen beeld van waar u aan kunt werken om goed voorbereid te zijn op AVG
- bedoeld voor *verwerkingsverantwoordelijken (*iedere organisatie, groot of klein, die persoonsgegevens verwerkt en daarvoor zelf doel en middelen bepaalt
  - bedrijven / overheidsinstanties / stichtingen / kleine zelfstandigen

https://rvo.regelhulpenvoorbedrijven.nl/avg/#/welkom

122

JWinfotainment

de taaiste wet- en regelgeving boeiend en glashelder gebracht

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

123