ACTUALITEITEN PRIVACY
HR Seminar 2018

De AVG, wat moet HR ermee?

Doorn en Keizer
Employment Lawyers • Arbeidsrecht Advocaten

DenK

1. **D-day AVG: (g)een level playing field**
2. **Basics gegevensbescherming blijven ongewijzigd**
3. ***Eerste wijziging*: Handhaving en sancties AP, geen tandeloze tijger meer..**
4. ***Tweede wijziging*: Accountability, werkgever wordt ter verantwoording geroepen**
5. ***Derde wijziging*: Nieuwe (en aangescherpte) rechten werknemers, nieuwe vragen voor de praktijk**
6. **Key take away: protect data, protect your business**

1. D-day AVG: (g)een level playing field?

Ingangsdatum

25 mei 2018

~~Wet Bescherming Persoonsgegevens & Vrijstellingsbesluit vervallen~~

Uniforme regels in EU

Ja, maar geen invulling privacynormen voor arbeidsverhoudingen (art. 88), dat is aan de lidstaten

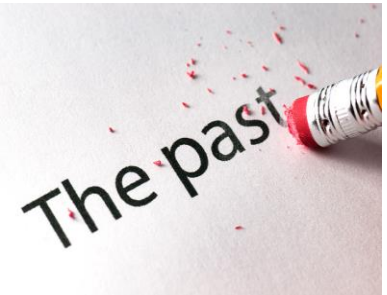
AVG & Uitvoeringswet AVG (UAVG)

Wijziging privacyregels

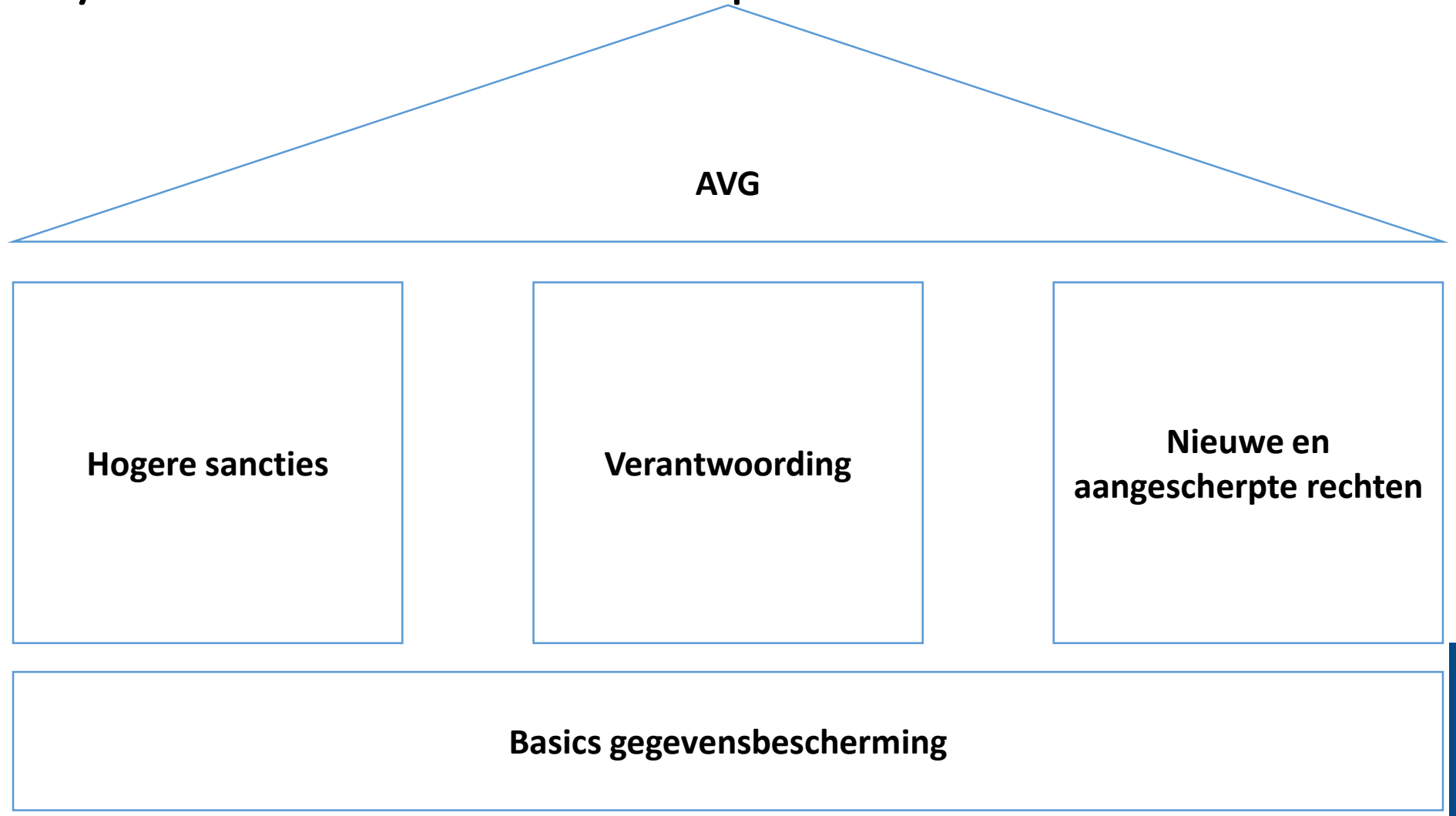
Belangrijkste wijziging sinds 1995

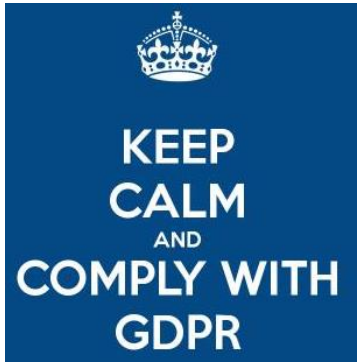
Basisbeginselen in de kern ongewijzigd

Brandbrief VNO aan kabinet - amendement UAVG



1. D-day AVG: AVG in een notendop





2. Basics gegevensbescherming blijven ongewijzigd: casus

HR Seminar B.V.

Vacature:
Data Protection Officer

Personalia

Kerkstraat 1
1211CR Hilversum

0687654321

ditismijnemail@email.com

Geboortedatum: 1 januari 1960

Geboorteplaats: Hilversum

Geslacht: Man

Nationaliteit: Nederlandse

Burgelijke staat: Gehuwd

Rijbewijs: A, B

Vaardigheden

MS office
Leidinggeven
Commercieel
Strategisch

Talen

Nederlands
Engels
Duits
Frans

Hobby's en Interesses

- Vissen
- Sporten

Opleidingen

HBO, HEAO (behaald) 1980 - 1984
Hogeschool Utrecht, Utrecht

MBO, MEAO (behaald) 1977 - 1980
Christelijke MEAO, Amersfoort

Cursussen

Bedrijfshulpverlening (behaald) 2006 - 2006

Kenneth Smit, Sales (behaald) 2003 - 2003

Werkervaring

Sales Improvers, Amsterdam 2013 - 2014
Functie: Sales consultant

Bij Sales Improvers ben ik op freelance basis als Sales consultant gaan werken. Ik heb bedrijven geanalyseerd en geadviseerd hoe ze hun verkoopafdeling kunnen verbeteren.

PTC wholesale, Amersfoort 2001 - 1012
Functie: Sales Manager

1. Eindverantwoordelijk voor de verkoopresultaten in Vlaanderen
2. Motiveren en begeleiden van vertegenwoordigers;
3. Bewaken van de klanttevredenheid;
4. Opstellen van maand prognoses en resultaten;
5. Managementrapportages opstellen.

PTC wholesale, Amersfoort 1991 - 2001
Functie: Verkoopmedewerker buitendienst

1. Verantwoordelijk voor het binnenhalen van 'new business' in Noord-Nederland;
2. Opvolgen van leads en het benaderen van potentiele klanten.
3. Signaleren van verkoopmogelijkheden en commerciële kansen;
4. Prognoses opstellen en rapporteren aan de sales manager.

PTC wholesale, Amersfoort 1984 - 1999
Functie: Accountmanager binnendienst

1. Verantwoordelijk voor de bestaande klantenportfolio in Noord-Nederland;
2. Contact onderhoudenmet klanten ;
3. Opstellen van account- en prospectplannen;
4. Signaleren van verkoopmogelijkheden en commerciële kansen;
5. Opstellen van rapportages aan de manager.

Referenties

Referenties op aanvraag beschikbaar.

2. Basics gegevensbescherming blijven ongewijzigd: 6 stappen

1. Verwerk ik persoonsgegevens?

Verwerking:
Alle handeling mbt persoonsgegevens (verzamelen, bewerken, vernietigen, doorgeven, etc.)

Persoonsgegevens:
Informatie die (in)direct herleidbaar is tot persoon (**betrokkene**).

Bijzondere persoonsgegevens:
Ras, religie, vakbonds-lidmaatschap, genetische en biometrische gegevens, gegevens mbt gezondheid of seksualiteit.

2. Welke rol heb je bij de gegevensverwerking?

Verwerkings-verantwoordelijke:
Initiatiefnemer, bepaalt doel en middelen (“controller”).

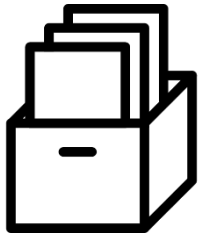
Verwerker:
Uitvoerder, verwerkt ten behoeve en op instructie van de verantwoordelijke (“processor”).

3. Heb ik een doel en grondslag?

Doel:
Vooraf omschreven, welbepaald, uitdrukkelijk en rechtvaardig.

Wettelijke grondslag:
Toestemming, vitale belangen, wettelijke plicht, uitvoering overeenkomst, algemeen belang en gerechtvaardigd belang.
Noodzakelijk: proportionaliteit & subsidiariteit.

4. Hoelang bewaar en hoe beveilig ik de gegevens?



Bewaren:
Niet langer dan noodzakelijk voor doel.

Beveiligen:
Passende technische en organisatorische maatregelen.

5. Waarborg ik de rechten van betrokkene?

Informeren, inzage, correctie en verzet

6. Waarborg ik privacy bij evt. internationale doorgifte?

Passend beschermingsniveau.
Buiten EER: nee, tenzij

2. Basics gegevensbescherming blijven ongewijzigd: tips

Basics gegevensbescherming

<u>Vrijstellingsbesluit</u>:
Per onderwerp overzicht **doelen**, categorieën gegevens, categorieën ontvangers en **bewaartermijn**.

Voorbeelden onderwerpen:
Sollicitanten, Arbeidsbemiddeling, Personeelsadministratie, Pensioen en vervroegde uitdiensttreding, Computersystemen, Toegangscontrole, Bezoekersregistratie, Videocameratoezicht, Intranet en Persoonlijke websites.

CBP Informatieblad bewaartermijnen

<u>Beveiliging:</u>

- **Technische maatregelen**: Up to date virusscan, Beveiligde USB-sticks, Accurate beveilliging medewerkerstelefoon, Unieke inlogcode en wachtwoord (regelmatig aanpassen), Versleutelde email, Geen onbeveiligde externe harde schijven, Geen onbeveiligde back ups maken, Geen documenten op privé laptop op slaan en Principle of least privilege (toegang op need-to-know basis) en certificering (NEN 7510/7513, ISO 27001).
- **Organisatorische maatregelen**: Clean desk policy, Laptop niet onbemand achterlaten, Laptop nooit achterlaten in de auto, Privacy screens, Oude documenten op juiste wijze vernietigen en Zorgvuldig gebruik USB-sticks.

3. Handhaving en sancties AP (i): een greep uit de handhavingspraktijk

Overzicht meldingen datalekken eerste kwartaal 2017

Persbericht / 10 mei 2017 Categorie: Meldplicht datalekken

Van januari tot en met maart 2017 zijn er ruim 2300 datalekken gemeld aan de Autoriteit Persoonsgegevens (AP). De meeste datalekken werden gemeld vanuit de sectoren gezondheid en welzijn (27%), financiële dienstverlening (21%) en openbaar bestuur (20%).

Overzicht thematische beleidsregels

- Machtigingsvereiste zorgpolis
  december 2016
- De zieke werknemer
  april 2016
- Cameratoezicht
  januari 2016
- Meldplicht datalekken
  december 2015
- Beveiliging van persoonsgegevens
  februari 2013
- Kopie identiteitsbewijs
  juli 2012
- Openbaarmaking van overheidsinformatie
  augustus 2009
- Toepassing van ANPR door de politie
  juli 2009
- Informatieplicht basisscholen onderwijskundig rapport
  juni 2009
- Publicatie van persoonsgegevens op internet
  december 2007

Bijlage Jaarverslag 2017

Personeel en formatie

Formatie

De feitelijke bezetting eind 2017 was 102,69 fte. In het begin van dat jaar was de bezetting nog 75,71 fte. Deze toename komt doordat de AP zich al aan het voorbereiden is op de nieuwe situatie per 25 mei 2018, als de nieuwe privacywetgeving van toepassing is. De personele groei is in lijn met de hierover gemaakte afspraken met het ministerie van Justitie en Veiligheid. In 2018 neemt de groei naar verwachting verder toe tot circa 140 fte medio 2018.

Bezetting

	2016		2017	
Aantal medewerkers einde jaar	**80**		**117**	
Verdeling man/vrouw	28,75 % man	71,25 % vrouw	34,2% man	65,8 vrouw
Gemiddelde leeftijd	44 jaar		41,5 jaar	
Gemiddeld aantal dienstjaren	8,8 jaar		6,6 jaar	
Gemiddelde schaalwaarde	12		11	
In-/uitstroom	5fte instroom	7 fte uitstroom	36 fte instroom	6 fte uitstroom

Onderzoeksrapport

Alcohol- en drugscontroles bij werknemers

De verwerking van persoonsgegevens bij de uitvoering van alcohol- en drugscontroles door Uniper Benelux N.V. (voorheen E.ON Benelux N.V.)

Bron:
www.autoriteitpersoonsgegevens.nl

AUTORITEIT PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

De Staatssecretaris van Veiligheid en Justitie

Directie Wetgeving en Juridische Zaken
Sector Staats- en bestuursrecht
Postbus 20301
2500 EH DEN HAAG

Datum	Ons kenmerk	Uw brief van
6 april 2017	z2017-02390	20 maart 2017

Onderwerp
Advies wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming

3. Handhaving en sancties AP (ii): geen tandeloze tijger meer…

Handhaving

Informeren

Vergaande onderzoeks-bevoegdheden

Publicatie rapportage van bevindingen (reputatieschade)

Sancties

~~Bindende aanwijzing~~

Waarschuwing

Stopzetting verwerking

Last onder dwangsom

Boetes:
1. max. €10 mio (of indien hoger) 2% wereldwijde jaarlijkse omzet voorgaande boekjaar
2. max. €20 mio / 4% (idem)

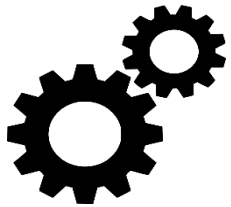
Nieuw boetebeleid met staffel (MKB?)

One-stop-shop

Vestigingen in meerdere lidstaten: 1 leidende toezichthouder (hoofdvestiging)

Lokale toezichthouders houden autoriteit bij specifieke lokale verwerkingen – HR?

4. Accountability: werkgever wordt ter verantwoording geroepen (i)



Passende compliance-maatregelen

Wg moet naleving privacybeginselen aantonen (art. 5)

Technische en organisatorische maatregelen (art. 24 lid 1)

Passend gegevens-beschermingsbeleid

"wanneer in verhouding staat tot de verwerkings-activiteiten" (art. 24 lid 2)

Privacy by design en default

Privacybescherming door ontwerp en standaardinstellingen (art. 25)

Meldplicht datalekken

Meldplicht AP/betrokkene en register datalekken (art. 33 en 34)

4. Accountability: tips

Accountability = documenteren kun je leren

AVG compliance en passend beleid: privacy incorporeren in bedrijfsDNA

Audit: wie, wat, waarom en hoe?

Documenteer beleid, processen en procedures en maatregelen die AVG compliance aantonen, o.m.:

- Datastromen, register verwerkingsactiviteiten
- Externe privacy statement op website
- Intern privacybeleid voor werknemers in arbeidsovereenkomst of personeelshandboek (**Ondernemingsraad!**)
- NDA en update geheimhoudingsclausule
- Notice aan ontvangers nieuwsbrief

Stel een data retention policy en security policy op

Tip: handleiding AVG Rijksoverheid

Privacy governance structuur:

- Wijs rollen en verantwoordelijkheden expliciet aan en beschrijf taken en bevoegdheden in beleidsdocument/functieomschrijving (heldere rapportagelijnen, DPO/privacyfunctionaris)
- Train verantwoordelijken (management) en personeel en gerichte training voor DPO/privacyfunctionaris (tip: IAPP, opleiding CIPM en CIPP/E)
- Maak voldoende budget vrij voor privacy programma (procesinrichting/aanpassing, training en beveiliging). Waarborg continuïteit en structurele aandacht, en hou rekening met inhuren externe hulp
- Zorg voor periodieke evaluatie en actualiseer beleid indien nodig (neem het op in de jaarplanning)
- Sluit waar mogelijk aan bij privacycodes of certificering (DDMA, AVG Verenigingen MKB)

4. Accountability: tips

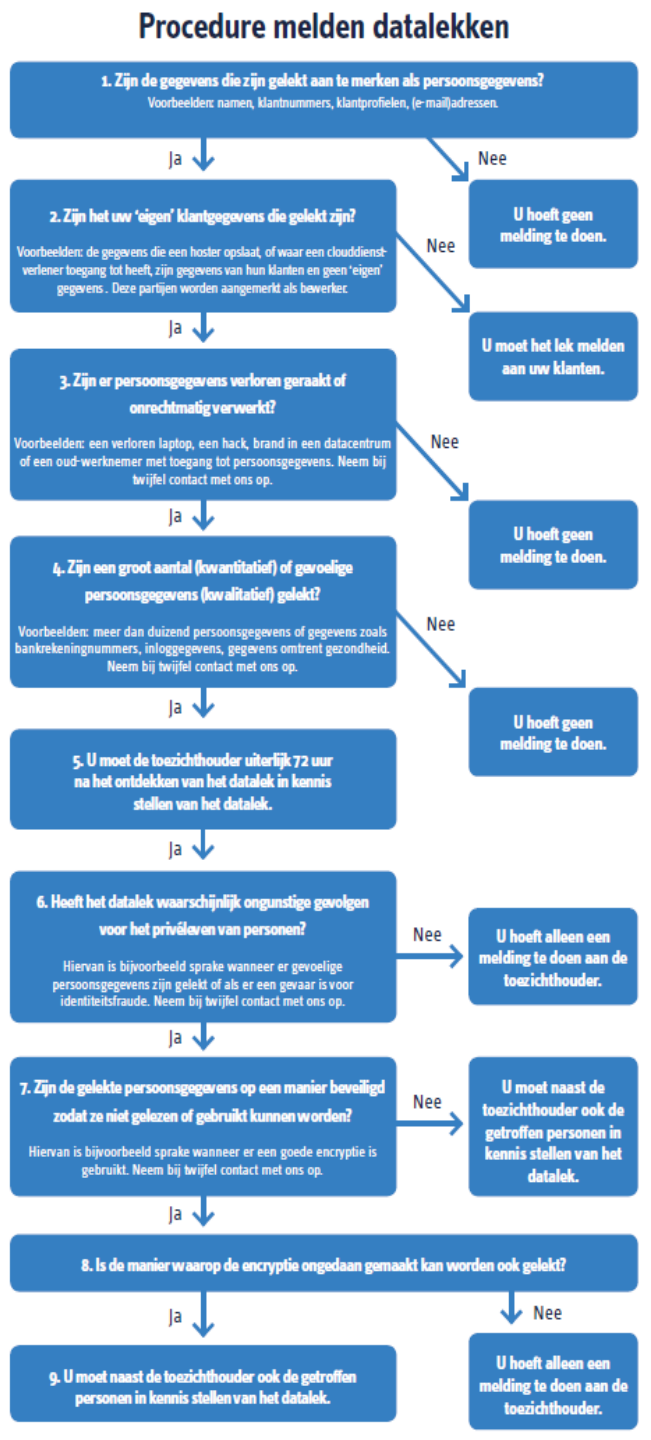
Accountability = minimaliseren en anticiperen

Privacy by design, by default:

- Verwerk niet meer dan noodzakelijk, spreek met bronhouders af welke data wordt geleverd
- Beveilig gegevens
- Gebruik pseudonimisering en versleuteling
- Privacy moet vast onderdeel zijn van project start architectuur
- Bouw privacy in, in systemen en processen en test dit regelmatig (audits)
- Maak dit inzichtelijk voor betrokkenen (bijv. publicatie auditverklaring/ certificering op website)
- **Tip: Baseline beveiliging Rijk**

Datalekken:

- Check beleidsregels datalekken AP
- Protocol en draaiboek datalekken om reputatieschade te voorkomen
- Register datalekken: de plicht om voortaan alle datalekken te registreren (ook die niet hoeven te worden gemeld aan de AP)
- Periodieke “dummy test”/audit met IT
- BYOD?
- Remote wipe/delete
- Maak duidelijke afspraken met verwerkers over datalekken (bijv. verwerker neemt zelf geen contact op met AP of betrokkene)
- **Tip: check website VNG en Rijksoverheid (privacy dossier voor factsheets en handige schema’s)**



4. Accountability: werkgever wordt ter verantwoording geroepen (ii)

Register verwerkingsactiviteiten

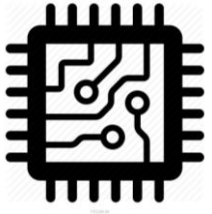
Minimumeisen register verwerkingsactiviteiten (art. 30).

DPIA

Gegevensbescherming-effectbeoordeling (art. 35)

FG

Functionaris gegevensbescherming (art. 37)



Verwerker

Minimumeisen verwerkersovk (art. 28)

4. Accountability: tips

Accountability = registreren en grote risico's inventariseren

Register:

- Verplichting grote onderneming (>250), ook voor kleinere als verwerking risicovol/niet incidenteel.
- Breng alle verwerkingen in kaart (wie, wat, waarom en hoe, ontvangers, bewaartermijnen, doorgifte, technische/organisatorische maatregelen)
- Geen doel op zich, het moet inzicht geven
- In steekwoorden
- Ook voor het verleden?
- Waarborg dat verwerker ook een register bijhoudt
- Implementeer procedure om register up-to-date te houden (elke wijziging werkproces vermelden en beleg taak expliciet bij DPO of procesdeskundige)
- **Tip: check website VNG voor hulpmiddelen en template**

DPIA:

- Verplicht bij hoog risico
- Vooraf raadplegen AP (art. 36)
- Richt een proces in om te bepalen of een DPIA nodig is en hoe die wordt uitgevoerd
- Leg vast wie het uitvoert, wie betrokken is en hoe het proces administratief wordt afgehandeld
- **Tip: model gegevenseffectbeoordeling Rijksdienst (PIA), model NOREA**

4. Accountability: tips

Accountability = DPO introduceren en verwerker attenderen

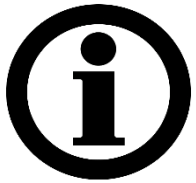
Functionaris Gegevensbescherming/DPO:

- Niet verplicht, tenzij..
- Ontslagbescherming
- Deskundig
- Review rol en taken: voorlichting, advisering, monitoring, samenwerking met de AP, loketfunctie, benodigde resources.
- Maak werkafspraken over de manier van communiceren en samenwerken
- **Tip: (informatieblad) eisen en wetenswaardigheden FG volgens AP**

Verwerkersovereenkomst:

- In kaart brengen en huidige contracten updaten. Bijv. arbodienst, pensioen- uitvoerder, IT service provider, salarisadministratie, accountant, etc.
- Pas waar nodig ovk's aan of sluit nieuwe ovk's en neem daarin op dat de verwerker:
  - Uitsluitend op uw instructie persoonsgegevens worden verwerkt;
  - Een zelfstandige beveiligingsplicht heeft (passende technische en organisatorische maatregelen);
  - De met verwerking belaste personen tot vertrouwelijkheid moet verplichten;
  - Bijstand verleent bij nakomen verplichtingen mbt rechten betrokkenen;
  - Persoonsgegevens na afloop wist of retourneert;
  - Informatie ter beschikking stelt die nodig is voor audits/inspecties toezichthouder;
  - Meldplicht datalekken;
  - Zo nodig: audit (via externe auditor: rapport aan alle klanten).
- **Tip: templates online te verkrijgen, maar maatwerk is vereist**

5. Nieuwe (en aangescherpte) rechten werknemers, nieuwe vragen voor de praktijk (i)



Recht op informatie

Vooraf aan betrokkene melden wie en waarom (art. 12, 13 en 14)

Begrijpelijke kennisgeving

Recht op inzage

Inzage en kopie (art. 15)

Recht op rectificatie

Correctie (art. 16)

Onjuist of onvolledig

Recht op wissing

Om “vergeten” te worden (art. 17)

Zonder onredelijke vertraging wissen, redelijke maatregelen.

Tenzij…

5. Nieuwe (en aangescherpte) rechten werknemers: tips

Rechten: begrijpelijk informeren, inzien, corrigeren en verwijderen

Informatie:
- Tref ‘passende maatregelen’ om in beknopte, transparante, begrijpelijke en toegankelijke vorm en in duidelijke en eenvoudige taal te communiceren met betrokken (elektronisch=> elektronisch)
- Betrek DPO/privacyfunctionaris en/of jurist voor juiste vorm
- Communiceer bij het verzamelen van gegevens de aard van de verwerking aan betrokkene, bijv. privacy statements (goed zichtbaar op bijv. website of klantportaal)
- **Tip: Missie en privacy statement KPN of IND**

Inzage:
- Richt een proces en voorziening (loket) in om betrokkene inzage te kunnen geven in gegevensverwerking (op afstand in vorm van beveiligd portaal, op kantoor met fysieke balie of schriftelijk)

Rectificatie:
- Richt een proces in voor afhandeling van rectificatieverzoeken. Vaak een (extra) administratieve handeling in een bestaand proces.

Wissing:
- Idem, richt een proces op voor wissen en afschermen gegevens
- Ook back up wissen, technisch mogelijk?
- Derden informeren
- Geldt niet bij verwerkingen op basis van wettelijke verwerkingsverplichting, wel bij verwerkingen op basis van toestemming, onrechtmatige verwerking, aanbod aan kinderen.
- Geldt ook niet: vrijheid van meningsuiting en informatie, algemeen belang, instelling, onderbouwing, uitoefening rechtsvordering

5. Nieuwe (en aangescherpte) rechten werknemers, nieuwe vragen voor de praktijk (ii)

Recht om te beperken

Verwerking beperken (art. 18)

Juistheid gegevens betwist of niet meer nodig voor doel.

Tenzij…

Kennisgevingplicht derden

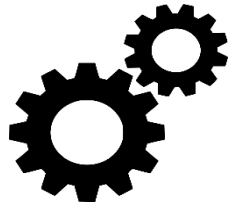
Kennisgevingsplicht rectificatie, verwijdering, beperking (art. 19)

Recht op dataportabiliteit

Gegevens over te dragen (art. 20)

Kopie gegevens verstrekken aan betrokkene of derde

Tenzij…



Recht van bezwaar

Bezwaar tegen geautomatiseerde verwerking, waaronder profilering (art. 21 en 22)

5. Nieuwe (en aangescherpte) rechten werknemers: tips

Rechten: beperken, kennisgeven ontvanger, doorleveren en bezwaar	
Beperking: - Implementeer een procedure om verwerking te beperken in geval de verwerking wordt betwist - Mogelijk door inbouwen van een mechanisme in de verwerking die verder gebruik van de betwiste gegevens voorkomen (bijv. door markeren dossier of tijdelijk naar ander systeem verplaatsen) **Kennisgeving:** - Implementeer een procedure voor notificatie van afnemers in geval van rectificatie, wissing of beperking. - Ontwerp mechanisme om ontvangers en betrokkenen in te lichten. - Tenzij het onmogelijk is of onevenredige inspanning (leg dit goed vast).	**Dataportabiliteit:** - Procedure voor (door) leveren van gegevens - Een technische voorziening om de gegevens in een ‘gestructureerd, gangbaar, machine leesbaar en interoperabel formaat” door te leveren (downloadprogramma’s, API’s) - Wijs op “minder veilig na overdracht” - Geldt niet bij verwerking op basis van wettelijke verplichting - Geldt wel op basis van toestemming of overeenkomst - **Tip: AP “Richlijnen voor het recht op dataportabiliteit”** **Bezwaar:** - Verwerking obv gerechtvaardigd belang of direct marketing - Stoppen tenzij dwingende gerechtvaardigde gronden of rechtsvordering - Richt een proces in voor toetsing en afhandeling van bezwaarverzoeken (loketfunctie). - Bijv. webformulier, klantportaal, klachtenlijn en instrueer service medewerkers. - Beperking geautomatiseerde besluitvorming. Onderzoek verwerkingen waar geen mensenhand meer aan te pas komt en breng eventuele risico’s daarvan in kaart (met behulp van DPO/privacyfunctionaris en jurist).

6. *Key take away*: protect data, protect your business!

AVG =
meer verplichtingen voor werkgever

Beleid =
is het halve werk als het gaat om verantwoording

Meer rechten =
interne processen op orde (*ongoing process*)

THANK YOU

Doorn en Keizer
Employment Lawyers • Arbeidsrecht Advocaten

DenK