# Privacy goed geregeld

Gouda (Westergouwe), 1 februari 2018

VESA Network Solutions

VESA NETWORK SOLUTIONS

# Wat is privacy?

- Ruimtelijke → heeft betrekking op eigen werkplek
- Relationele → vertrouwelijke info die wordt geuit op bv. social media
- Informationele → verwerking persoonsgegevens
- Lichamelijke integriteit → alcohol- en drugstest

## Algemene Verordening Persoonsgegevens (AVG)

**Persoonsgegeven:**

VESA NETWORK SOLUTIONS

- Elk gegeven dat informatie bevat over een natuurlijk persoon
- Gegevens die een persoon identificeerbaar maken

**Bijzonder persoonsgegeven:**

- Genetische gegevens (overgeërfd of verworven - analyse monster)
- Biometrische gegevens (gezichtsafbeeldingen of vingerdrukgegevens)
- Gegevens over gezondheid (ook over verleende gezondheidsdiensten)

# Pseudonieme data

*“persoonsgegevens die niet kunnen worden toegeschreven aan een specifiek persoon zonder het gebruik van aanvullende informatie (bv. algoritmen, koppeling database)".*

Doel:

VESA NETWORK SOLUTIONS

- Risico’s verminderen
- Helpen verwerkingsverantwoordelijken en verwerkers verplichtingen na te komen
- Indien aantoonbaar niet-identificeerbaar: art. 15 t/m 20 AVG n.v.t. (informatie, toegang, rectificatie en wissing persoonsgegevens)

# Pseudonieme data

**Voorwaarden:**

- Aanvullende info wordt afzonderlijk bewaard
- Technische- en organisatorische maatregelen waarborgen Niet bedoeld om

  gegevensbeschermingsmaatregelen uit te sluiten

**Verschil pseudonimisering en anonimisering:**

VESA NETWORK SOLUTIONS

- **Pseudonimisering** (encryptie) → mogelijkheid tot omkeerbaarheid → Persoonsgegeven → Privacywetgeving is van toepassing
- **Anonimisering** (randomisatie en generalisatie) → onomkeerbaar → Privacywetgeving niet van toepassing (er kan geen individu uit dataset worden gehaald, gegevens te linken aan een individu, info worden gehaald over individu).

## (Geautomatiseerde) verwerking persoonsgegevens

**Elk gegeven over een geïdentificeerde of identificeerbaar natuurlijk persoon.**

Voorbeelden gegevensverwerking:

- Verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

**Op passende manier beveiligen door technische en organisatorische beschermingsmaatregelen.**

Criteria:

- Stand techniek
- Aard persoonsgegevens
- Kosten tenuitvoerlegging

VESA NETWORK SOLUTIONS

# Verwerking persoonsgegevens

**Verwerking persoonsgegevens:**

- Vastgesteld doel
- Rechtmatige grondslag

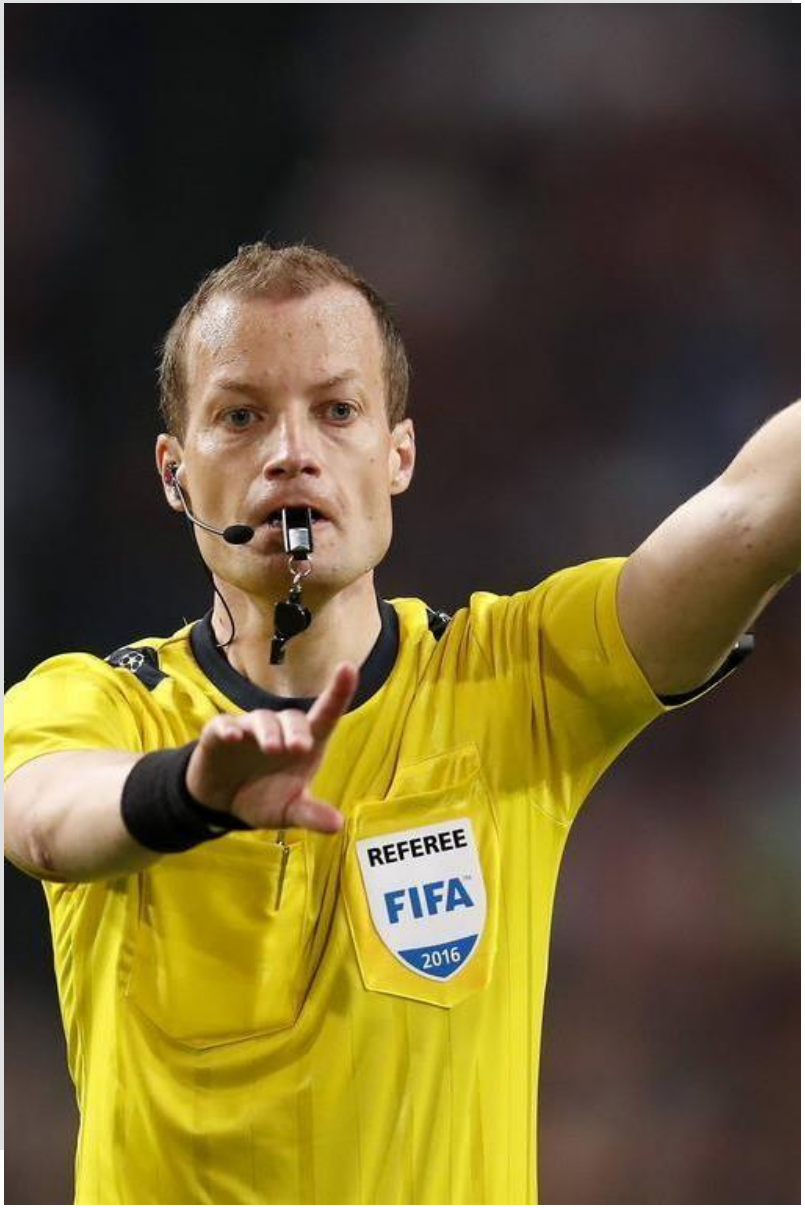
**AVG stelt eisen aan:**

- Bewaartermijnen
- Beveiliging persoonsgegevens

VESA NETWORK SOLUTIONS

# Beginselen verwerking persoonsgegevens

- Doelbinding/ doelbeperking
- Dataminimalisatie
- Accuraat en relevant
- Niet langer dan nodig bewaren
- Afdoende beveiligd
- Verwerkingsverantwoordelijke draagt verantwoordelijkheid




VESA NETWORK SOLUTIONS

# Grondslagen verwerking persoonsgegevens

- Toestemming betrokkene
- Uitvoering overeenkomst
- Wettelijke plicht
  (bijv. aan Belastingdienst)
- Vitale belangen betrokkene
  (bijv. bij ongeval)
- Algemeen belang of uitvoering overheidstaak
- Gerechtvaardigd belang
  (belangenafweging)

NB:

Alleen de gegevens die **noodzakelijk** zijn

# Toestemming

*Vrijelijk gegeven, specifiek beschreven doel, geïnformeerd en ondubbelzinnige toestemming*

## Ondubbelzinnige toestemming

- Geen twijfel mogelijk
- Expliciete mededeling d.m.v. verklaring
  of actieve handeling
  (bijv. aanvinken op aanvinkvakje)

## Twijfelachtig

- Expliciete toestemming in privacyreglement, algemene voorwaarden of door werknemer

# Toestemming

- Bewijslast bij verwerkingsverantwoordelijke
- Opnieuw vragen als ander onderwerp wordt gevraagd
- Altijd intrekbaar (net zo gemakkelijk als toestemming geven)
- Melden bij Autoriteit Persoonsgegevens als intrekking leidt tot einde dienstverlening
- Bij personen < 16 jaar: toestemming ouders (redelijke inspanningsplicht om dit te controleren)

# Gerechtvaardigd belang

**Belangenafweging:**

- Verantwoordelijke weegt eigen belang af tegenover (privacy)belang betrokkene
- Noodzakelijk voor een legitiem doel (bijv. netwerk- en informatiebeveiliging)
- Betrokkene mag (verdere) verwerking persoonsgegevens redelijkerwijs verwachten gezien relatie verantwoordelijke
- Tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert
- Recht van bezwaar voor betrokkene
- Geldt niet voor de overheid

# De praktijk

- Zorgvuldig omgaan met persoonsgegevens zichtbaar maken

- absoluut minimale set aan persoonsgegevens vastleggen;
- een duidelijk doel ligt ten grondslag aan de verwerkte persoonsgegevens;
- Consumenten/ werknemers te allen tijde inzicht hebben in de van hen vastgelegde gegevens;
- er ondubbelzinnige toestemming is van de betrokken consument/werknemer om de gegevens te verwerken;
- deze toestemming op elk moment ingetrokken kan worden;
- er bij voorkeur getest wordt met **gepseudonimiseerde** data;
- de omvang van de gebruikte testset aansluit bij het beoogde doel.

VESA NETWORK SOLUTIONS

# Kopiëren van ID-bewijzen

## Geen kopie

**maar hoe dan wel?**

- In- of uitlener moet zelf identiteit werknemer controleren
- Alleen overschrijven en geen kopie maken
- Tenzij: inleenkrachten buiten EER (dan kopie ID-bewijs verplicht)
- Onderaannemers of uitleners mogen BSN-nummer werknemer verstrekken aan inlener/aannemer

VESA NETWORK SOLUTIONS

# Bewaartermijnen

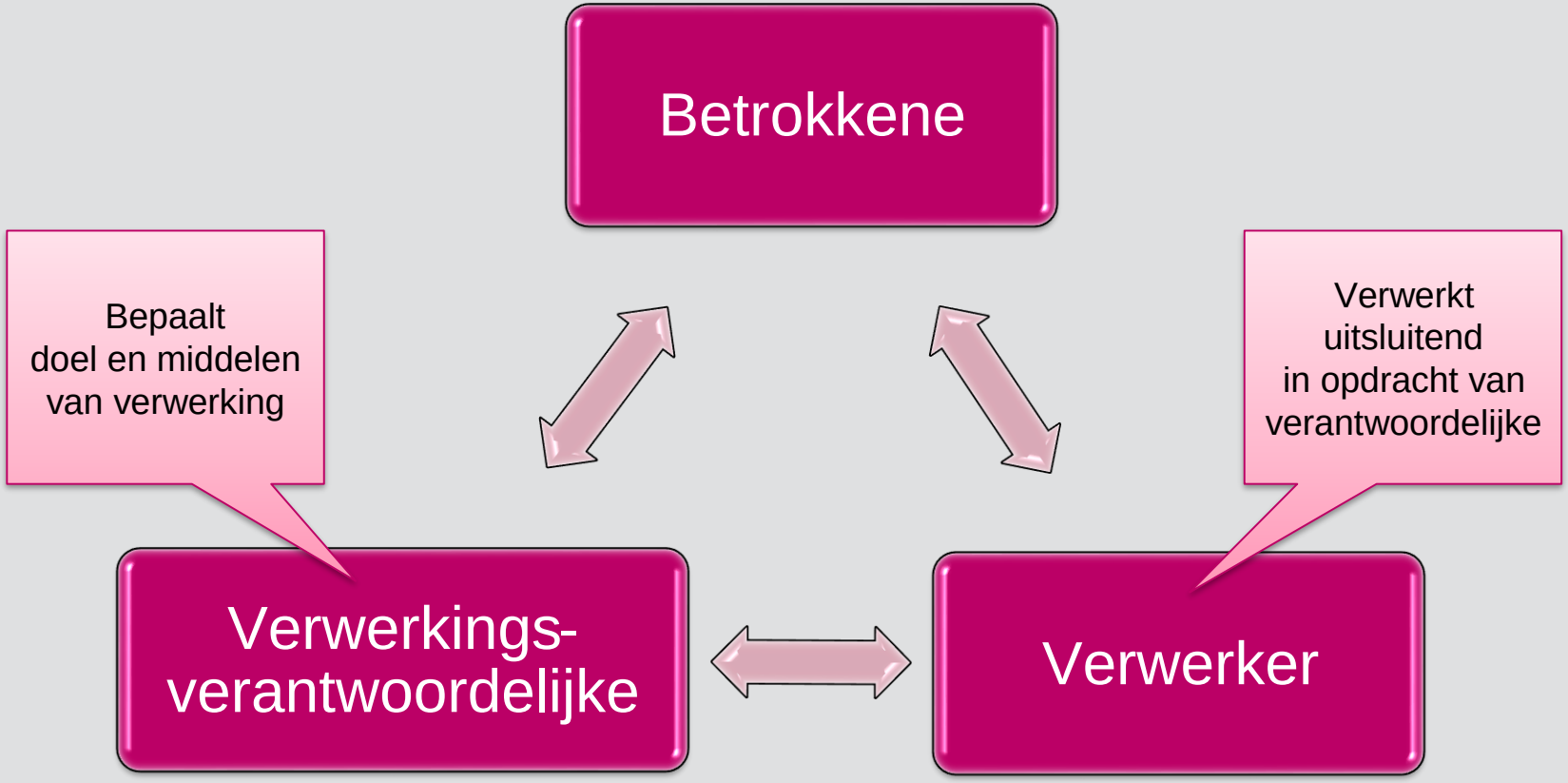
- Niet langer bewaren dan noodzakelijk
- Bewaartermijnen bedoelde wetgeving aanhouden:
  a) ID-bewijs en loonbelastingverklaring 5 jaar
  b) burgerlijke staat werknemer 7 jaar
  c) overige gegevens meestal 2 jaar
- Anders: kijken hoelang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld of gebruikt
- Persoonsgegevens vernietigen of anonimiseren als bewaartermijn is verstreken of niet meer noodzakelijk is

# Personeelsdossier

**Werkgevers:**

- Zijn verantwoordelijk voor de juistheid en nauwkeurigheid persoonsgegevens
- Moeten werknemers informeren waarom zij hun gegevens verzamelen
- Moeten de gegevens beveiligen
- Mogen de gegevens niet langer bewaren dan noodzakelijk
- Moeten werknemers de mogelijkheid bieden hun gegevens in te zien en eventueel te corrigeren of laten verwijderen
- Bij digitalisering dossier originele papieren dossier pas verwijderen bij goede beveiliging

# Partijen en rollen (verwerking persoonsgegevens)




**Verschil tussen verwerker en (mede)verwerkingsverantwoordelijke**

## Verwerker

- Opdracht tot verwerken van gegevens (bv. salarisadministrateur)
- Opdrachtgever blijft verantwoordelijk
- Verplicht verwerkersovereenkomst aan te gaan (voor meldplicht)

## (Mede)verwerkingsverantwoordelijke

- Inkoop van diensten (ene partij levert op kosten van andere partij diensten) bv. woningbouwvereniging geeft lijst bewoners aan installateur i.v.m. schoonmaken ketels
- Beide partijen (mede)verantwoordelijk
- Verdeling verantwoordelijkheden vastleggen
- Meldplicht door verantwoordelijke

NB: VESA Network Solutions beschikt over **model** verwerkersovereenkomst - en een modelregeling gezamenlijke verwerkingsverantwoordelijken (op aanvraag)

VESA NETWORK SOLUTIONS

# Subverwerkers

- Inschakelen derden mag alleen na toestemming verwerkingsverantwoordelijke
- Verwerker moet dezelfde verplichtingen uit de verwerkersovereenkomst voortzetten naar de sub-verwerker
- Verwerker volledig aansprakelijk voor het nakomen van de verplichtingen tegenover verwerkingsverantwoordelijke
- Verwerker wordt als verwerkingsverantwoordelijke beschouwd wanneer het de doeleinden en de middelen gaat bepalen

# Doorgifte naar niet-Europese landen

**Doorgifte persoonsgegevens toegestaan als:**

- EC het veilig acht
- Instrument tussen overheden
- Artikel 47 Binding Corporate Rules (BCR)
- Modelcontract opstellen
- Er een gedragscode geldt (art. 40 BCR)
- Het is gecertificeerd
- Verwerkersovereenkomst door toezichthouder is goedgekeurd

# Wanneer datalek?

Als het nadelige gevolgen kan hebben bij:

- Tekortschietende beveiligingsmaatregelen
- Hack van een ICT-systeem
- Verlies of diefstal USB-stick, mobiele telefoon etc.
- Menselijke factoren bv. verzending verkeerde e-mail
- Calamiteit: bv. Brand in datacentrum
- Gestolen laptop

VESA NETWORK SOLUTIONS

# Passend beschermingsniveau

- Adequaat en tijdig kunnen reageren op incidenten
- Vertrouwelijkheid, beschikbaarheid en integriteit waarborgen
- Voorkomen (wachtwoorden instellen of cryptografische verwerking)
- Detecteren bv. het loggen van het gebruik van bestanden
- Het beperken (bv. door het op afstand wissen van gegevens)
- Herstellen (bv. door het maken van back-ups

VESA NETWORK SOLUTIONS

# Passend beschermingsniveau

**Betrouwbaarheidseisen**

- Beschikbaarheid: waarborgen dat *geautoriseerde* gebruikers op de *juiste* momenten toegang hebben tot informatie;
- Integriteit: waarborgen van de *juistheid, tijdigheid en volledigheid* van informatie en verwerking;
- Vertrouwelijkheid: waarborgen dat informatie *alleen toegankelijk* is voor degenen die daarvoor is *geautoriseerd*;
- Controleerbaarheid: met voldoende zekerheid vaststellen dat aan eisen zijn voldaan

VESA NETWORK SOLUTIONS

# Passende beschermingsniveau

Ook bij:

- Versleutelde verbindingen;
- Beveiligde databases
- ACL/ authenticatie, logfiles en BYOD

Advies:

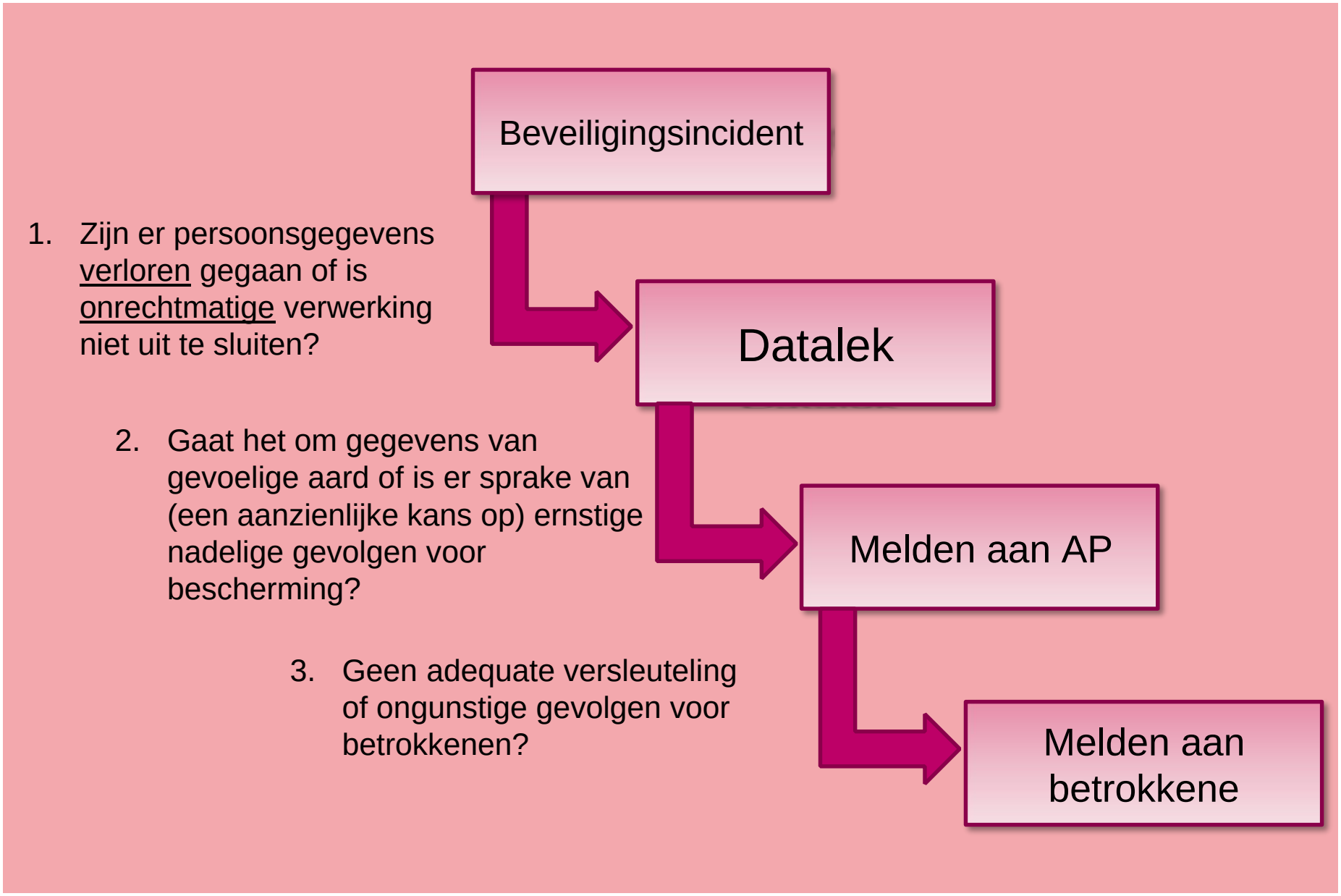
- Eisen stellen aan betrouwbaarheid;
- Technische en/of organisatorische maatregelen treffen;
- Controle hierop inbouwen
- Beveiligingsmaatregelen periodiek onder de loep nemen of ze nog wel in lijn zijn met de techniek en zonodig aanpassen;

VESA NETWORK SOLUTIONS

# Melding persoonsgegevens

- Persoonsgegevens van gevoelige aard
- Aard en omvang leidt of kan leiden tot ernstige nadelige gevolgen
- Geldt voor alle verantwoordelijken verwerking persoonsgegevens bv. van klanten, personeel of opdrachtgevers
- Datalek binnen 72 uur melden soms bij betrokkene en bij Autoriteit Persoonsgegevens: www.datalekken.autoriteitpersoonsgegevens.nl
- Verplicht overzicht bijhouden over mogelijke gevolgen en genomen maatregelen

VESA NETWORK SOLUTIONS



# Privacy by design en privacy by default

**Gegevensbescherming door ontwerp en standaardinstellingen**


## Privacy by design:

Al bij de ontwikkeling van produkten en diensten (informatiesystemen) moeten er privacy-verhogende maatregelen worden getroffen.

## Privacy bij default:

Privacy is een standaardinstelling van een programma, app, website, dienst of apparaat.

VESA NETWORK SOLUTIONS

# Verwerkingsregister > 250 werknemers


**<u>Doel:</u>**

Documenteren van alle verwerkingen binnen organisatie

- Schriftelijk of elektronisch
- Zowel voor verantwoordelijke als verwerker verplicht

**Geen meldingsplicht**

- Inzageplicht op verzoek toezichthouder

**Ook register bij < 250 werknemers wanneer:**

- Stelselmatige verwerking (bijzondere) persoonsgegevens
- Verwerking risico voor betrokkene inhoudt

# Verwerkingsregister

**Registratie per verwerkingsactiviteit verantwoordelijke en verwerker**

- De naam en contactgegevens van de (gezamenlijke) verantwoordelijke,
  (verwerker) en de Functionaris Gegevensbescherming (de FG)
- De doeleinden voor gegevensverwerking
- Een beschrijving van de categorieën betrokkenen en categorieën persoonsgegevens
- De categorieën ontvangers  van de gegevens (inclusief landen)
- De beoogde bewaartermijnen en
- een algemene beschrijving van de beveiligingsmaatregelen
- Inschatting risiconiveau (verhoogd of normaal)

VESA NETWORK SOLUTIONS

# Privacy Impact Assessment (PIA)

## Wat is PIA?

- Instrument om vooraf de privacy-risico's van gegevensverwerking in kaart te brengen
- Maatregelen nemen om risico's te verkleinen

## Wanneer PIA?

Verwerking verhoogd privacy-risico voor betrokkene


VESA NETWORK SOLUTIONS

# Privacy Impact Assessment (PIA)

**In ieder geval verplicht bij:**

- Beoordelen van mensen op basis van persoonskenmerken
- Grootschalige en systematische monitoring openbare toegankelijke ruimtes
- Gebruik nieuwe technologieën
- Gekoppelde database
- Grootschalige gegevensverwerking
- Geautomatiseerde besluitvorming (rechtsgevolg)
- Blokkering contract, dienst of recht
- Gevoelige gegevens (bv. financieel)
- Doorgifte persoonsgegevens buiten EU


VESA NETWORK SOLUTIONS

# Inhoud en consultatie PIA

**In ieder geval omschrijven in PIA:**

- Omschrijving uit te voeren verwerkingen
- Beoordeling noodzakelijkheid, proportionaliteit en subsidiariteit
- Een risicoanalyse
- Maatregelen preventie risico's

<u>Verplichte Consultatie</u>

- Uit PIA blijkt hoge risico's die niet direct oplosbaar zijn
- Toezichthouder reageert binnen acht weken

# Privacy Impact Assesment

- Niet voor bestaande verwerking tenzij:
- Verwerking verandert voor ander doel of nieuwe technologie
- Omgeving verandert: bv. Gevolgen van bep. Beslissingen zijn belangrijker geworden

Advies:

Bij bestaande verwerking na 3 jaar (vanaf 25 mei 2018) PIA

Bij nieuwe verwerkingen gelijk indien noodzakelijk

VESA NETWORK SOLUTIONS

# Functionaris gegevensbescherming (FWG)

**Houdt toezicht op toepassing en naleving AVG**

Verplicht bij:

- > 250 werknemers
- Verwerking wordt verricht door overheid (behalve gerecht)
- Vereiste regelmatige en stelselmatige observatie van betrokkenen
- Grootschalige verwerking bijzondere persoonsgegevens
- Persoonsgegevens strafbare feiten en veroordelingen (stappenplan maken)

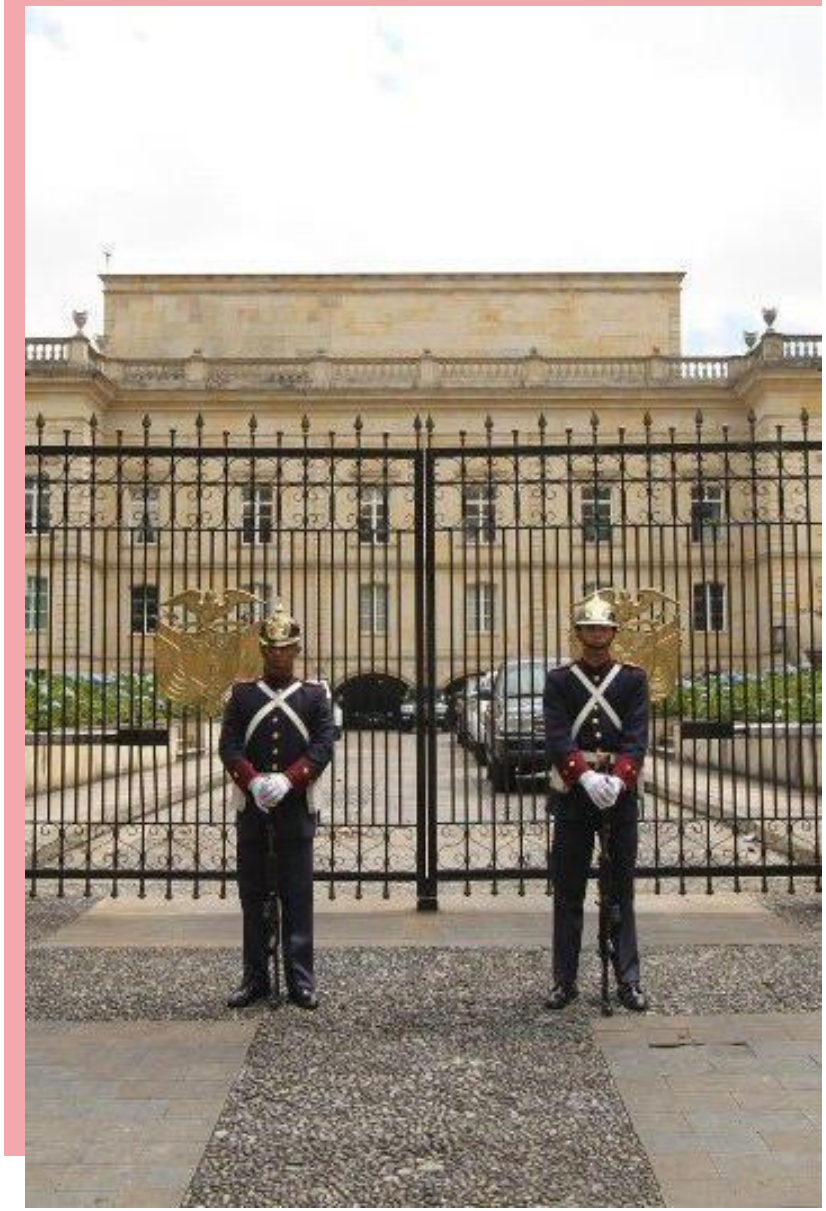

VESA NETWORK SOLUTIONS

# U bent kortom verplicht:

- Persoonsgegevens te beschermen
- Melden van een beveiligingsincident bij Autoriteit Persoonsgegevens en betrokkene
- Passende maatregelen te nemen
- (reparatie lek en voorkomen verdere verspreiding)
- Registratie bijhouden van beveiligingsincidenten

<u>Boete</u>

Bij overtreding maximaal € 900.000,-.



VESA NETWORK SOLUTIONS