Gegevensbeschermingseffectbeoordeling en risicoanalyse

Koen Hostyn
Bureau voor Digitale Veiligheid
DPO AHOVOKS & athumi (Vlaams Datanutsbedrijf)

DIGITAAL VLAANDEREN

Vlaamse overheid

Overzicht

Wat is een DPIA?

Wanneer voer je een DPIA uit?

Hoe voer je een DPIA uit?

DPIA en risico-beheer

Workshops

De gegevensbeschermingseffectbeoordeling

Gegevensbeschermingseffectbeoordeling

DEFINITIE

Een DPIA is een systematisch proces dat is ontworpen om **de waarschijnlijkheid van de risico's** voor de rechten en vrijheden van natuurlijke personen in verband met een bepaalde gegevensverwerking **vast te stellen** en **deze risico's te kunnen beperken**. De beoordeling is met name gericht op de noodzaak en evenredigheid van de verwerking in kwestie en op het bepalen van de maatregelen om de potentiële risico's aan te pakken.

DPIA's zijn belangrijke instrumenten om verantwoording af te leggen, aangezien ze verwerkingsverantwoordelijken niet alleen helpen om te voldoen aan de vereisten van de AVG, maar ook om aan te tonen dat er passende maatregelen zijn genomen om naleving van de verordening te waarborgen.

Met andere woorden, **een DPIA is een proces om naleving op te bouwen en aan te tonen**.

Artikel 35 van de AVG

→ " Wanneer een type verwerking, met name met behulp van nieuwe technologieën, en rekening houdend met de aard, de omvang, de context en de doeleinden van de verwerking, waarschijnlijk een ***hoog risico*** voor de rechten en vrijheden van natuurlijke personen met zich meebrengt,

→ de verwerkingsverantwoordelijke voert voorafgaand aan de verwerking een

→ **beoordeling van de gevolgen van de beoogde verwerkingen voor de bescherming van persoonsgegevens**. (...)

Omstandigheden die een DPIA vereisen

In drie gevallen :

1) **‘Waarschijnlijk een hoog risico’** voor de betrokkenen
2) **Met name vereist** in bepaalde gevallen (zie hiernaast)
3) Toezichthoudende autoriteit kan **lijst** opstellen

Artikel 35 (3)

Met name vereist in de volgende gevallen:

a) een **systematische en uitgebreide beoordeling** van persoonlijke aspecten, die is gebaseerd op geautomatiseerde verwerking, waaraan voor de natuurlijke persoon **rechtsgevolgen zijn verbonden**;

b) **grootschalige verwerking** van **bijzondere categorieën** van persoonsgegevens, of van gegevens met betrekking tot **strafrechtelijke veroordelingen** en strafbare feiten; of

c) **stelselmatige en grootschalige monitoring** van openbaar toegankelijke ruimten.

Voorbeelden van verwerkingsactiviteiten waarbij er ‘waarschijnlijk een hoog risico’ is (WP29-RICHTLIJNEN 4.10.2017)

Verwerkingsactiviteit	Mogelijke relevante criteria
Een ziekenhuis dat genetische en gezondheidsgegevens van patiënten verwerkt	Gevoelige gegevens of gegevens van zeer persoonlijke aard. Gegevens over kwetsbare betrokkenen. Gegevens die op grote schaal worden verwerkt.
Het gebruik van een camerasysteem om het rijgedrag op snelwegen te monitoren, waarbij de controller overweegt om een intelligent videoanalysesysteem te gebruiken om karretjes te selecteren en kentekens te herkennen	Systematische controle. Innovatief gebruik of toepassing van technologische of organisatorische oplossingen.
Een bedrijf dat systematisch de activiteiten van zijn werknemers controleert, inclusief het controleren van het werkstation van de werknemers, internetactiviteiten, enz.	Systematisch toezicht. Gegevens over kwetsbare betrokkenen.
Het verzamelen van openbare sociale-mediagegevens voor het genereren van profielen.	Evaluatie of scoren. Verwerking van gegevens op grote schaal. Matchen of combineren van datasets. Gevoelige gegevens of gegevens van zeer persoonlijke aard:
Opslag voor archiveringsdoeleinden van gepseudonimiseerde persoonlijke gevoelige gegevens van kwetsbare proefpersonen van onderzoeksprojecten of klinische proeven	Gevoelige gegevens. Gegevens over kwetsbare betrokkenen. Verhindert betrokkenen een recht uit te oefenen of toegang tot een dienst of contract.

Is voor deze verwerkingsactiviteiten noodzakelijkerwijs een DPIA vereist?

Verwerking	Mogelijke relevante criteria	*antwoord*
Een verwerking van "persoonsgegevens van patiënten of cliënten door een individuele arts, andere gezondheidswerker of advocaat".	Gevoelige gegevens of gegevens van zeer persoonlijke aard. Gegevens over kwetsbare betrokkenen.	neen
Een instelling die een nationale kredietbeoordelings- of fraudedatabase opzet	Evaluatie of puntentelling. Geautomatiseerde besluitvorming met wettelijke of vergelijkbare significante gevolgen. Verhindert de betrokkene om een recht uit te oefenen of toegang tot een dienst of contract. Gevoelige gegevens of gegevens van zeer persoonlijke aard	ja
Een online magazine dat een mailinglijst gebruikt om een algemene dagelijkse samenvatting naar zijn abonnees te sturen.	Gegevens die op grote schaal worden verwerkt.	neen
Een e-commerce website die advertenties weergeeft voor oldtimeronderdelen met beperkte profilering op basis van bekeken of gekochte artikelen op de eigen website.	Evaluatie of puntentelling	neen

DPIA Lijst VTC (O/2020/01)

OP BASIS RICHTSNOEREN WP29

Op basis **categorieën persoonsgegevens**

- Biometrische gegevens
- Locatiegegevens
- Gegevens van zeer persoonlijke aard
- Telefonie- internet of andere communicatiegegevens
- Camera's, webcams of drones
- Zwarte lijsten

Op basis van **gevolgen**

- Beslissing dienstverlening stop te zetten
- Beslissing dienstverlening te starten

Op basis **categorieën betrokkenen**

- Kinderen en jongeren
- Migratie achtergrond
- Kwetsbare segmenten bevolking
- Monitoring activiteiten werknemers

Op basis **verwerkingswijze**

- Toestellen of sensoren (IoT)
- Matching of samenvoegen datasets
- Niet-Europese leveranciers
- Her-identificatie gepseudonimiseerde gegevens

*Het uitoefenen van een DPIA is **niet altijd verplicht**, maar wel **altijd een goede praktijk** bij systematische verwerking van persoonsgegevens*

Hoe voer je een DPIA uit?

De beoordeling bevat ten minste:

(a) een systematische **beschrijving van de beoogde** verwerkingen en de **doeleinden** van de verwerking, met inbegrip van, in voorkomend geval, het gerechtvaardigde belang dat door de voor de verwerking verantwoordelijke wordt nagestreefd;
(b) een beoordeling van de **noodzakelijkheid en evenredigheid** van de verwerkingen in verhouding tot de **doeleinden**
(c) een beoordeling van de **risico's voor de rechten en vrijheden** van de betrokkenen;
(d) de voorgenomen **maatregelen** om de risico's aan te pakken, met inbegrip van garanties, beveiligingsmaatregelen en mechanismen om de bescherming van persoonsgegevens te waarborgen en de naleving van deze verordening aan te tonen, rekening houdend met de rechten en legitieme belangen van de betrokkenen en andere betrokken personen.

1. Wanneer

VOORAFGAAND AAN DE VERWERKING

Deze vereiste is consistent met **de principes van gegevensbescherming by design en by default**.

De DPIA is een hulpmiddel bij de besluitvorming over de verwerking.

Het moet **zo vroeg mogelijk** in het ontwerp van de operaties worden gestart, zelfs als niet alle operaties bekend zijn, en vervolgens **tijdens het gehele levenscyclusproject** worden bijgewerkt.

Het is een **continu proces**, geen eenmalige oefening: het moet worden bijgewerkt zodra de verwerking daadwerkelijk is gestart, vooral wanneer een verwerking dynamisch is en onderhevig aan veranderingen.

2. Wie?

DE VERWERKINGSVERANTWOORDELIJKE, MET DE DPO EN DE VERWERKER(S)

De **verwerkingsverantwoodelijke blijft verantwoordelijk** voor de taak, zelfs als deze door iemand anders wordt uitgevoerd.

De verwerkingsverantwoordelijke moet **advies inwinnen bij de DPO**, die toezicht blijft houden op de uitvoering van de DPIA.

Als de verwerking geheel of gedeeltelijk wordt uitgevoerd door een **verwerker**, moet deze de verwerkingsverantwoordelijke **bijstaan bij het uitvoeren** van de DPIA.

Waar nodig moet de voor de verwerking verantwoordelijke de **betrokkenen** om hun mening vragen. (toestemming voor verwerking is geen manier)

Het is een goede praktijk om de **rollen en verantwoordelijkheden** te definiëren en te documenteren, bijvoorbeeld in een intern gegevensbeschermingsbeleid.

*De DPO mag de **DPIA zelf niet uitvoeren**, want moet er **onafhankelijk advies** bij kunnen geven*

3. Wat is de methodologie om een DPIA uit te voeren?

VERSCHILLENDE METHODOLOGIEËN MAAR GEMEENSCHAPPELIJKE CRITERIA

De AVG specificeert niet welk DPIA-proces moet worden gevolgd, maar staat in plaats daarvan toe dat de verwerkingsverantwoordelijke **een kader invoeren dat hun bestaande werkpraktijken** aanvult, op voorwaarde dat het rekening houdt met de componenten die worden beschreven in artikel 35, lid 7.

Er zijn verschillende gevestigde processen binnen de EU en wereldwijd die rekening houden met de in overweging 90 beschreven aspecten:

- de context bepalen: "rekening houdend met de aard, het toepassingsgebied, de context en de doeleinden van de verwerking en de bronnen van het risico";

- de risico's beoordelen: "beoordeel de specifieke waarschijnlijkheid en ernst van het hoge risico";

- **de risico's behandelen**: "dat risico beperken" en "de bescherming van persoonsgegevens waarborgen", en "aantonen dat deze verordening wordt nageleefd".

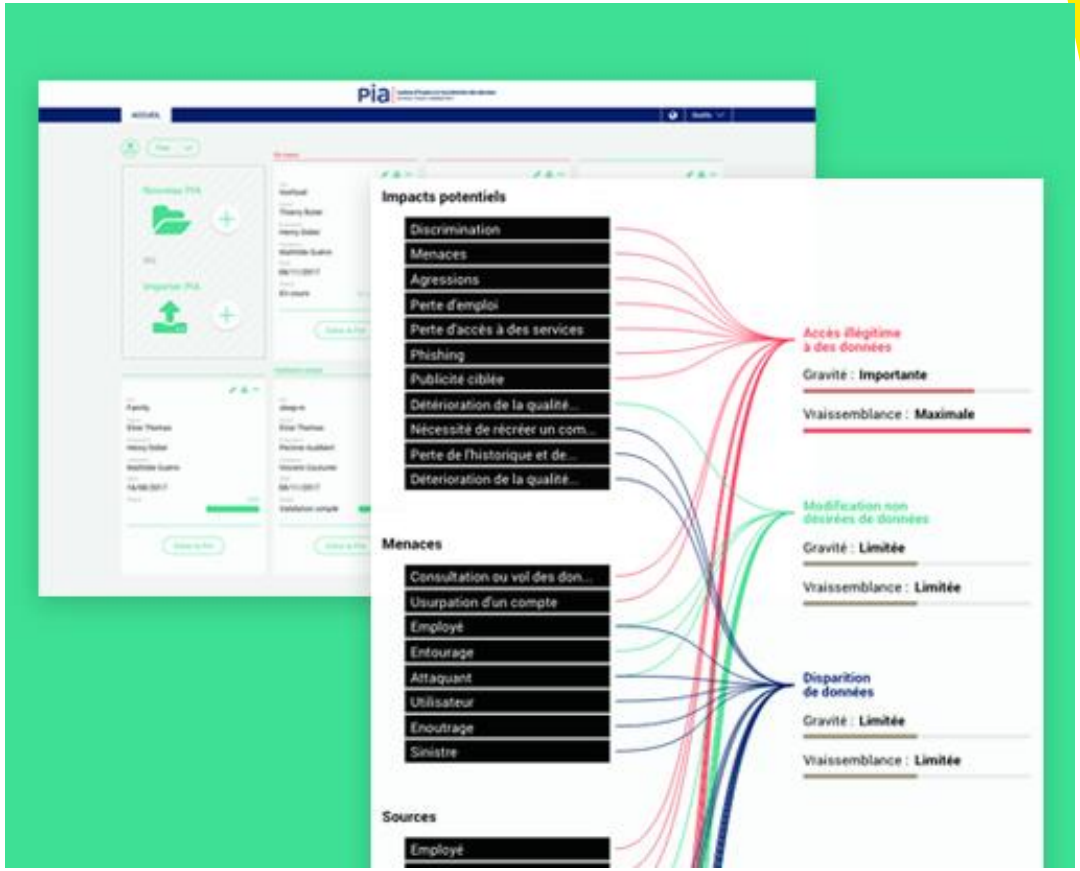
Idealiter sluit het proces van de DPIA nauw aan op het ***risico-beheersingsproces van de organisatie***

Inspiratie

ENKELE VOORBEELDEN

Voorbeeld 1

PIA-TOOL CNIL



Enkele highlights

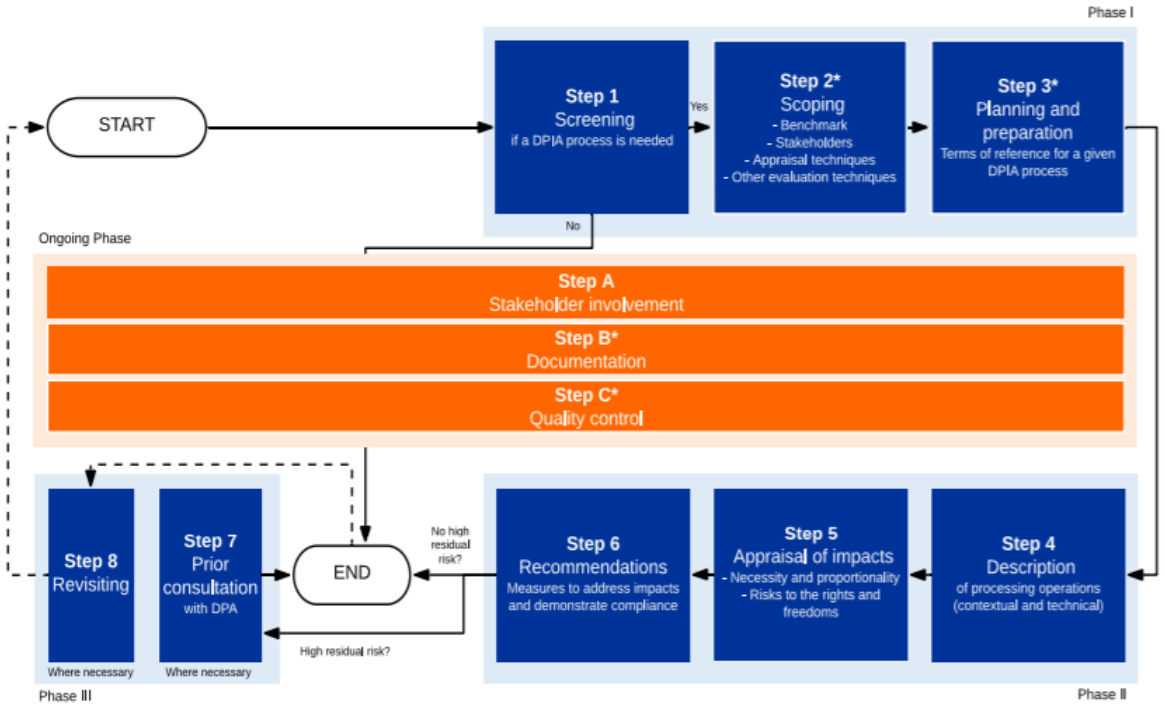
- Ontwikkeld door toezichthouder
- Open Source
- Geïntegreerd in andere GDPR-management tools (bv. Responsum of Dastra)
- Bevat (visuele) risico-mapping
- Vergezeld van richtlijnen over hoe DPIA uit te voeren

Beperkingen

- Beperkt aantal risico's om in te schalen
- Software is niet intuïtief voor beginners

Voorbeeld 2

D.PIA.LAB (VUB) TEMPLATE



Enkele highlights

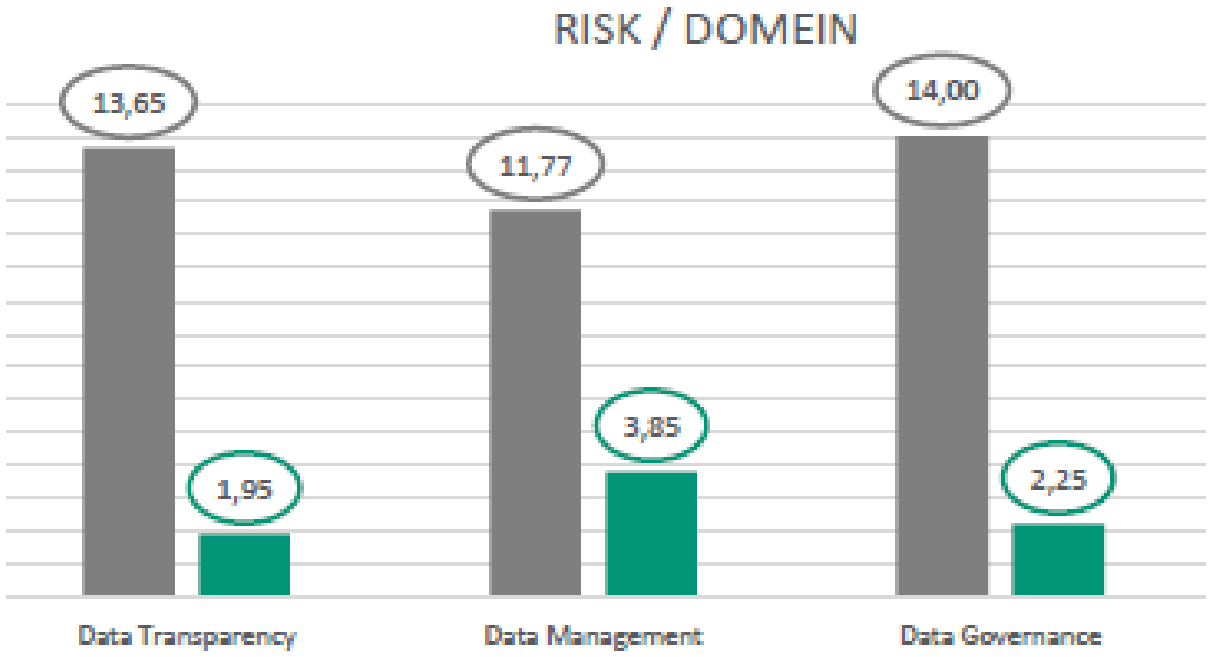
- Ontwikkeld met steun van de Europese Commissie
- Zeer uitgebreid
- Bedoeld als template om verder aan te passen naar concrete situaties (bijvoorbeeld VO)

Beperkingen

- Zeer uitgebreid : invulbare template is >80 blz.

Voorbeeld 3

DPIA MOBILITEITSCENTRALE



Enkele highlights

- Uitgevoerd door externen (USG-profiel)
- Uitgebreide oefening (52 blz.)
- Duidelijke visuele risico-mapping (dashboard)
- 5x5 risicomatrix
- Aanpak inzake risico-analyse is atypisch
  - Data Transparantie Risico's
  - Data Management Risico's
  - Data Governance Risico's

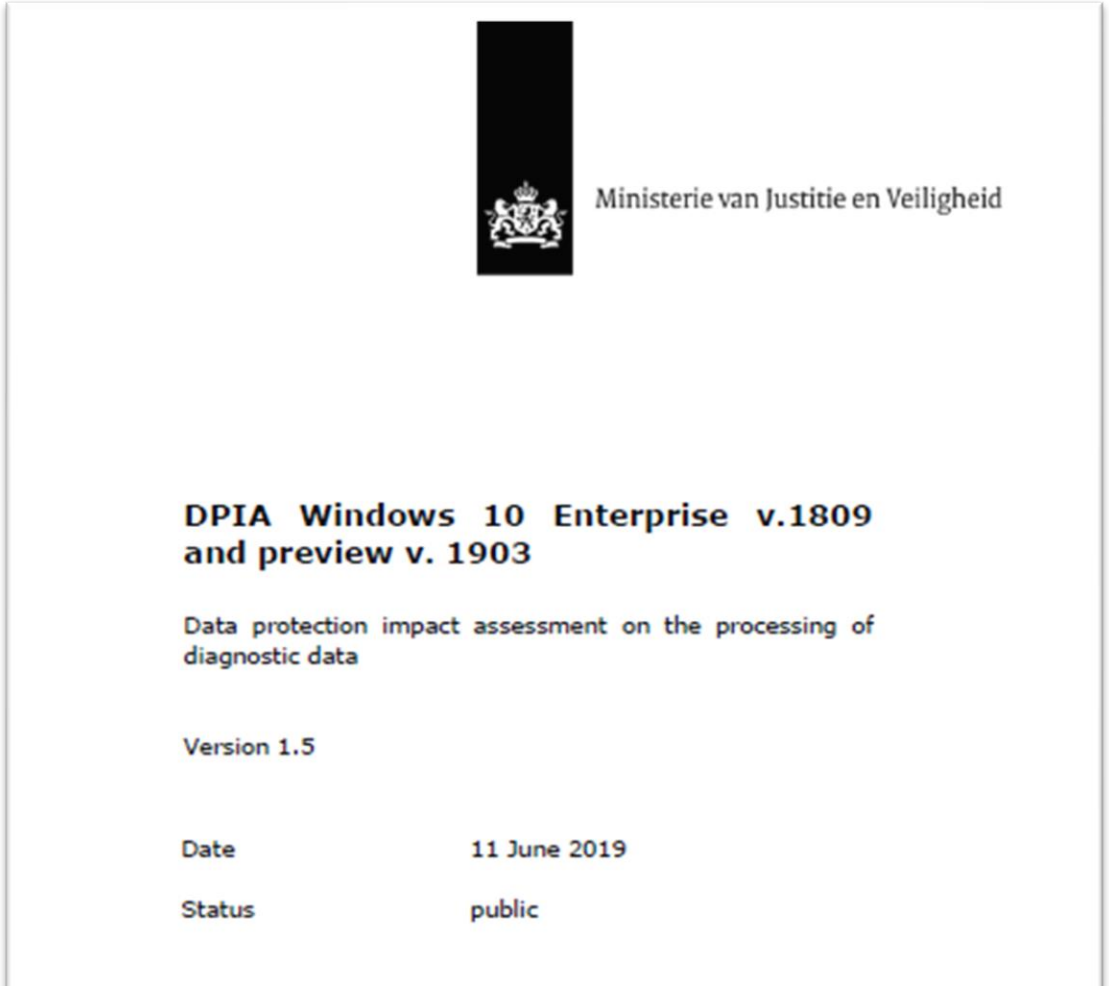
Beperkingen

- Kostprijs USG-profiel (dient binnen budget voorzien te zijn)

Voorbeeld 4

DPIA WINDOWS 10

MINISTERIE VEILIGHEID EN JUSTITIE (NL)



Ministerie van Justitie en Veiligheid

DPIA Windows 10 Enterprise v.1809 and preview v. 1903

Data protection impact assessment on the processing of diagnostic data

Version 1.5

Date 11 June 2019

Status public

Enkele highlights

- Zeer uitgebreide oefening (totaal 180 blz.) met veel tekst
- Voornamelijk juridische insteek
- Bedoeld als instrument om druk op leverancier (bv. Google of Microsoft) uit te oefenen

Beperkingen

- Zeer zware oefening
- Weinig aandacht voor risico-beheersing (mbt. betrokkenen)

Voorbeeld 5

DPIA SJABLOON VTC


Vlaamse overheid

Gegevensbeschermingseffectbeoordeling
(GEB/DPIA)
sjabloon

<NAAM GEB>

Enkele highlights

- Op basis model D.PIA.LAB VUB
- Word-document (vaak toegankelijker dan Excel voor niet-technische profielen)
- Beoordeling beginselen en privacy by design & by default

Beperkingen

- Weinig uitgewerkt kader rond risico-analyse

Criteria om te beoordelen of een DPIA voldoende uitgebreid is om te voldoen aan de AVG

SYSTEMATISCHE BESCHRIJVING VERWERKING

- ☐ er wordt rekening gehouden met de aard, omvang, context en doelen van de verwerking;
- ☐ de persoonsgegevens, de ontvangers en de periode gedurende welke de persoonsgegevens worden bewaard worden geregistreerd;
- ☐ er wordt een functionele beschrijving van de verwerking verstrekt;
- ☐ de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen) worden geïdentificeerd;
- ☐ er wordt rekening gehouden met de naleving van de goedgekeurde gedragscodes;

BEOORDELING NOODZAAK EN EVENREDIGHEID

Maatregelen die bijdragen aan de **evenredigheid en noodzaak** van de verwerking op basis van:

- ☐ een of meer gespecificeerde, expliciete en legitieme doeleinden;
- ☐ rechtmatigheid van de verwerking;
- ☐ toereikend, ter zake dienend en beperkt tot wat noodzakelijke gegevens zijn;
- ☐ beperkte bewaartermijn;

Maatregelen die bijdragen aan de **rechten van de betrokkenen**

- ☐ informatie verstrekt aan de betrokkene;
- ☐ recht van inzage en recht op overdraagbaarheid van gegevens;
- ☐ recht op rectificatie en recht op gegevenswissing;
- ☐ recht van bezwaar en recht op beperking van de verwerking;
- ☐ relaties met verwerkers;
- ☐ waarborgen omtrent internationale doorgifte(n);
- ☐ voorafgaande raadpleging.

CRITERIA OM TE BEOORDELEN (2)

De **risico's voor de rechten en vrijheden** van betrokkenen worden beheerd:

- ☐ er wordt rekening gehouden met de oorsprong, de aard, het specifieke karakter en de ernst van de risico's of, meer specifiek, voor elk risico (onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens) vanuit het perspectief van de betrokkenen:
- ☐ er wordt rekening gehouden met de bronnen van de risico's;
- ☐ de mogelijke gevolgen voor de rechten en vrijheden van de betrokkenen worden geïdentificeerd in geval van gebeurtenissen zoals onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens;
- ☐ bedreigingen die kunnen leiden tot onrechtmatige toegang, ongewenste wijziging en de verdwijning van gegevens worden geïdentificeerd;
- ☐ de waarschijnlijkheid en ernst worden ingeschat;
- ☐ de beoogde maatregelen om de risico's aan te pakken worden bepaald;

De **belanghebbenden** worden betrokken:

- ☐ het advies van de functionaris voor gegevensbescherming wordt ingewonnen;
- ☐ indien nodig wordt de betrokkenen of hun vertegenwoordigers naar hun mening gevraagd.

4. VOORAFGAANDE RAADPLEGING
Artikel 36 van de AVG

ARTIKEL 36 (1)

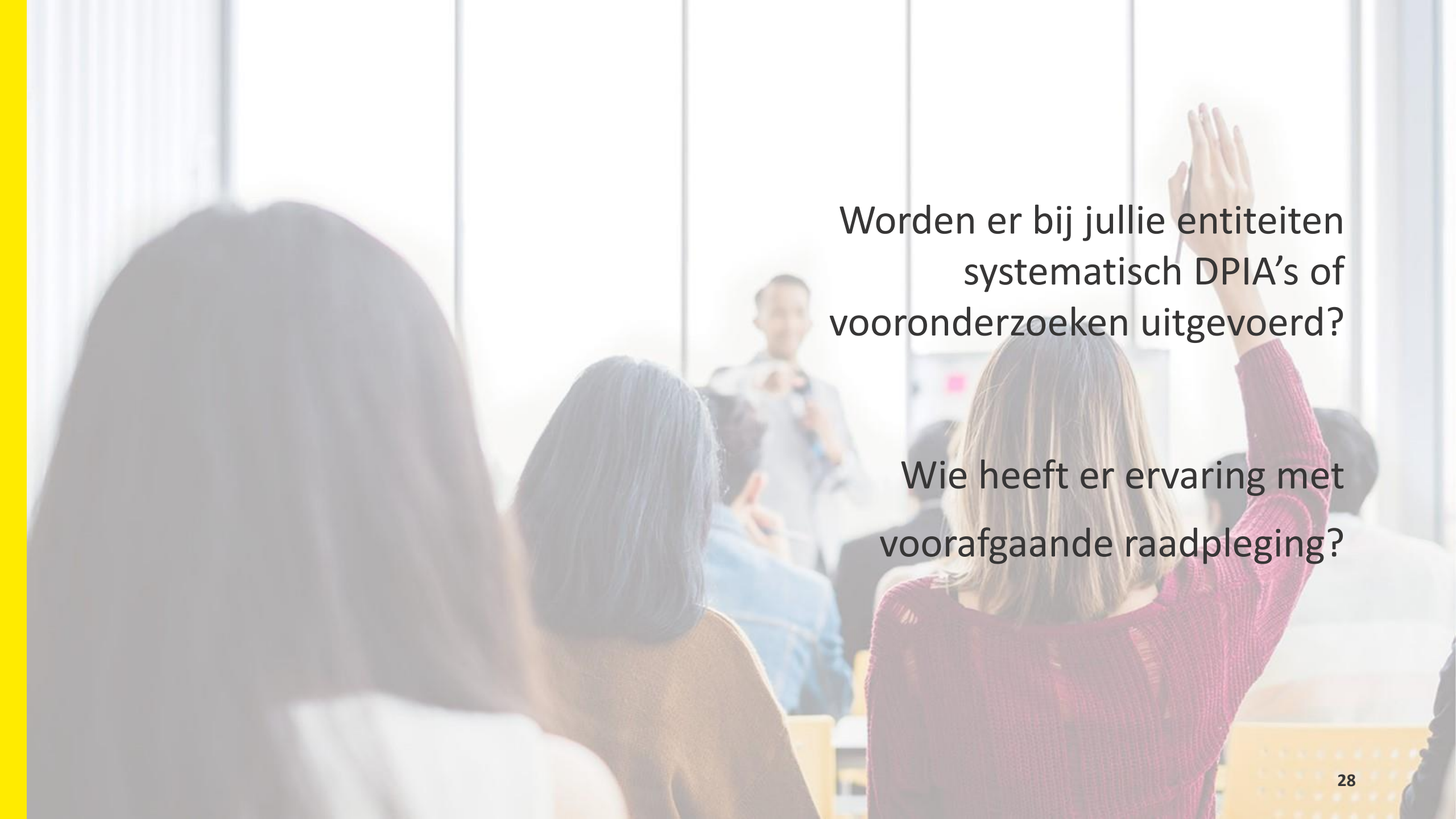
“Wanneer uit een gegevensbeschermingseffectbeoordeling krachtens artikel 35 blijkt dat de verwerking **een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt** om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit.”

OVERWEGING 84

“Wanneer een gegevensbeschermingseffectbeoordeling uitwijst dat verwerking gepaard gaat met **een hoog risico dat de verwerkingsverantwoordelijke niet kan beperken door maatregelen** die met het oog op de beschikbare technologie en de uitvoeringskosten redelijk zijn, dient vóór de verwerking een raadpleging van de toezichthoudende autoriteit plaats te vinden.”

Bij raadpleging van de toezichthoudende autoriteit verstrekt de verwerkingsverantwoordelijke:

- ❑ De respectieve verantwoordelijkheden van verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijken, betrokken verwerker(s)
- ❑ Doeleinden en middelen van de beoogde verwerking
- ❑ Maatregelen en waarborgen ter bescherming van de rechten en vrijheden van de betrokkenen
- ❑ Contactgegevens van de functionaris voor gegevensbescherming, indien van toepassing
- ❑ De DPIA
- ❑ Alle andere informatie waar de toezichthoudende autoriteit om vraagt



Worden er bij jullie entiteiten systematisch DPIA’s of vooronderzoeken uitgevoerd?

Wie heeft er ervaring met voorafgaande raadpleging?

Uitvoeren van de DPIA

ENKELE BEDENKINGEN

- Rol van DPO : vaak **asymmetrie in kennis** en know-how met product owners : belang van opleiding personeelsleden en (waar nodig) externe ondersteuning
- Uitvoeren DPIA maakt deel uit van een **goed Data Governance proces**. Compliance en/of voorkomen van sancties is positief bij-effect
- Nieuwe trend : **gebruik van AI** bij opmaak registers en risico-analyses : opgepast voor delen van bedrijfsgevoelige info en bias van het model
- Om te kunnen aantonen of er hoge risico's zijn, dient er altijd **minstens een vooronderzoek** uitgevoerd te worden

Risicobeheer

Risicobeheer en DPIA: wat is het verschil?

(WP29-RICHTLIJNEN 4.10.2017)

Risicomanagement is een systematisch proces van het identificeren van risico's waarmee een organisatie kan worden geconfronteerd, het uitvoeren van risicoanalyses om de waarschijnlijkheid en impact van de risico's te bepalen, het kwantificeren van de risico's door het bepalen van risicoscores en het toepassen van noodzakelijke risicobeperkende strategieën.

DPIA - strikt verbonden met hoge risico's voor betrokkenen.

Risicomanagement - kan andere gebieden omvatten (informatiebeveiliging) en is vooral gericht op de organisatie.

Veel onderdelen van de DPIA met betrekking tot het risicobeoordelingsgedeelte overlappen met onderdelen van risicobeheer.

Er zijn verschillende raamwerken voor het beoordelen van beveiligingsrisico's (bijv. ISO, NIST)

KADER

Risico : een kwetsbaarheid voor bedreigingen.

Bedreiging : een ongewenste gebeurtenis die zich voordoet zonder waarschuwing en die de organisatie (of in casu : de betrokkenen) schade kan berokkenen.

Risicobeoordeling: het resultaat van de risicoanalyse vergelijken met vooraf bepaalde risicocriteria om te bepalen of het risico (en/of de omvang ervan) al dan niet aanvaardbaar of draaglijk is.

Risicobeheersingsproces: systematische toepassing van managementbeleid, -procedures en -praktijken op de activiteiten van communiceren, raadplegen, de context bepalen en risico's identificeren, analyseren, evalueren, behandelen, controleren en herzien.

Risicocriteria: referentiecriteria aan de hand waarvan het belang van een risico wordt geëvalueerd

"Inherent" risico: verwijst naar de waarschijnlijkheid van een negatief effect bij afwezigheid van beschermende maatregelen

“Residueel" risico: dit verwijst naar de waarschijnlijkheid van een negatieve impact ondanks maatregelen om het (inherente) risico te beperken

Bron: 1) **ISO Guide 73:2009(en)** Risicobeheer. 2) securitesociale.be **BLD RISK** 7 maart 2017

DPIA is niet verplicht voor elke verwerkingsactiviteit

→ alleen voor verwerking met een relevante mate van waarschijnlijkheid van risico's voor de betrokkenen

RISICO

= een scenario dat een gebeurtenis en de gevolgen ervan beschrijft, geschat in termen van ernst en waarschijnlijkheid.

RECHTEN EN VRIJHEDEN

= in de eerste plaats het recht op gegevensbescherming en privacy, maar kan ook betrekking hebben op andere grondrechten zoals vrijheid van meningsuiting, vrijheid van gedachte, vrijheid van verkeer, verbod op discriminatie, recht op vrijheid, geweten en religie.

= vanuit het perspectief van de betrokkene.

"Loopt de betrokkene risico op...?"

Overweging 84

Teneinde de naleving van deze verordening te verbeteren indien de verwerking waarschijnlijk gepaard gaat met ***hoge risico's in verband met de rechten en vrijheden*** *van natuurlijke personen, dient de verwerkingsverantwoordelijke of de verwerker verantwoordelijk te zijn voor het verrichten van een gegevensbeschermingseffectbeoordeling om met name* ***de oorsprong, de aard, het specifieke karakter en de ernst van dat risico*** *te evalueren.*

Met het resultaat van de beoordeling dient rekening te worden gehouden bij het bepalen van de passende maatregelen die moeten worden genomen om aan te tonen dat deze verordening bij de verwerking van persoonsgegevens wordt nageleefd.

Op risico gebaseerde aanpak

HANDLEIDING HULPMIDDEL (VTC / THOMAS MORE) – 16 MAART 2020

Stappen 2 en 3: beschrijf verwerkingsactiviteiten en Bedreigingen voor betrokkenen

ENKELE AANDACHTSPUNTEN

- Maak onderscheid tussen verschillende bronnen, types en oorzaken risico's
  - **Bronnen** : Interne medewerkers, externe medewerkers, onbekenden, natuurlijke fenomenen
  - **Oorzaken** : Opzettelijk gedrag, nalatig gedrag, onafhankelijk van menselijk gedrag
  - **Types** : Ongeautoriseerde toegang of wijziging, (tijdelijke) onbeschikbaarheid van gegevens
- **Minimaal** : risico's inzake verlies aan vertrouwelijkheid, integratie en beschikbaarheid
- Bedenk (realistische) **risico-scenario's** vanuit het perspectief van de betrokkenen
  - Misbruik van gelekte gegevens voor (spear)phishing
  - Discriminatie op de arbeidsmarkt
  - Beperkte toegang tot (overheids)diensten
- Organiseer indien nodig **een workshop** met (vertegenwoordigers van) de betrokkenen en/of (niet-technische) personeelsleden die vertrouwd zijn met het proces

Workshop

WELKE RISICO'S ZIE JIJ?

- ✓
- ✓
- ✓
- ✓
- ✓
- ✓
- ✓
- ✓
- ✓
- ✓

Schepen Mathias Van de Walle en burgemeester Pieter De Crem
© Erwin Mynsberghe

Proefproject in Aalter: haal je rijbewijs of reispas gewoon uit een automaat

In Aalter kan je met de app itsme op je smartphone belangrijke documenten zoals een voorlopig rijbewijs of internationaal paspoort afhalen uit een automaat. De automaat met kluizen staat aan het gemeentehuis. Het gaat om een proefproject van één maand.

Marc Dewilde
vr 07 jul 17:41

Workshop : Welke risico’s zie jij?

VANUIT CIA-MODEL

	Vertrouwelijkheid	Integriteit	Beschikbaarheid
veroorzaakt door nalatig gedrag – intern			
veroorzaakt door nalatig gedrag - extern			
veroorzaakt door opzettelijk gedrag - intern			
veroorzaakt door opzettelijk gedrag - extern			
veroorzaakt door gevarenbronnen die onafhankelijk zijn van menselijk gedrag			

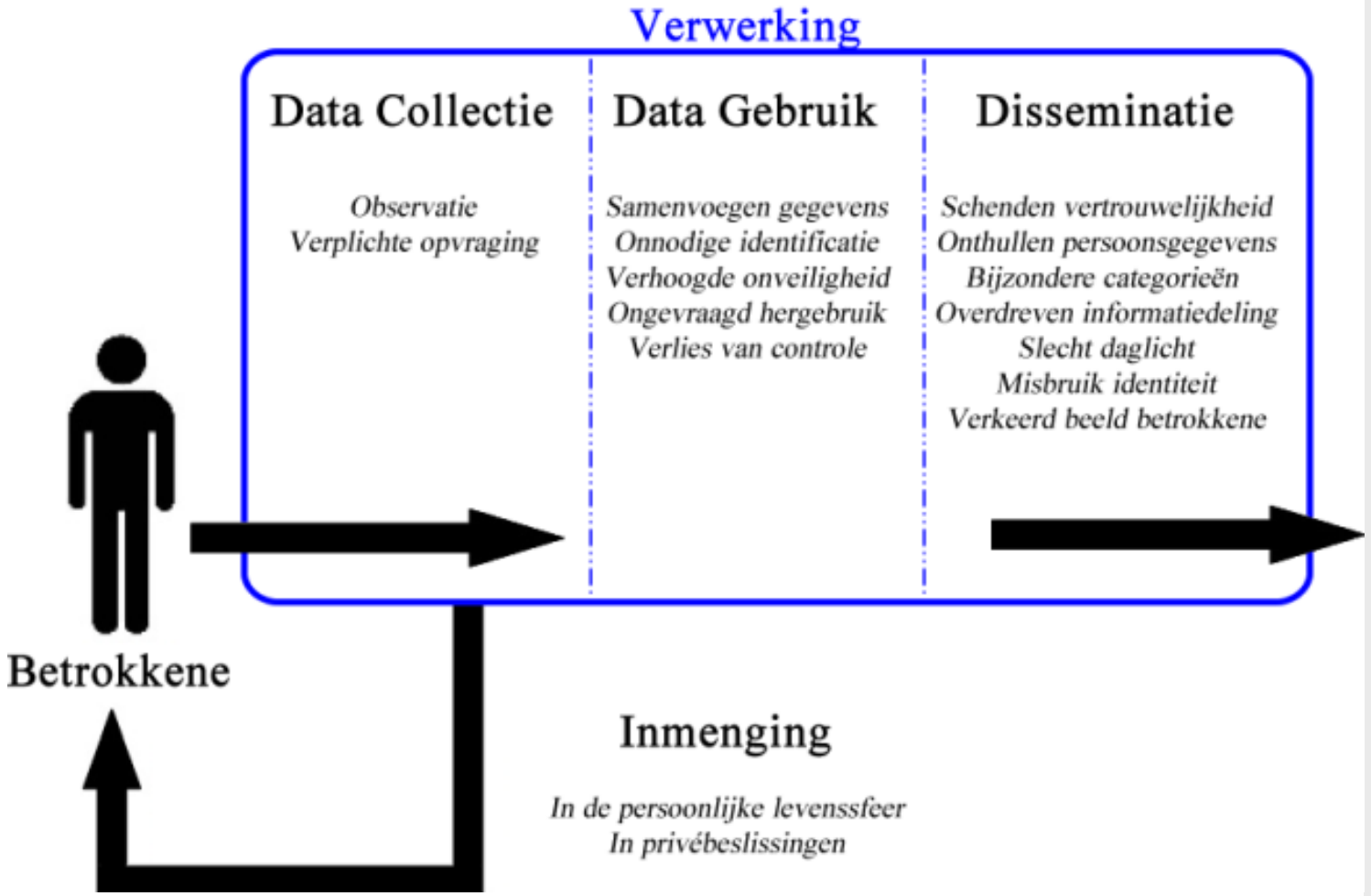
Tool VTC risico betrokkenen

IN 2017 ONTWIKKELD DOOR THOMAS MORE HOGESCHOOL

	C	Bedreiging voor de betrokkene	Loopt de betrokkene het risico dat ...	Samenvatting	Voorbeeld 1	Voorbeeld 2	Risico voor betr	Motiveer waarom er GEEN risico zou zijn voor de betrokkene
Data Collectie	A1	Observatie	... diens doen en laten te regelmatig wordt geregistreerd, zonder dat hij/zij het weet of zonder dat er een rechtsgrond voor is?	Wanneer mensen of organisaties continu op een bepaalde manier naar ons kijken of luisteren, zoals bijv. bij bewaking, heeft surveillance een problematisch effect. Dit kan gevoelens van angst en ongemak veroorzaken. Het risico van een "huiveringwekkend effect" is zo groot dat het de manier waarop mensen zich in de samenleving gedragen kan veranderen , uit angst voortdurend te worden geobserveerd.	Een leerling neemt de lessen op (audio) omdat die omwille van handbreuk niet kan noteren, dit houdt in dat die ook opmerkingen van andere leerlingen opneemt waardoor zij, omwille van die opname, misschien tijdens de les minder	Een werkgever observeert sollicitanten voordat ze binnenkomen voor het gesprek om te kijken hoe zenuwachtig ze zijn en dus de stressbestendigheid te analyseren.	O	
	A2	Verplichte opvraging	... hij/zij zich, vanuit een onevenwichtige relatie met de verwerkingsverantwoordelijke, gedwongen voelt informatie te geven die niet noodzakelijk is voor de verwerking?	Het opvragen van informatie door middel van expliciete of inherente dwang en is een schadelijke activiteit, zelfs als de informatie niet aan derden beschikbaar wordt gesteld. De dwang hoeft niet direct te zijn, en moet niet verstaan worden als regelrechte dwang met expliciete bedreigingen. Dwang kan bijv. ook voortkomen uit de angst om geen baan te krijgen of om sociaal schande te vermijden.	Een werkgever vraagt aan een werknemer dat die medische informatie vertelt over zichzelf of anders kan er niet overgegaan worden tot een vast contract.	Vooraleer je toegang kan krijgen tot extra informatie over de muziekawards en eventueel gratis jouw stem kunt uitbrengen voor jouw favoriete artiest, moet je een account op de website aan maken. Voor dit profiel zijn een e-mail adres, woonplaats en geboortedatum verplichte velden.	O	
Data gebruik	B1	Samenvoegen gegevens	... er, door het combineren van gegevenssets, nieuwe persoonsgegevens over hem/haar worden 'gecreëerd'?	Door het verzamelen van informatie over een persoon en deze te gaan combineren, beginnen de verschillende stukjes en beetjes van gegevens een portret van een persoon te vormen. Het geheel wordt groter dan de som van de delen. Bij analyse kan samengevoegde informatie nieuwe feiten over een persoon onthullen waarvan de betrokkene niet verwacht had dat dit onthuld zou worden toen de originele, geïsoleerde gegevens werden verzameld.	Gegevens van een ANPR-camera (nummerplaat-herkenning) worden gekoppeld aan parkeergegevens en gegevens van het gebruik van het openbaar internetnetwerk om het doen en laten van toeristen te volgen.	Zoektermen bij zoekmachines, aankoopgedrag op het internet en locatiegegevens worden via smartphones apps met elkaar gecombineerd om zo gerichte reclame te kunnen maken naar aanstaande moeders	O	
	B2	Onnodige identificatie	... hij/zij op basis van de gegevens kan worden geïdentificeerd zonder dat dit nodig is voor de verwerking en/of zelfs schadelijk kan zijn?	Bij identificatie gaat het niet zo zeer om de inhoud van de digitale gegevens maar eerder over de link die kan gelegd worden met de fysieke persoon, over verschillende datasets heen. Identificatiedocumenten/checkpoints/... hebben enkele voordelen, zoals het verminderen van de kans op fraude of in de strijd tegen terrorisme. Maar anonimiteit en pseudonimiteit beschermen mensen tegen vooroordelen op basis van hun identiteit en stellen mensen in staat om vrijer te stemmen, te spreken en te verbinden	Bij een sollicitatieprocedure wordt er op basis van de naam een onderscheid gemaakt tussen mannen/vrouwen, autochtoon/allochtoon, ...	Een energie leverancier geeft op hun site de mogelijkheid tot een gratis inschatting over energieverbruik en het beste energiecontract. Bij de verwerking wordt er, op basis van het opgegeven adres en e-mail adres, een (financieel) profiel opgesteld van de aanvrager, om zo 'oninteressante' klanten te	O	
	B3	Verhoogde onveiligheid	... hij/zij door onachtzaamheid bij de verwerking later schade zal ondervinden?	Onzorgvuldige beveiliging gaat niet over schade die iemand wordt toegebracht door het onthullen van persoonsgegevens met de huidige verwerking, maar over nalatigheid en onzorgvuldige bescherming van informatie die leidt tot mogelijke toekomstige schade. Verschillende bedrijven en instellingen houden "digitale dossiers" - uitgebreide opslagplaatsen van persoonlijke informatie - bij van de betrokkene. Het niet	Personeelsdossiers staan op de gemeenschappelijke schijf van de organisatie.	Omwille van het gebruikersgemak, kunnen alle gegevens van het Elektronisch Patiënten Dossier van een groep geselecteerd patiënten met enkele klikken worden gekopieerd naar Excel.	X	
	B4	Ongevraagd hergebruik	... zijn/haar gegevens voor een nieuw doel worden verwerkt, zonder dat hij/zij daarvan op de hoogte is?	Hergebruik wordt gedefinieerd als het gebruik van gegevens voor een doel dat niet gerelateerd is aan het doel waarvoor de betrokkene heeft toegestemd om zijn gegevens te delen. De schade van hergebruik schuilt in de angst en onzekerheid over hoe iemands informatie in de toekomst zal worden gebruikt, waardoor een gevoel van	Het adres dat werd opgegeven voor een levering, wordt later gebruikt door een ander bedrijf om gerichte reclame te versturen.	De contactgegevens van de patiënten van een lokaal publiek ziekenhuis worden door politici gebruikt om verkiezingsinformatie op te sturen.	O	
	B5	Verlies van controle	... hij/zij geen informatie of controle heeft over welke gegevens over hem/haar er worden verwerkt en met welk doel?	Uitsluiting gebeurt door na te laten om de betrokkene op de hoogte te brengen van en informatie te geven over de verwerking. De schade wordt berokkend door de betrokkene geen toegang te geven tot zijn persoonlijke gegevens, niet te informeren over hoe die gegevens worden gebruikt en doordat de betrokkene niets kan ondernemen om invloed uit te oefenen op het gebruik van zijn gegevens.	Voor het volgen van het kijkgedrag van de digitale televisie wordt toestemming gevraagd, maar er wordt niet gespecifieerd hoe ze dit kijkgedrag gaan volgen en wat ze ermee gaan doen. Ook heeft de kijker zelf geen toegang tot zijn	De klant doet samen met zijn bestelling mee aan een tombola waarvoor hij enkele vragen moet invullen. Achteraf kan de klant zijn antwoorden en de resultaten van de tombola niet meer raadplegen. Hij krijgt enkel een verwittiging indien hij iets gewonnen heeft.	O	

Workshop : Welke risico’s zie jij?

MET BEHULP RISICO TOOL RISICOCRITERIA VTC



- Data Collectie: wordt er voor de verwerking, persoonsgegevens van een betrokkene verzameld of gegenereerd?
- Data gebruik: wordt er tijdens de verwerking, persoonsgegevens van een betrokkene gebruikt?
- Disseminatie: worden er persoonsgegevens vanuit de verwerking (de toepassing, het project) verspreid - intern of extern?
  - Dit kan zowel menselijk leesbaar (bijv. webpagina) of machine leesbaar (bijv. API of een file) zijn.
- Inmengen: beïnvloed de verwerking het gedrag of de besluitvorming van de betrokkene?

*Let op voor de **inherente bias** van de opstellers van de DPIA. Zij dienen zich te verplaatsen in het **perspectief van de betrokkenen** (bijvoorbeeld kwetsbare segmenten van de bevolking)*

STAP 4 EN 5 : RISICOANALYSE EN MAATREGELEN

Een tabel moet de risico's koppelen aan een aantal maatregelen.

Geef voor elk aan:

1. Een inschaling van de waarschijnlijkheid en impact het inherente risico
2. De technische, organistaorische en juridische maatregelen om het risico te beperken
    1. Technisch : Veiligheidsbouwstenen, encryptie, toegangsbeheer (technisch), etc
    2. Organisatorisch : Procedures, bewustmaking, enzovoort
    3. Juridisch : Contracten, protocollen, vertrouwelijkheidsverklaringen, SLA's, etc
3. Een inschaling van het residuele risico
4. De risico-aanvaardings strategie (zie verder)

Risico-matrix

EEN VOORBEELD

Impact	**Maximum impact (4)** Betrokkene kan significante, of zelfs onomkeerbare, gevolgen ondervinden	4	8	12	16
	Belangrijke impact (3) Betrokkenen kunnen significante gevolgen ondervinden, die zij kunnen overkomen mits met ernstige problemen	3	6	9	12
	Beperkte impact (2) Betrokkenen kunnen significante ongemakken ondervinden, die zij ondanks enkele moeilijkheden kunnen overkomen	2	4	6	8
	Verwaarloosbare impact (1) Betrokkenen zijn niet beïnvloed of ondervinden enkele ongemakken, die ze zonder enig probleem overkomen	1	2	3	4
		Niet erg waarschijnlijk (1) (0%-20%) (bv. minder dan één keer per jaar)	**Waarschijnlijk (2)** (21%-49%) (bv. minstens één keer per jaar maar niet maandelijks)	**Zeer waarschijnlijk (3)** (50% - 85%) (bv. Maandelijks maar niet wekelijks)	**Bijna zeker (4)** (> 85%) (bv. wekelijks)
		Waarschijnlijkheid / Kans			

*Een risicobeoordeling dient **voldoende schalen te bevatten** teneinde een genuanceerde evaluatie van geïdentificeerde risico mogelijk te maken.*

*Het voorzien van **slechts drie schalen** (laag, medium en hoog) om risico's te beoordelen **is onvoldoende** om tot een correcte appreciatie te leiden.*

- Richtlijnen risico-beoordeling KSZ (BLD Risk)

Workshop

SCHAAL DEZE RISICO'S IN

Impact	**Maximum impact (4)** Betrokkene kan significante, of zelfs onomkeerbare, gevolgen ondervinden	4	8	12	16
	Belangrijke impact (3) Betrokkenen kunnen significante gevolgen ondervinden, die zij kunnen overkomen mits met ernstige problemen	3	6	9	12
	Beperkte impact (2) Betrokkenen kunnen significante ongemakken ondervinden, die zij ondanks enkele moeilijkheden kunnen overkomen	2	4	6	8
	Verwaarloosbare impact (1) Betrokkenen zijn niet beïnvloed of ondervinden enkele ongemakken, die ze zonder enig probleem overkomen	1	2	3	4
		Niet erg waarschijnlijk (1) (0%-20%) (bv. minder dan één keer per jaar)	**Waarschijnlijk (2)** (21%-49%) (bv. minstens één keer per jaar maar niet maandelijks)	**Zeer waarschijnlijk (3)** (50% - 85%) (bv. Maandelijks maar niet wekelijks)	**Bijna zeker (4)** (> 85%) (bv. wekelijks)
		Waarschijnlijkheid / Kans			

Risico 1 : De gemeente Aalter verliest Willem (53) zijn identiteitsbewijs. Hij heeft tijdelijk geen toegang tot bepaalde diensten van de overheid.

Risico 2 : Een onbekende steelt de telefoon van Ahmad (19) en slaagt erin een identiteitsbewijs aan te vragen die hij/zij gebruikt om identiteitsfraude te plegen.

Risico 3 : Jitse (33) haar rijbewijs is ingetrokken door te rijden onder invloed tijdens de werkuren, deze informatie komt terecht bij haar werkgever.

Risico 4 : Henk (43) wil zijn recht op vergetelheid uitoefenen bij een online winkel, maar krijgt het kastje met z'n nieuwe identiteitsbewijs niet open.

Risico 5 : Nieke (78) wil een internationaal paspoort aanvragen en krijgt de boodschap dat ze dat maar online moet doen.

STAP 6 : RISICO EVALUATIE

Er zijn **verschillende strategieën** voor risico-beheersing

- Aanvullende maatregelen nemen om risico verder te reduceren
- Risico's overdragen (bijvoorbeeld naar een verwerker of derde partij)
- Voorafgaande raadpleging toezichthoudende autoriteit
- Risico's aanvaarden

Hangt af van de **risico-appetijt** van de verwerkingsverantwoordelijke

De **restrisico's** moeten, na advies van de DPO, **formeel worden aanvaard** door de verwerkingsverantwoordelijke (Meestal verantwoordelijke voor het dagelijkse bestuur)

Indien de verwerkingsverantwoorlijke **afwijkt van het advies**, dient hij dit binnen een termijn van 90 dagen gemotiveerd laten weten (cf. DPO-besluit)

*Het uitvoeren van de DPIA en de risico-aanvaarding is **een krachtig instrument voor de DPO** om aanvullende maatregelen onder de aandacht te brengen*

Risico-evalutie

EN WAT VERDER?

De risico’s dienen opgenomen te worden in **een risico register** en hieraan dient ook **een risico levencyclus** gekoppeld te worden, bijvoorbeeld :

- Stap **IDENTIFICATIE** : voeg risico's toe of verwijder ze. Pas eventueel de beschrijving van het risico aan de context.
- Stap **ANALYSE** : analyseer alle in het register voorgestelde risico's, dwz schat voor elk risico de waarschijnlijkheid en impact, controle (beschrijf de relevante elementen indien nodig), **bepaal de risico-eigenaar** en geef een aanbeveling voor de mogelijke risico 'response’.
- Stap **EVALUTIE** : bepaal de kost van de te nemen maatregeling en beslis de uiteindelijke actie.
- Stap **OPVOLGING** : bepaal op regelmatige tijden de status van de vooruitgang van de uitvoering van de maatregelingen en verander eventueel geschatte waarden.

Wijzigt de verwerkingsactiviteit of zijn de **beheersingsmaatregelen achterhaald**, pas dan de DPIA en de risico-analyse aan

Vragen?