Ministerie van Veiligheid en Justitie

Werkwijze DGSenB voor rechtmatige en gestructureerde gegevensuitwisseling

Versie 1.0 - 1 juni 2017

Ten geleide

• Voorliggend document betreft een **werkwijze** voor rechtmatige en gestructureerde gegevensdeling;

• Om voorliggend document leesbaar te houden, betreft het een beschrijving van de werkwijze op **hoofdlijnen**.

• De voorbeelden berusten op de werkelijkheid, maar zijn a) **geanonimiseerd** en b) **volstrekt willekeurig** ingevuld. Neem ze niet letterlijk!

• De werkwijze biedt **handvatten**, **geen garantie** voor rechtmatige en gestructureerde gegevensdeling; wij zijn daarom niet verantwoordelijk voor de uitkomsten.

• Deze werkwijze betreft een **best practice** die is opgesteld en beproefd in de praktijk. De werkwijze is niet in beton gegoten. Suggesties voor verbeteringen? Stuur deze naar Ketenregie (ketenregie@minvenj.nl);

• Voor **vragen** over (de toepassing van) de werkwijze, kunt u tevens contact opnemen met Ketenregie (ketenregie@minvenj.nl).

Gegevensdeling

In de praktijk wisselen we gegevens met elkaar uit om onze taken uit te voeren. Zo kunnen we goede zorg verlenen, bijstand bieden of opsporing en vervolging mogelijk te maken.

Gegevens delen is nodig om:

- **Enerzijds:**

  noodzakelijk om bredere doelstellingen te realiseren en urgente maatschappelijke problemen op te lossen, zoals terrorisme, veiligheid, mobiliteit en goede en betaalbare zorg.

- **Anderzijds:**

  ieder mens heeft het recht om met rust gelaten te worden. Uitgangspunt is dat de overheid niet mag ingrijpen in het leven van haar burgers en geen persoonsgegevens mag verwerken, tenzij daar een lettelijke grondslag voor is (‘geen inmenging, dan voor zover bij wet is voorzien’).

Gegevensbescherming: waarom belangrijk?

- **Historische achtergrond privacy**

  → het recht om met rust te worden gelaten

- **Grondrecht verankerd in internationale en nationale wetgeving**

  → Art. 17 VN-verdrag voor Burgerlijke en politieke rechten:

  Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam.

  → Art. 8 EVRM:

  Lid 1: *Een ieder heeft het recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*

  Lid 2: *Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien.*

  → Artikel 10 Grondwet:

  Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer

Gegevensbescherming: waarom *verder* belangrijk?

28 december 2015

CBP krijgt boetebevoegdheid en wordt Autoriteit Persoonsgegevens

Nieuwsbericht / 28 december 2015

Op 1 januari 2016 treden belangrijke wijzigingen van de Wet bescherming persoonsgegevens (Wbp) in werking. De naam van het College bescherming persoonsgegevens verandert op dat moment in Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens kan direct boetes opleggen als organisaties de Wbp overtreden. Daarnaast geldt vanaf 1 januari de meldplicht datalekken.

8 juli 2016

CBP krijgt boetebevoegdheid en wordt Autoriteit Persoonsgegevens

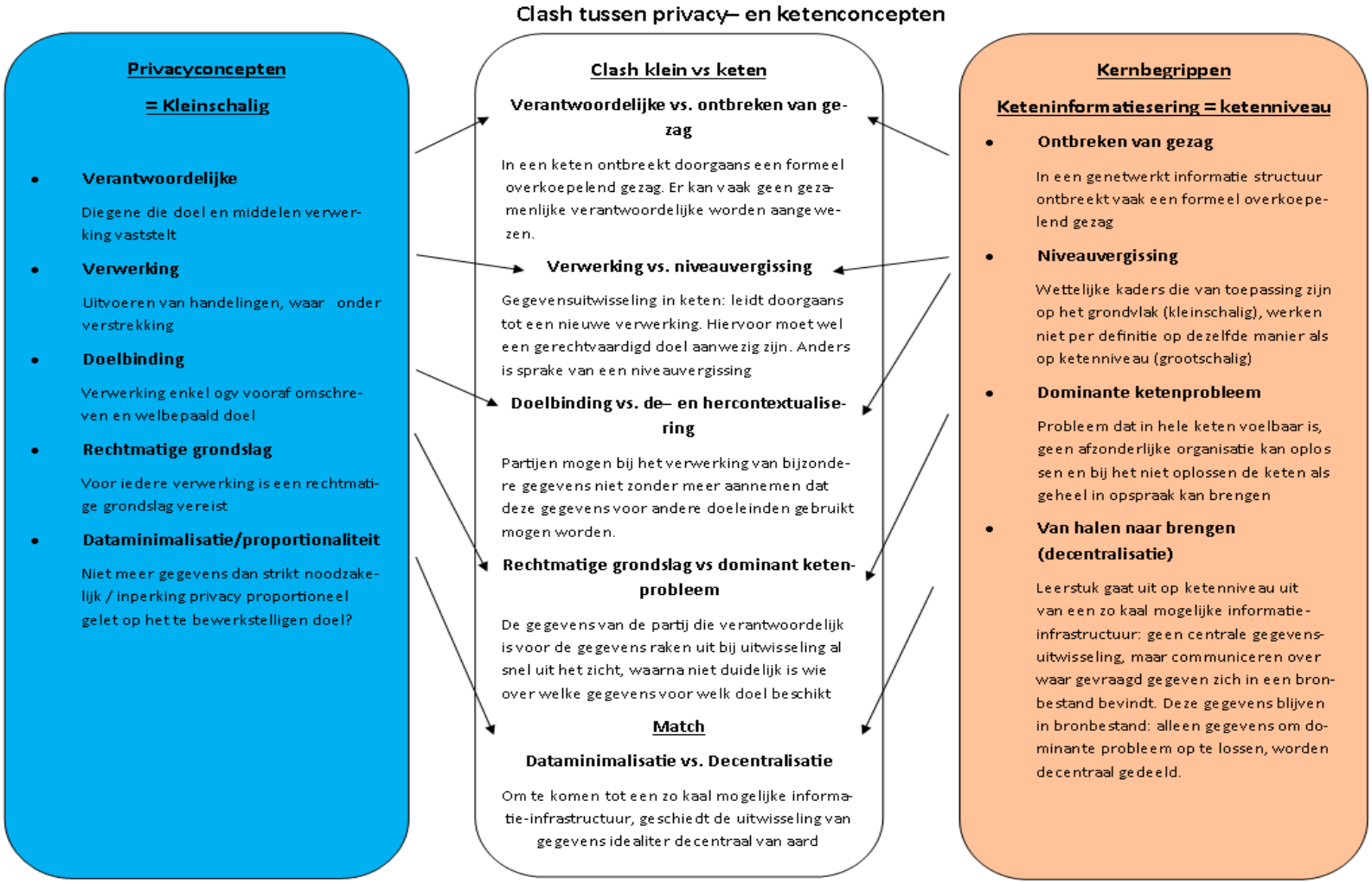
Nieuwsbericht / 28 december 2015

Op 1 januari 2016 treden belangrijke wijzigingen van de Wet bescherming persoonsgegevens (Wbp) in werking. De naam van het College bescherming persoonsgegevens verandert op dat moment in Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens kan direct boetes opleggen als organisaties de Wbp overtreden. Daarnaast geldt vanaf 1 januari de meldplicht datalekken.

28 mei 2017: AVG

5. Inbreuken op onderstaande bepalingen zijn overeenkomstig lid 2 onderworpen aan administratieve geldboeten tot 20 000 000 EUR of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is:

Gegevensbescherming in ketens: waarom een lastig onderwerp?



Zie M.J. Bonthuis, Dataprotectie in ketens, P&I, Afl. 4 – augustus 2016

Dit vraagt om een oplossing!

Omdat we in de praktijk vaak aanlopen tegen onwetendheid, niet voldoende kennis (vaak door tijdgebrek) en verschillende wettelijke regimes is het lastig om eenduidig aan te geven wat wel en niet mag.

Uit noodzaak is daarom een praktische werkwijze ontwikkeld. Een werkwijze gekenmerkt door samenwerking en multidisciplinariteit die leidt tot concrete oplossingen voor op de werkvloer.

Op gestructureerde wijze aanpakken van soorgelijke vraagstukken levert veel duidelijkheid en kansen op om zorgvuldig gegevens met elkaar te delen.

De aanpak van de werkwijze

Aanpak

1. Breng het proces en de verstrekkingsmomenten hierbinnen op objectieve wijze in kaart;
2. Beoordeel de rechtmatigheid van de verwerking (door zowel de verstrekker als de ontvanger);
3. Beschrijf en beoordeel risico's;
4. Beschrijf voorgenomen maatregelen.

Inzet door de organisaties

- Gezamenlijk met ketenpartners

  → *leidt tot een uniform, gedeeld beeld van het proces*

- Multidisciplinaire teams (werknemers op de werkvloer, juristen en ICT'ers /informatiedeskundigen)

  → *leidt tot een zo volledig en juist mogelijk beeld van het proces*

Kansen en voordelen van de werkwijze

De medewerker

- Leidt tot meer houvast en duidelijkheid bij gegevensuitwisseling;
- Leidt tot een kleinere kans op fouten, minder zorgen.

Organisatie

- Draagt bij aan accountability (aantoonbaar aan de wet voldoen).
- Draagt bij aan een efficiënter primair proces;
- Draagt bij aan het borgen van kennis en expertise over gegevensuitwisseling in de organisatie.
- Bundeling schaarse expertise en ontzorgen binnen projecten/programma's

Systemen

- Draagt bij aan een betere beheersing van beschermingsmaatregelen (zoals bijvoorbeeld het voorkomen van datalekken).

De maatschappij

- Draagt bij aan verantwoording en transparantie door publieke organisaties;
- Draagt bij aan dat betrokkenen hun rechten kunnen uitoefenen.

Stap 1a. Beschrijf het proces

Alle relevante aspecten…

- Breng het werkproces in kaart (bijv. met een grond-/procesplaat);
- Van A tot Z;
- Op objectieve wijze;
- Met actoren, relaties tussen actoren en (informatie)producten;
- Benoem de verstrekkingsmomenten.

..vanuit een multidisciplinair perspectief

- Medewerkers op de werkvloer

  → *kunnen input leveren over bijvoorbeeld hoe het proces eruit, welke gegevens uitgewisseld worden en welke gegevens noodzakelijk zijn voor een goede taakuitoefening;*

- Juristen

  → *kunnen input leveren over bijvoorbeeld de taak en grondslag voor verwerking van betrokken organisaties;*

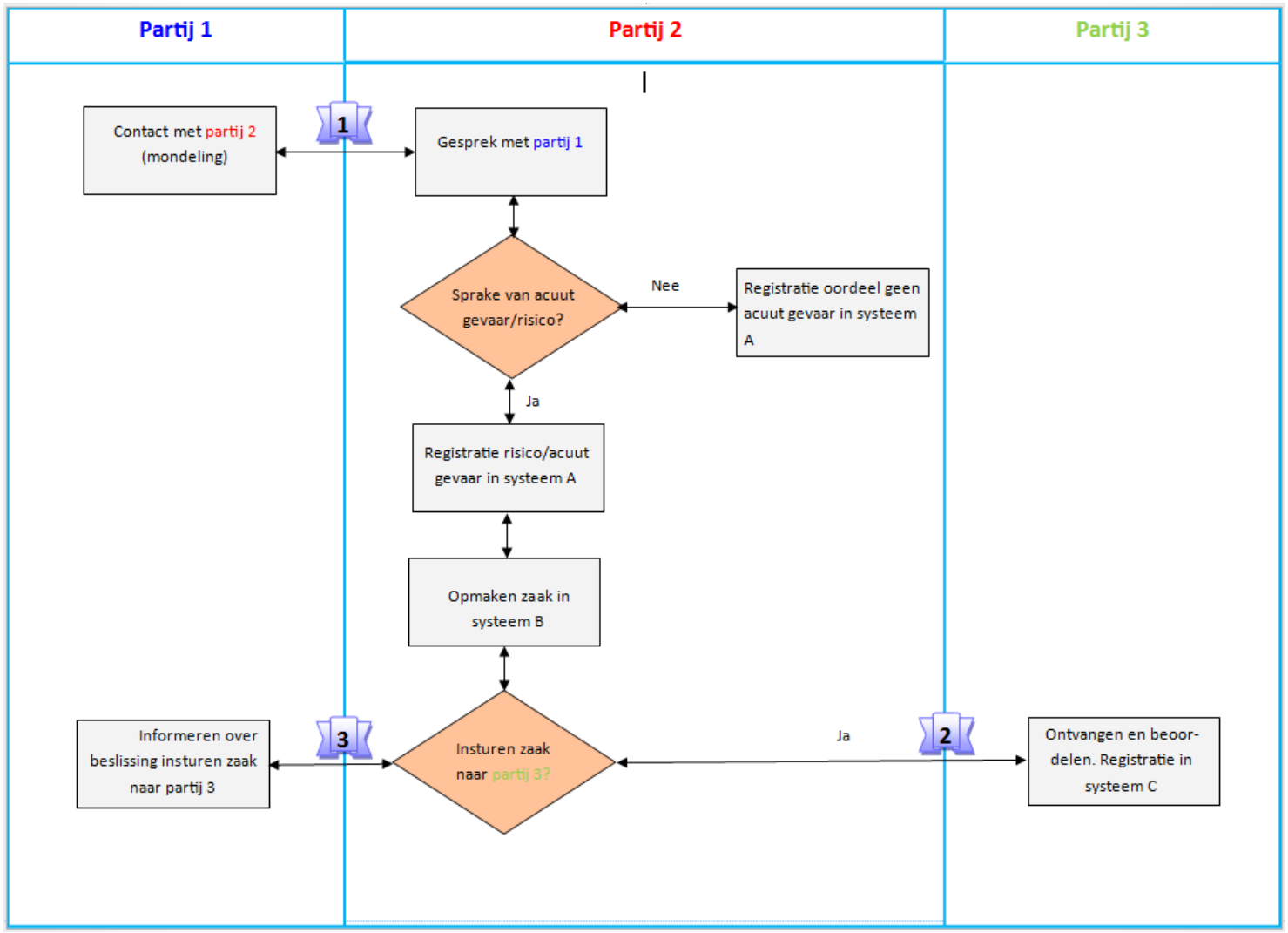
- Informatiekundigen

  →*kunnen de juiste vragen stellen en passende vraagformuleringen voorbereiden;*

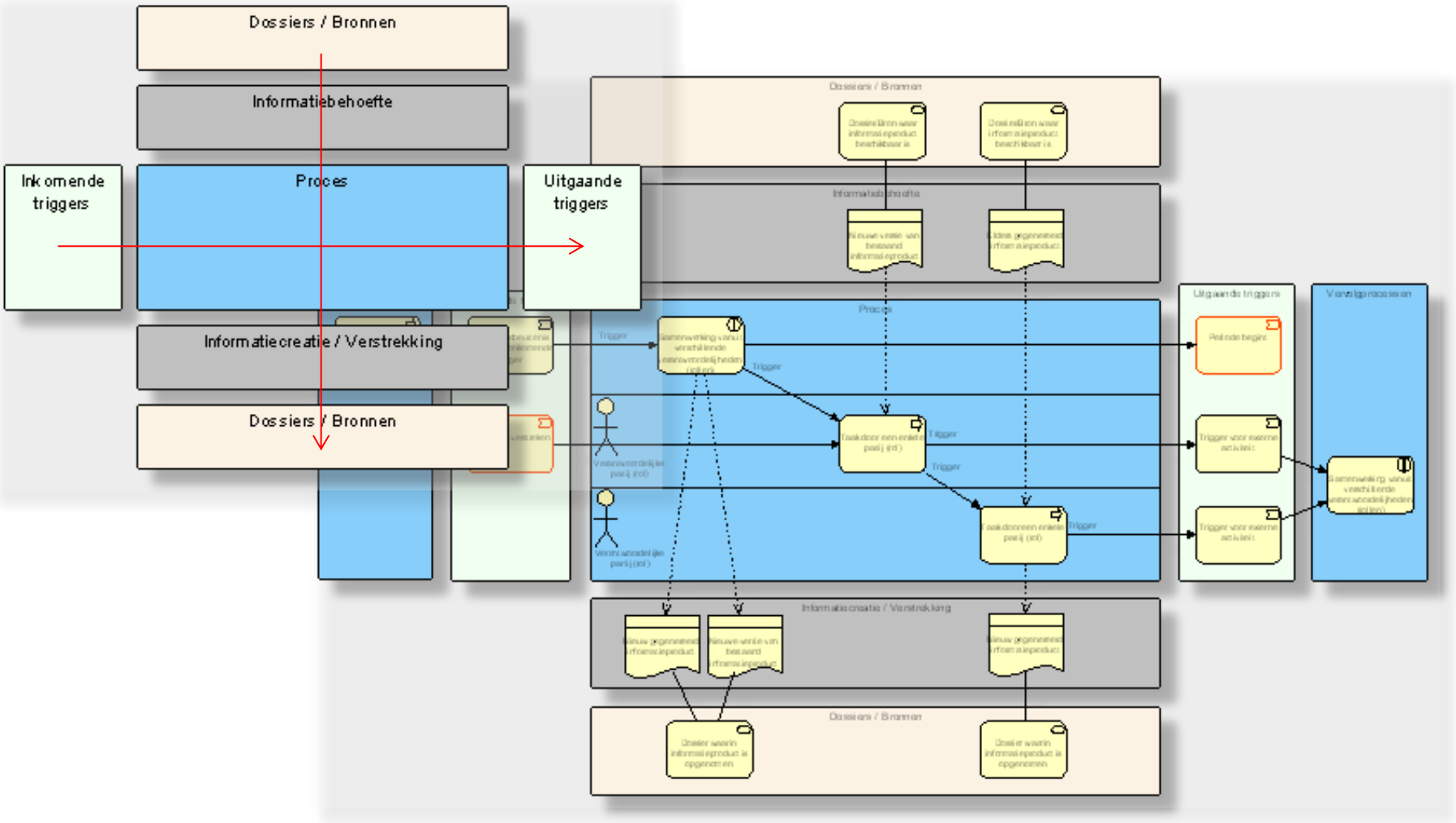
- ICT'ers/systeembeheerders

  → *kunnen input leveren over processen, systemen, informatiestromen en informatieproducten.*

Voorbeeld werkproces



Voorbeeld grondplaat



Stap 1b. Beschrijf de verstrekkingsmomenten

- Categorie + type persoonsgegevens;
- Voorgenomen gegevensverwerking;
- Verwerkingsdoeleinde (zo specifiek mogelijk);
- Betrokken partijen;
- Techniek van gegevensverwerking: geautomatiseerde; besluitvorming, profilering en big data;
- Juridisch en beleidsmatig kader;
- Bewaartermijnen.

LET OP! Bovenstaande lijst betreft geen uitputtende opsomming. Zie wet- en regelgeving, richtlijnen en organisatievoorschriften voor nadere kenmerken.

Voorbeeld

1

VOORBEELD

Vertrekking tussen partij 1 en partij 2 (mondeling)

Welke gegevens? (op basis van need to know)

- ID partij 1;
- Gebeurtenis/feit;
- Context (eerdere gebeurtenissen, persoonlijke omstandigheden).
- Etc.

UITWERKING VOORBEELD

Welke gegevens? (op basis van need to know)

- ID partij 1

  - NAW: noodzakelijk voor identificatie betrokkene en om beschikking naar betrokkene te kunnen toezenden;

  - Geboortedatum: niet noodzakelijk voor taakuitvoering;

  - E-mailadres: noodzakelijk voor communicatie met betrokkene;

  - Telefoonnummer: niet noodzakelijk voor taakuitvoering, communicatie geschiedt per e-mail.

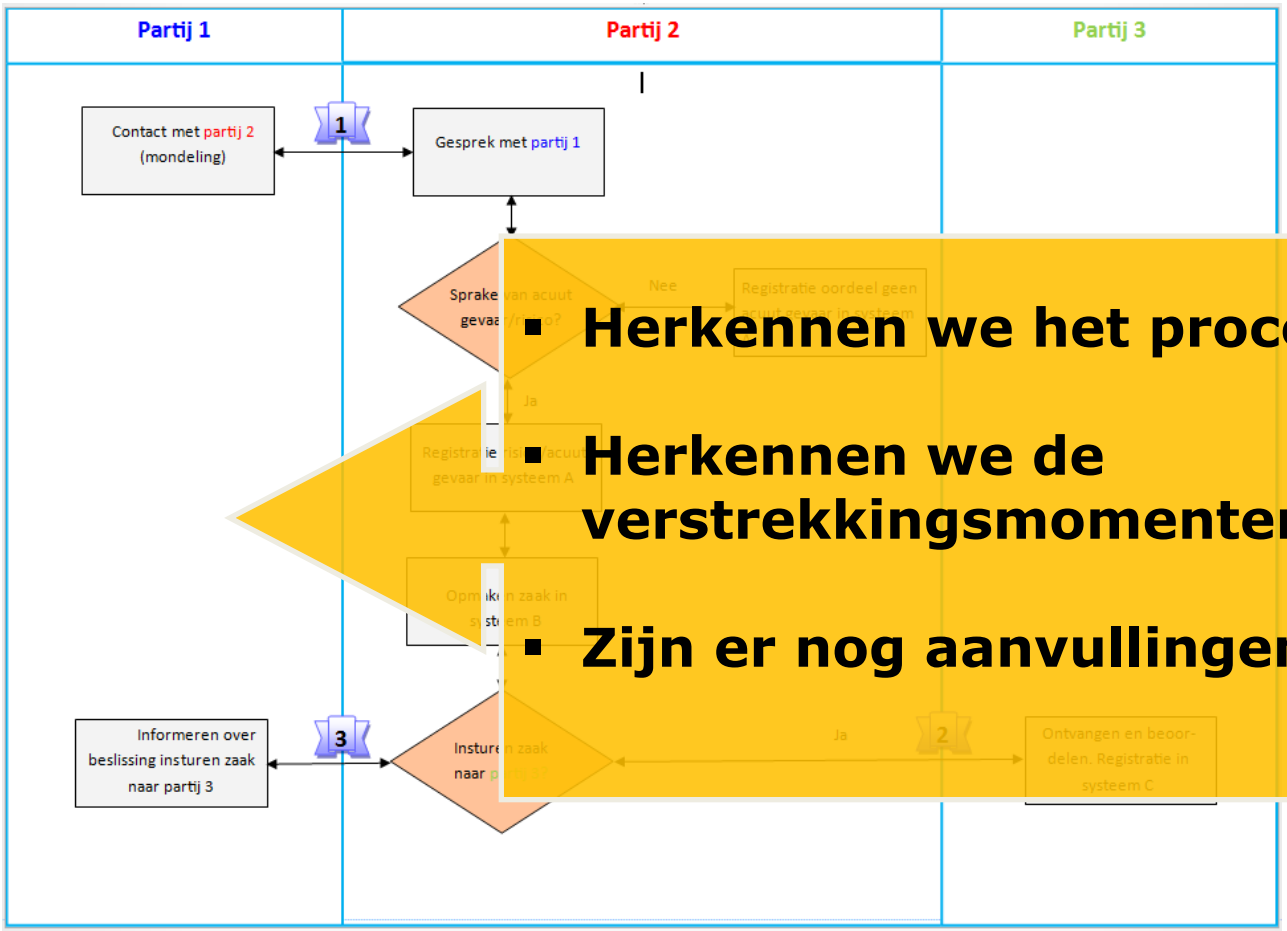
- Gebeurtenis/feit: betreffen geen persoons– maar zaaksgegevens;

- Context

  - Eerdere gebeurtenissen: betreffen geen persoons– maar zaaksgegevens;

  - Persoonlijke omstandigheden: welke persoonsgegevens zijn noodzakelijk voor een goede taakuitvoering? Welke persoonlijke omstandigheden er precies zijn, of kan worden volstaan met de kennis *dat* er persoonlijke omstandigheden zijn (op grond van dataminmalisatie/need to know)?

Stap 1c. Afsluiting en controle stap 1



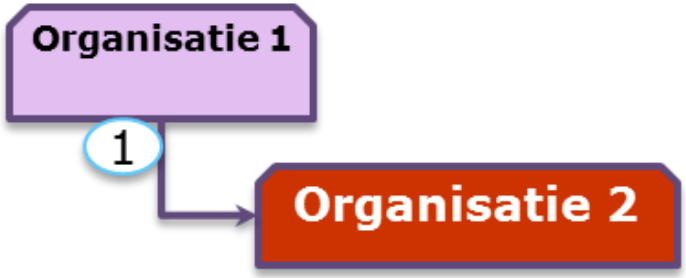
- **Herkennen we het proces?**
- **Herkennen we de verstrekkingsmomenten?**
- **Zijn er nog aanvullingen?**

Stap 2. Beoordeel per verstrekkingsmoment de randvoorwaarden voor het verstrekken

- Grondslag voor de verwerking;
- Bijzondere en strafrechtelijke persoonsgegevens;
- Doelbinding
- Noodzaak en evenredigheid
  - Kan het met minder gegevens (Proportionaliteit)
  - Kan het op een andere manier? (Subsidiariteit)

- Uitgangspunt:
  Taak- en vraaggebonden informatievoorziening

Voorbeeld



Organisatie 1 komt met een verzoek. Dit stelt organisatie 2 in staat om er een zaak van te maken.
Organisatie 1 verstrekt persoonsgegevens aan organisatie 2

A. Welke gegevens worden er verstrekt en waarom?

- Voornaam/achternaam/geboortedatum;
- Parketnummer;
- Delictsbeschrijving.

Waarom/met welk doel heeft de ontvanger de gegevensnodig?

- Voornaam/achternaam/geboortedatum: noodzakelijk voor identificatie/authenticatie betrokkene
- Parketnummer: noodzakelijk voor intern zaakvolgsysteem;
- Delictsbeschrijving: noodzakelijk voor een maatgericht aanpak.

B. Is er een grondslag? Aan welk artikelen kunnen we toetsen?

- Artikel 21 lid 3 Wbp: strafrechtelijke gegevens ten behoeve goede zorgverlening.
- Artikel 21 lid 1 onder d Wbp: persoonsgegevens betreffende de gezondheid;

Stap 3. Beschrijf en beoordeel risico's

- (On)rechtmatigheid v/d verwerking
  - Geen grondslag;
  - Geen doelbinding;
  - Inbreuk is disproportioneel en/of er zijn minder ingrijpende alternatieven voorhanden.

- Negatieve gevolgen van gegevensverwerking voor de rechten en vrijheid van betrokkenen
  - Risico's tav vertrouwelijkheid, beschikbaarheid en integriteit van de persoonsgegevens;
  - Kans dat gevolg zich voordoet zoals het in openbaarheid komen van persoonsgegevens;
  - Impact voor betrokkene als dit gebeurt.

Voorbeeld risicobeschrijving en -beoordeling

Bevindingen	Lichte impact	Gemiddelde impact	Zware impact
1) Gegevensuitwisseling 2) Wettelijke kader 3) Inbreuk rechten			
Risico's	**Laag**	**Midden**	**Hoog**
a. Rechtmatige grondslag b. Doelbinding c. Rechtmatigheid gegevens			
Mate beheersing risico's	**Laag**	**Midden**	**Hoog**
a. Rechtmatige grondslag b. Doelbinding c. Rechtmatigheid gegevens			

Stap 4. Beschrijf de voorgenomen maatregelen

Beschrijf per risico de voorgenomen technische, organisatorische en juridische maatregelen om de beschreven risico's in redelijkheid te voorkomen of te verminderen

Bijvoorbeeld:

- Pseudonimiseren (bv. Versleutelen) en anonimiseren persoonsgegevens;
- Dataminimalisatie;
- Beperken inzageniveau;
- Service level agreements / verwerkersovereenkomsten;
- Integriteitscontroles;
- Logging en monitoring.