Toelichting bij evaluatie ontwerpprotocol

versie 1

KADER VOOR DE EVALUATIE VAN EEN MEDEDELING OP BASIS VAN EEN ONTWERPPROTOCOL

Dit kader kan – zoals ook het formulier – later bijgeschaafd worden. Hergebruik daarom best geen oude versies. Dit is toelichting 1.0.1 bij formulier versie 1.0 .
Sommige aspecten werden voldoende uitgewerkt in het formulier van de VTC en worden hierna niet hernomen.

Met "de kaderwet" wordt de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (*B.S.*, 5 september 2018) bedoeld.

DEEL I TOETSING AAN BEGINSELEN - TOELICHTING

1. Verantwoordingsplicht

- Met het protocol moeten de verantwoordelijken kunnen aantonen dat de beginselen van de AVG worden nageleefd[1].

Zie FAQ "Hoe een mededeling van persoonsgegevens beoordelen"
De VTC heeft een model opgesteld dat de verantwoording door de verantwoordelijke en het advies van de functionaris en VTC vergemakkelijkt.

- Aanwezigheid van een voldoende actuele versie van het verwerkingsregister

- waar de verwerking van de bron in opgenomen is
- waar de verwerking zal in opgenomen worden door de ontvanger of al opgenomen is bij een wijziging

Het verwerkingsregister zal een grote hulp zijn voor het beantwoorden van diverse vragen.

Wetgeving:
- artikel 5, 2, AVG: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de beginselen vermeld in artikel 5, 1 en kan deze aantonen.
- artikel 30, AVG: elke verwerkingsverantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke moet een register bijhouden van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden
- artikel 8, e-govdecreet

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:

[1] Zie de verantwoording van het amendement dat de protocolregeling invoerde: "zodat duidelijk wordt dat aan de principes van de AVG wordt voldaan, zoals finaliteit, proportionaliteit, de rechtsbasis voor de verwerkingen, de veiligheidsmaatregelen, de periodiciteit, de duurtijd en andere concrete technische modaliteiten over de concrete gegevensuitwisselingen."

1° de identificatie van de verwerkingsverantwoordelijken;
De evaluatie van de beginselen zoals opgenomen in het protocol (na advisering).

2. Doelbinding

Wetgeving:
- artikel 5, 1, b), en 6, 4, AVG samen gelezen met de overweging 50, AVG:

- de verwerking van persoonsgegevens voor **andere doeleinden** dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel worden toegestaan **indien** de verwerking **verenigbaar** is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld. In dat geval is er geen andere afzonderlijke rechtsgrond vereist dan die op grond waarvan de verzameling van persoonsgegevens werd toegestaan.
- de verdere verwerking gebeurt door de verantwoordelijke die de gegevens meedeelt; de doorgifte is een vorm van verwerking; in hoofde van de ontvanger van de gegevens is er sprake van een onrechtstreekse verkrijging en een latere verwerking; de doeleinden van de verdere verwerking bij mededeling worden dus bepaald door de **doeleinden van de ontvanger** van de persoonsgegevens, die die zal moeten formuleren in het ontwerp van protocol;
- de verwerkingsverantwoordelijke moet, om na te gaan of een doel van verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld, nadat hij aan alle voorschriften inzake rechtmatigheid van de oorspronkelijke verwerking heeft voldaan, onder meer **rekening houden met**:
  - een eventuele koppeling tussen die doeleinden en de doeleinden van de voorgenomen verdere verwerking;
  - het kader waarin de gegevens zijn verzameld; met name de redelijke verwachtingen van de betrokkenen op basis van hun verhouding met de verwerkingsverantwoordelijke betreffende het verdere gebruik ervan;
  - de aard van de persoonsgegevens;
  - de gevolgen van de voorgenomen verdere verwerking voor de betrokkenen; en
  - passende waarborgen bij zowel de oorspronkelijke als de voorgenomen verdere verwerkingen.
- "Wanneer de betrokkene zijn **toestemming** heeft gegeven **of** wanneer de verwerking gebaseerd is op **Unierecht of lidstatelijk recht** dat in een democratische samenleving een noodzakelijke en evenredige maatregel vormt voor met name het waarborgen van belangrijke doelstellingen van algemeen belang, moet de verwerkingsverantwoordelijke de mogelijkheid hebben de persoonsgegevens verder te verwerken, ongeacht of dat verenigbaar is met de doeleinden."

- voor **archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden** geldt een uitzondering volgens artikel 5, 1, b), tweede zinsdeel AVG: deze verwerkingen worden niet als onverenigbaar beschouwd met de oorspronkelijke doeleinden. Voor deze verwerkingen is er een apart onderdeel opgenomen in DEEL 2 van het modelprotocol.

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
2° de doeleinden waarvoor de persoonsgegevens worden medegedeeld;
10° de beschrijving van de precieze doeleinden waarvoor de gegevens oorspronkelijk werden ingezameld door de instantie die beheerder is van de gevraagde gegevens;
11° ingeval van latere verwerking van de ingezamelde gegevens, vermelding van de verenigbaarheidsanalyse van de doeleinden van deze verwerking met het doeleinde waarvoor de gegevens aanvankelijk zijn verzameld overeenkomstig artikel 6, lid 4, van de algemene verordening gegevensbescherming;

Aandachtspunten

- zie de aandachtspunten onder punt 3 i.v.m. de wettelijke basis voor de verwerking.
- er moet in principe gekeken worden naar **het oorspronkelijke doel** van de gegevensverzameling bij de betrokkenen (en niet enkel naar de verwerking bij instantie waarbij men de gegevens wilt opvragen en waar al sprake kan zijn van een latere verwerking); mogelijk werden voor de eerste gegevensstromen nog geen machtigingen verleend of protocollen gesloten.
- in principe is de verwerking **verboden bij onverenigbaarheid**
- in de praktijk zullen vooral volgende elementen kunnen gebruikt worden:
    - de latere verwerking is gekaderd door voldoende precieze wettelijke en reglementaire bepalingen, of
    - kadert binnen redelijke verwachtingen betrokken persoon.
- de **uitzondering voor onderzoek**: dan worden de doeleinden als niet onverenigbaar beschouwd
De VTC is van oordeel in verband met wetenschappelijk onderzoek, dat ook al betreft het een onderzoek voor beleidsondersteuning, dat niet wegneemt dat het als wetenschappelijk onderzoek kan beschouwd worden. Adviezen van de opvolger van de Werkgroep 29, het Europees Comité voor gegevensbescherming (het Comité of The Board) kunnen dit verder verduidelijken.
- de verenigbaarheid is een **evolutieve beoordeling** (bv. steeds verdergaande digitalisering die de redelijke verwachtingen kan beïnvloeden).

3. Rechtmatigheid

Wetgeving:
- artikel 5, 1, a), AVG
- rechtmatigheid: artikel 6, AVG
Rechtmatigheid betreft de naleving van alle toepasselijke wettelijke en reglementaire bepalingen. Hier wordt evenwel gefocust op de bepalingen die specifiek van toepassing zijn op de bestaande en geplande verwerking. Zie ook onder punt 2 'Doelbinding'

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
5° de wettelijke basis van zowel de mededeling als de inzameling van de gegevens;

Aandachtspunten:
- de **oorspronkelijke verwerking** moet natuurlijk ook rechtmatig zijn: als de gegevens al niet mogen verzameld en verwerkt worden door de gevende partij, mogen ze natuurlijk ook niet aan een andere partij meegedeeld worden.
- een **ontwerptekst** wordt niet als voldoende beschouwd; als er toch een protocol tot stand komt dat verwijst naar toekomstige wet- of regelgeving - en op dit punt dan voorwaardelijk is - dan moet er voor de mededeling van de gegevens nog nagegaan worden of de goedgekeurde tekst al dan niet verschilt van de ontwerptekst op punten die van belang waren bij de beoordeling van de rechtmatigheid en doelbinding (dat moet dan als voorwaarde worden opgenomen in het protocol); dit is evenwel een af te raden praktijk.
- de **rechtsgrond voor de verwerkingen door overheden** is normaal gezien ofwel de vervulling van een taak van algemeen belang of het openbaar gezag ofwel de uitvoering van wettelijke verplichtingen.
- een wettelijke basis is meestal aanwezig voor wat betreft **de bevoegdheden** van de betrokken instanties (zoals bepaald in oprichtingsdecreten) en **de taken** waarvoor de persoonsgegevens worden verzameld of opgevraagd voor latere verwerking (sectorale wetgeving) omdat het overheden zijn.
- voor de concrete databank, toepassing, datawarehouse is er echter in bepaalde (belangrijke) gevallen een **specifieke wettelijke basis** aangewezen
- is de wettelijke verplichting **specifiek genoeg** in het licht van de AVG? Van de vroegere machtigingen van de sectorale comités van de CBPL en van de VTC en de beraadslagingen van het toekomstige Informatieveiligheidscomité (IVC) kan gezegd worden dat ze normatieve kracht hebben en minstens dat ze tegenstelbaar zijn aan derden (de betrokkenen). Dat is niet het geval bij een protocol. Een protocol omvat

louter afspraken tussen de betrokken partijen. Daardoor is een specifieke wettelijke grondslag voor de mededeling en/of de toekomstige verwerking nu belangrijker.
- bij het creëren van een wettelijke basis is het van belang om volgende **essentiële elementen** mee te nemen:
    - aanduiding verantwoordelijke voor de verwerking
    - doeleinde van de verwerking
    - welke categorieën persoonsgegevens
    - welke categorieën ontvangers (dat geeft de betrokkenen ook inzicht)
    - bewaartermijnen
- als **toestemming** als rechtsgrond wordt gebruikt, wat slechts zeer uitzonderlijk op zijn plaats zal zijn voor instanties, gaat het dan om een toestemming zoals bedoeld in de AVG? Artikel 4, 11), AVG, definieert toestemming van de betrokkene als volgt:": *elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt*;". Zie ook artikel 7 AVG i.v.m. de voorwaarden voor toestemming. De VTC wijst er op dat een toestemming die enkel wordt gegeven omdat men anders het recht op een premie, tegemoetkoming of subsidie zal verliezen niet beantwoordt aan het principe van een vrije toestemming. In de relaties met de overheid en arbeidsrelaties is er meestal sprake van een onevenwicht waardoor de "toestemming" niet vrij kan worden genoemd.
- **gerechtvaardigd belang** (artikel 6, f), AVG, kan niet ingeroepen worden door overheidsinstanties volgens artikel §, 1, laatste lid, AVG. Bij overheidsinstanties kunnen verwerkingen die dit als rechtsgrond zouden nodig hebben meestal gekaderd worden in het algemeen belang. Het werd dan ook niet in het formulier opgenomen omdat een protocol enkel verplicht is voor overheden. In de mate dat het formulier ook gebruikt wordt voor mededeling aan een organisatie die geen overheid is en gerechtvaardigd belang wordt ingeroepen, moet volgende afweging worden gemaakt: nagaan of de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. Dit moet dan gemotiveerd worden.

4. Behoorlijkheid en transparantie

Wetgeving:
- artikel 5, 1, a), AVG: beginsel;
- artikel 12 AVG bepaalt dat de verwerkingsverantwoordelijke passende maatregelen neemt opdat de betrokkene de in de artikelen 13 en 14 bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34 bedoelde communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt;
- artikel 13, 1, d) en 14, 1, d), AVG, bepaalt dat in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens moeten meegedeeld worden aan de betrokkenen wanneer persoonsgegevens bij de betrokkene worden verzameld;
- artikel 13, 3, en 14, 4, AVG: de verwerkingsverantwoordelijke verstrekt de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2;
- artikel 14, 3, AVG: de ontvangende verwerkingsverantwoordelijke verstrekt de bedoelde informatie:
    a) binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;
    b) indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of
    c) indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
- bekendmaking van het protocol zelf

Aandachtspunten:
Transparantie:
Uitzonderingen op transparantieplicht, maar de VTC is van oordeel dat in het kader van een behoorlijke verwerking een minimale transparantie, bv. via de geschikte webpagina's, aangewezen is.
Intussen is er meestal wel op een webpagina een vermelding van de gegevensstroom, maar
- dikwijls ontbreken een aantal verplichte punten
- dikwijls is de webpagina moeilijk te vinden
- dikwijls is de informatie niet bijgewerkt
- sommige instanties geven een heel korte samenvatting: dit is een aan te bevelen praktijk.

Behoorlijkheid:
Transparantie is een wijze om tot een behoorlijke verwerking te komen.
Ook het faciliteren van de betrokkenen bij de uitoefening van de rechten is een element dat bijdraagt tot een behoorlijke verwerking.
De VTC beveelt aan om daar een zekere uniformiteit voor te zoeken en suggereert om dit systematisch op te nemen in een (vlot vindbare) privacyverklaring.

5. Minimale gegevensverwerking

Wetgeving:
- artikel 5, 1, c), AVG
- artikel 4, 5), AVG: definitie van "pseudonimisering"
- artikel 25: beginselen gegevensbescherming door ontwerp en door standaardinstellingen* (o.a. pseudonimisering) zie overwegingen 28, 29 en 78, AVG.

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
- 3° de categorieën en omvang van de medegedeelde persoonsgegevens conform het proportionaliteitsbeginsel;

- 4° de categorieën van ontvangers en derden die mogelijks de gegevens eveneens verkrijgen;

- 7° de periodiciteit van de mededeling;

- 8° de duur van de mededeling;

Aandachtspunten:

Overweging 39, AVG legt de link met het principe van opslagbeperking.

De overweging verduidelijkt ook dat persoonsgegevens allen mogen worden verwerkt indien het doel van de verwerking niet redelijkerwijze op een andere wijze kan worden verwezenlijkt. Deze toets moet dus altijd gebeuren.

GEGEVENS:

- om de toets goed te doen moet gekeken worden naar de gegevens in de **vorm dat ze meegedeeld worden** door de gevende partijen (en niet hoe ze ontvangen worden – dat hoort bij de te nemen maatregelen)

- aard gegevens: gaat het om door of in opdracht van de gevende partij **gepseudonimiseerde** gegevens, dan moet verduidelijkt worden hoe dat gebeurt en beoordeeld worden of dat op een degelijke manier gebeurt

- als er sprake is van **anonieme gegevens**, klopt dat dan wel? soms worden gecodeerde gegevens ten onrechte geanonimiseerd genoemd. Bij anonimisering kan men achteraf de betrokkene niet meer terugvinden. Bij onderzoek waarbij gegevens gekoppeld worden is er dus nooit sprake van anonimisering voor er gekoppeld werd.

- de definitie van “persoonsgegevens” is **zeer ruim**, het zijn dus:

  - meer dan identificatoren (naam, adres, RRnr,…)

  - niet beperkt tot privacy/persoonlijke levenssfeer

- **een lijst met enkel identificatoren** bevat meestal meer informatie door de context bv. de namen van leerlingen die regelmatig afwezig zijn, het rijksregisternummer van huurders van een sociale woning; de persoonsgegeven zijn dan “leerling zijn”,“ regelmatig afwezig zijn”, “huurder zijn van een sociale woning”.

- **open velden** bannen of er sluitende criteria voor bepalen

- opletten met **toegevoegde documenten** (bv. pdf met foto’s waar dan een hoop informatie over de persoon uit blijkt!)

- **niet meer dan nodig?**

  bv. voor een studie: geboortedatum of is een range voldoende

  bv. voor een studie: mag er geen ruis zitten op de (locatie)data

  bv. als RRnr waarom nog de andere identificatiegegevens

- samenhangend: het **formaat van de data** is van belang: dat een formaat van het type "ja of neen" of "aantal personen waaruit het gezin bestaat" of nog "inkomstenniveau hoger of lager dan een bepaald bedrag" kan in sommige gevallen ruimschoots volstaan. (cf. noot in advies CBPL over kaderwet)

- proportionaliteit is ook afhankelijk van de **administratieve vereenvoudiging** die gerealiseerd wordt.

DUUR MEDEDELING:

- dit is de periode waarin de gegevens zullen meegedeeld worden (is niet hetzelfde als de bewaartermijn)
Voorbeelden: voor één jaar, voor onbepaalde duur.

- Gekoppeld aan het wettelijk doel
  bv. taalbereidheidsvoorwaarde bij sociale huisvesting
- Gekoppeld aan uitvoering van een overeenkomst
  bv. duur opdracht voor een steunpunt of een studie
- Beperkte termijn bij een eenmalige gegevensoverdracht

- voorzie een voldoende lange maar redelijke termijn zodat er geen verlengingen nodig zijn bij vertraging bij het project.

PERIODICITEIT VAN DE MEDEDELING:

Dit kan eenmalig zijn (voor grote bestanden anders is er geen sprake van een systematische mededeling) of periodiek of permanent. Dit geeft eerder een beeld van de gegevensstroom dan dat hier op ingegrepen moet worden maar zal anderzijds de te nemen maatregelen wel mee bepalen.

BESTEMMELINGEN:
- er moet voor gezorgd worden dat de toegang tot de gegevens beperkt wordt voor de taken en het werkgebied waar iedere betrokkene voor bevoegd is.
- vermijden dat iedereen van een bevoegde dienst de gegevens ziet. Zo is meestal niet nodig dat de leidinggevenden ook de persoonsgegevens moeten kennen. (*_privacy by design_* en *_privacy by default_*).
- de derden waarnaar verwezen wordt, zijn personen die niet vervat zitten in het protocol; dit is dus een controlevraag die kan leiden tot een apart protocol (of een andere regeling voor doorgifte)

6. Opslagbeperking

Wetgeving:
- artikel 5, 1, e), AVG voorziet dat persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.
- overweging 39, AVG, stelt dat ervoor moet worden gezorgd dat de opslagperiode van de persoonsgegevens tot een strikt minimum wordt beperkt. De overweging verduidelijkt dat om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, de verwerkingsverantwoordelijke termijnen dient vast te stellen voor het wissen van gegevens of voor een periodieke toetsing ervan.

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
- ontbreken in de opsomming van artikel 8 e-govdecreet
- zouden wel in model protocol AIV komen

Aandachtspunten:
Onbeperkt duur is niet aanvaardbaar.
Lange duur zeer uitzonderlijk aanvaardbaar. Systematisch inperken is nodig.
Longitudinaal onderzoek:

- Anonimiseren kan niet (wel pseudonimiseren) en lange bewaartermijn
- Gevaar “oneigenlijk gebruik” van voor andere studies gebruikte datasets (mag niet)
- toch beperken in de tijd (een paar legislaturen bv.)

Onderscheid maken tussen de verschillende (clusters van) gegevens.
Effectieve vernietiging gevraagd, maar gerealiseerd?
Relatie met **archiefwetgeving** : onderscheid actief en passief klassement, dat laatste uitzonderlijk als alternatief voor vernietiging mits de vereiste veiligheidsmaatregelen.

7. Juistheid

Wetgeving:

- artikel 5, 1, d), AVG: beginsel: persoonsgegevens moeten AVG juist zijn en zo nodig worden geactualiseerd.
- overweging 39, AVG, stelt dat alle redelijke maatregelen moeten worden genomen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd of gewist.
- artikel 16, AVG geeft de betrokkene een recht op rectificatie van onjuiste persoonsgegevens
- artikel 18, AVG: geeft een recht op beperking van de verwerking als de juistheid wordt betwist.

Gegevens van het art. 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
- 12° afspraken omtrent de garantie van de kwaliteit van de gegevens (en in voorkomend geval de eerbiediging van het wettelijk kader dat de toegang tot de authentieke gegevensbron regelt – zie DEEL 2);

Aandachtspunten:
Voorbeelden: zie machtiging VTC/35/2018.
http://vtc.corve.be/docs/beraadslagingen/VTC_beraadslaging_2018_35.pdf
Voor wat het faciliteren van de rechten van de betrokken betreft, zie onder behoorlijkheid en transparantie.

8. Risicobenadering

Wetgeving:
- artikel 24, AVG i.v.m. de verantwoordelijkheid van de verwerkingsverantwoordelijke
- artikel 25, AVG i.v.m. gegevensbescherming door ontwerp en door standaardbepalingen
- artikel 26, AVG i.v.m. de beveiliging van de verwerking
Artikel 35, AVG m.b.t. de gegevensbeschermingseffectbeoordeling (GEB of DPIA).
Artikel 33, AVG i.v.m. de melding van inbreuken i.v;m. persoonsgegevens.
- overweging 75, 76 en 83, AVG (ondermeer)

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
- 6° de beveiligingsmaatregelen van de mededeling, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen;

Aandachtspunten:
- het gaat **niet om het bedrijfsrisico's**, maar om het risico's voor de rechten en vrijheden van de betrokkenen (zie de vermelde overwegingen).
- een eerste stap is de **informatieclassificatie**.
- een **risicoassessment** doen zoals de cloudevaluatiemodel van Smals, waardoor het risico zeer inzichtelijk wordt voorgesteld. De GBA is aan het werken aan een evaluatiemodel hierop geïnspireerd.
- controle of er een **GEB/*DPIA*** moe(s)t opgemaakt worden. Zie hiervoor de Richtsnoeren van de Groep Gegevensbescherming Artikel 29 (*Working Party 29* of WP29) nr. WP248 rev.01voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679.
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
en de aanbeveling nr. 01/2018 van 28 februari 2018van de CBPL: Aanbeveling uit eigen beweging met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging (CO-AR-2018-001)

https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2018.pdf
Zo ja, DPIA bekijken.
- de te nemen **maatregelen** (en de beslissing of de gegevens kunnen doorgegeven worden) hangen af van de gedane risicobeoordelingen. In het kader van de verantwoordingsplicht moeten de risicobeoordelingen **gedocumenteerd** zijn: er moet een argumentatie zijn dat de gekozen manier van werken veilig is.

9. Integriteits- en vertrouwelijkheidsbeginsel

- Maatregelen i.v.m. de specifieke gegevensoverdracht.
- Maatregelen op het niveau van de organisatie van de bron en vooral van de ontvanger.

Wetgeving:
- artikel 5, 1, f), AVG
- artikel 24, AVG):
  -de maatregelen moeten kunnen waarborgen en aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd
  - de evaluatie en indien nodig actualisatie van de maatregelen.
- artikel 32, AVG
- artikel 33 en 34 AVG

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
- 6° de beveiligingsmaatregelen van de mededeling, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen;
- 13° specifieke maatregelen die de gegevensmededeling omkaderen zoals
  - formaat van de mededeling: […]
  - logging van de toegangen zodat men kan controleren wie wanneertoegang had tot welke gegevens en waarom
  - invoering van een verwijzingsrepertorium in het geval van automatische mededeling van de wijzigingen aan de gegevens
  - bij e-mailen of andere eenmalige digitale overdracht van de gegevens: het bestand met de geëncrypteerde data zal via een digitaal kanaal worden bezorgd. Het paswoord voor het decrypteren van de bestanden wordt via een ander kanaal meegedeeld en uitsluitend aan de aangewezen contactpersonen.

Aandachtspunten:
- hoe is de **geheimhoudingsplicht** geregeld van de personen bij de ontvangende partijen die toegang zullen hebben tot de persoonsgegevens?
- er moet voor gezorgd worden dat de **beheerder van de infrastructuur** geen toegang heeft tot de data zelf tenzij strikt noodzakelijk.
tenzij strikt noodzakelijk.
- **basisvragen i.v.m. informatieveiligheid**:

- is er een informatieveiligheidsbeleid (engagement, high level)?
- is er een informatieveiligheidsplan (met termijnen en middelen)?
- is er een procedure om een inbreuk i.v.m. persoonsgegevens te melden?
- is er een robuuste encryptie voorzien?
- wordt er degelijk gelogd?
- zie vragenlijst met andere basisvragen.

Deze vragen zijn een essentie van de richtsnoeren informatieveiligheid (gebaseerd op de toepasselijke ISOnormen) en deze zijn nog altijd geldig
https://www.gegevensbeschermingsautoriteit.be/node/17453
http://vtc.corve.be/infoveiligheid.php

- de vereiste maatregelen moeten genomen zijn **voor de eerste mededeling** van de gegevens.
- louter doorverwijzen naar de verwerker volstaat niet, **de verantwoordelijke moet het zelf** kunnen antwoorden in het protocol (op basis van de informatie die de verwerker verstrekt)
- **encryptie**:
  - met robuust wordt bedoeld dat het zowel brute kracht als de tand des tijds moet kunnen doorstaan (sommige algoritmes blijken na verloop van tijd niet stevig genoeg).
  - SFTP zorgt enkel voor een beveiliging van de data (ook door encryptie) in transport tot op de ontvangende server. Als er encryptie wordt gevraagd in het kader van medeling van persoonsgegevens, wordt er meer bedoeld dan een beveiligd transport (*end-to-end* encryptie). Documenten moeten ook geëncrypteerd worden voor en na de verzending.
  - Zie ook het advies het VTC/A/02/2018, inzake de encryptiebouwsteen van het Facilitair Bedrijf voor het hosting door Amazon Web Services, waarbij de nadruk wordt gelegd op dynamische encryptie:
  http://vtc.corve.be/docs/adviezen/VTC_A_2018_02_encryptie_FB_AWS.pdf
- **melding inbreuken**: er moet ook de afspraak zijn dat de entiteiten elkaar informeren wanneer men denkt dat er een gegevenslek plaatsvond.

- het is de VTC nog niet duidelijk wat met “het formaat van de mededeling” in art. 8, §1, 2e lid, 13°, e-govdecreet wordt bedoeld (voor formaat van de gegevens, zie onder “minimale gegevensverwerking”, mogelijk gaat het om de wijze van mededeling (het medium, de drager).

DEEL 2 BIJZONDERE GEVALLEN

De onderdelen van DEEL 2 moeten slechts ingevuld worden als er eenverband is met de mededeling en de geplande verwerking door de ontvangende partijen.

10. Verwerkers

Wetgeving:
Artikel 4, 7), AVG: definitie van “verwerkingsverantwoordelijke”.
Artikel 4, 8), AVG: definitie van “verwerker”.
Artikel 28, 1, AVG bepaalt dat wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, de verwerkingsverantwoordelijke uitsluitend een beroep doet op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

Advies CBPL uit eigen beweging nr. 10/2016 van 24 februari 2016 over de gebruikmaking van cloudcomputing door de verantwoordelijke voor de verwerking (CO-A-2015-013).
Advies CBPL m.b.t. nr. 09/2016 van 24 februari 2016 de keuze voor een SaaS-HR-strategie bij talentmanagementprocessen van de Vlaamse Overheid (CO-A 2016-006).
Aanbeveling VTC nr. 01/2016 van 12 oktober 2016 betreffende het beheer van persoonsgegevens in een datacenter door een niet-Europese firma.
http://vtc.corve.be/docs/adviezen/VTC_AB_2016_01_aanbeveling_outsourcing_datacenter_def_vrpubl.pdf

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
- ontbreken

Aandachtspunten:

Het betreft niet alleen de verwerkers die voor de doorgifte van de gegevens ingeschakeld worden, maar ook die die instaan voor de geplande verwerking bij de ontvangende partijen. I bepaalde gevallen kunnen de verwerkers van de gevende partijen ook relevant zijn.

De verwerkers zijn meestal IT-firma's, maar het kunnen ook andere dienstverleners zijn. De dienst moet wel betrekking hebben op het verwerken van persoonsgegevens.

Een instantie kan ook een verwerker zijn voor een andere instantie (en op haar beurt met een onderaannemer werken).

Bij wetenschappelijk onderzoek zijn er verschillende hoedanigheden mogelijk:

- als de studie louter in opdracht van een instantie gebeurt is er een verwerkersrelatie (en moet een verwerkingsovereenkomst worden gemaakt i.p.v. een protocol)

- komt het initiatief van de onderzoeksinstantie zelf, dan is er een mededeling van de ene verantwoordelijke aan de andere (protocolregeling)

Op basis van vroegere wetgeving (KB ter uitvoering van de WVP) werd een verwerker die de gegevens afkomstig van verschillende bronnen koppelde zelf ook als een verantwoordelijke gezien.

Ook alle onderaannemers moeten worden beoordeeld bv. back-up in publieke cloud.

Er moet voor gezorgd worden dat de beheerder van de infrastructuur geen toegang heeft tot de data zelf tenzij strikt noodzakelijk.

Zie de hiervoor geciteerde aanbevelingen.

11. Intermediair en dienstenintegrator

Wetgeving:

Decreet van 13 juli 2012 houdende de oprichting en organisatie van een Vlaamse dienstenintegrator.
Wet van 15 januari 1990 houdende oprichting en organisatie van een kruispuntbank van de sociale zekerheid.
Wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen.

Artikel 202 en 203 van de kaderwet (over de derde vertrouwenspersoon of TTP).

Aanbeveling CBPL nr. 02/2010 van 31 maart 2010 omtrent de privacybeschermende rol van *Trusted Third Parties* (TTP) bij gegevensuitwisseling (A/09/022).
Aanbeveling CBPL uit eigen beweging nr. 03/2009 van 1 juli 2009 in verband met integratoren in de overheidssector (A/2007/043).

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:

13° specifieke maatregelen die de gegevensmededeling omkaderen […]

Aandachtspunten:

Als filtering of codering vereist is in het kader van minimale gegevensverwerking/proportionaliteit wordt vaak een beroep gedaan op een externe partij. Deze moet aangesteld zijn door de instantie die de gegevens meedeelt.

Het is belangrijk dat de vraag naar een intermediair of dienstenintegrator altijd gesteld wordt.

Het aanduiden van een intermediair of dienstenintegrator is niet altijd verplicht.

In het kader van anonimisering of pseudonimisering van de gegevens verwerkt met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden worden door de kaderwet wel regels opgelegd inzake het beroep doen op een “derde vertrouwenspersoon” (artikel 202 en 203).

Uitzonderlijk is het een decretale verplichting zoals bij de ontsluiting van Leer- en ervaringsbewijzen databank (LED).

Wat betreft de sociale sector treedt de KSZ op als dienstenintegrator. Instellingen van sociale zekerheid zijn verplicht beroep te doen op KSZ. Instellingen die geen instellingen van sociale zekerheid zijn, kunnen wel van de diensten gebruik maken. (EHealth is geen dienstenintegrator, maar stelt basisdiensten ter beschikking. Het gebruik van eHealth is niet verplicht.)

Contacteer tijdig de intermediair/dienstenintegrator.

De rol van de intermediair/dienstenintegrator wordt bij voorkeur ook in het schema vermeld op de eerste pagina van dit formulier of in een apart schema weergegeven.

12. Gebruik rijksregisternummer

Wetgeving:

Artikel 87, AVG dat ook voor andere identificatoren van algemene aard geldt.

Wachten op inwerkingtreding aanpassingen federale regelgeving om deze toelichting meer uit te werken.

Artikel 8 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, zoals gewijzigd door artikel 14 van de wet van [.....] houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters.

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
- 3° de categorieën en omvang van de medegedeelde persoonsgegevens conform het proportionaliteitsbeginsel;

Aandachtspunten:

Het rijksregisternummer is een zeer belangrijke sleutel om persoonsgegevens te koppelen.

Het rijksregisternummer bevat in de meeste gevallen ook de geboortedatum en het geslacht van de betrokkene.

Een lijst met (louter) rijksregisternummers (of een andere algemene identificator) is meer dan een lijst met nummers: de personen verbonden met die nummers hebben een kenmerk dat een persoonsgegeven is bv. een lijst met rijksregisternummers van studenten of inburgeraars houdt minstens de persoonsgegevens “is student” of “is inburgeraar” in. Deze gegevens moeten vermeld worden bij het overzicht van de gegevens en maken dat de procedures voor mededelingen moeten gevolgd worden.

De VTC kan het gebruik van het rijksregisternummer als sleutel niet meer mee machtigen aangezien ze geen machtigingen meer kan verlenen. In principe (er bestaan uitzonderingen) zal voor het gebruik van het rijksregisternummer een machtiging moeten worden gevraagd aan de (federale) minister bevoegd voor Binnenlandse Zaken. Als er reeds machtigingen bestaan, zal (in principe) het gebruik als sleutel bij de mededeling als een nieuwe netwerkverbinding ter goedkeuring aan dezelfde minister moeten worden voorgelegd. De minister kan delegeren aan de Algemene Directie Instellingen en Bevolking van de FOD Binnenlandse Zaken.

Het formulier voor de aanvraag van de machtiging vindt u hier:
http://www.ibz.rrn.fgov.be/nl/rijksregister/aanvraag-toegang-tot-het-rijksregister/

13. Toegang tot authentieke gegevensbronnen

Wetgeving:

De specifieke wetgeving m.b.t. deze gegevensbronnen moet worden toegepast, bv. inzake het Rijksregister of de LED.

Gegevens van artikel 8, §1, 2e lid, e-govdecreet die van belang zijn bij beoordeling:
- 12° (afspraken omtrent de garantie van de kwaliteit van de gegevens zie DEEL I -en) in voorkomend geval de eerbiediging van het wettelijk kader dat de toegang tot de authentieke gegevensbron regelt;

Aandachtspunten:

14. Verwerking van bijzondere categorieën van persoonsgegevens

Wetgeving:

Artikel 9, AVG:
Verwerking is verboden tenzij een van volgende wettelijke grondslagen voor gegevensverwerking:

- uitdrukkelijke toestemming van de betrokkene

- verplichtingen van arbeidsrecht, socialezekerheidsrecht of sociale beschermingsrecht
    - gebeurt de verwerking door of onder de verantwoordelijkheid van een beroepsbeoefenaar?
        - Ja -> welke
        - Nee

- ter bescherming van vitale belangen van een betrokkene of een persoon die niet in staat is om zijn toestemming te geven
- de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is
- de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
- in verband met een rechtsvordering of in het kader van de rechtsbevoegdheid van het gerecht
- redenen van algemeen belang
- doeleinden van preventieve of arbeidsgeneeskunde
- redenen van algemeen belang op het gebied van de volksgezondheid
- wetenschappelijk of historisch onderzoek of statistische doeleinden
    - Advies noodzakelijk van een ethisch comité?
        - Ja -> bijvoegen
        - Nee

Artikel 9 van de kaderwet: te nemen maatregelen voor wat de personen die toegang krijgen tot de persoonsgegevens bij de verwerking van genetische, biometrische of gezondheidsgegevens (uitvoering van artikel 9, 4, AVG).

Aandachtspunten:
De definitie van gegeven over gezondheid is ruimer geworden t.o.v. de WVP (privacywet).
Uit aansluiting bij een mutualiteit kan een politieke opvatting worden afgeleid.
Uit een schoolkeuze kan in bepaalde gevallen een religieuze of levensbeschouwelijke overtuiging worden afgeleid.
Gezinstaal en nationaliteit zijn op zich geen bijzondere categorieën van persoonsgegevens, maar de VTC beschouwt ze wel als bijzonder beschermingswaardige gegevens. Dit sluit aan bij wat de WP29 in haar richtsnoeren voor de DPIA (WP248) “gevoelige gegevens of gegevens van zeer persoonlijke aard” noemt, die buiten de in artikel 9 en 10, AVG ook andere data kunnen bevatten.
De geheimhoudingsverplichtingen werden reeds opgenomen in DEEL 1 voor het vertrouwelijkheidsbeginsel.

15. Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten

Zie modelprotocol.

Wetgeving:

Artikel 10, AVG
Artikel 10 van de kaderwet: te nemen maatregelen voor wat de personen die toegang krijgen tot de persoonsgegevens bij de verwerking van genetische, biometrische of gezondheidsgegevens (uitvoering van artikel 10, AVG).

Aandachtspunten:

De geheimhoudingsverplichtingen werden reeds opgenomen in DEEL 1 voor het vertrouwelijkheidsbeginsel.

16. Bij archivering en wetenschappelijk onderzoek

Het betreft verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden bedoeld in artikel 89, AVG.
Zie formulier VTC voor protocol.

Wetgeving:

Art. 5, lid 1, b) AVG
Art. 89 AVG
Titel 4 van de kaderwet bepaalt het uitzonderingsregime voor wat betreft de rechten van de betrokkenen voor deze verwerkingen. In het kader van mededelingen van persoonsgegevens zijn vooral volgende bepalingen relevant:
- artikel 201, 202, 203
- artikel 194: opgepast, deze federale regel heeft geen voorrang op de decretale protocolregeling: beide regelingen gelden naast elkaar. Het protocol kan (waarschijnlijk) wel beschouwd worden als de overeenkomst waarvan sprake is in de kaderwet. De uitzonderingen bepaald in de kaderwet gelden niet voor de decretale protocolregeling.

Aandachtspunten:

De verantwoordelijke moet **alle mogelijke middelen** inzetten om te vermijden dat de identiteit van de personen op wie de meegedeelde gegevens betrekking hebben, zou worden achterhaald. Het indelen in klassen of het weglaten van de variabelen die het grootste risico op heridentificatie inhouden, wordt beschouwd als een adequaat middel (uit machtigingen). Het toevoegen van “ruis” is ook een mogelijkheid.
Als onderzoekers niet anders kunnen dan op niet gepseudonimiseerde data werken (bv. omdat exacte adresgegevens nodig zijn om afstanden te berekenen) dan kan gewerkt worden volgens het ***safe room*** principe. Door het werken volgens het “safe room” principe , waarbij de ruimte en de middelen de mogelijkheid om de data mee te nemen uitsluiten, krijgt de onderzoeker toegang tot de gegevens, maar kan die enkel geanonimiseerde data meenemen. De *safe room* kan ingericht worden bij de mededelende partij of bij de TTP (*trusted third party* of derde vertrouwenspersoon). De Vlaamse Dienstenintegrator heeft een werkwijze uitgewerkt gelijkaardig aan deze opgelegd door Eurostat aan onderzoekers die de Community Innovation Survey microdata wensen te gebruiken voor een goedgekeurd onderzoek in het Eurostat Safe Center. Artikel 207 van de kaderwet verwijst ook naar dit principe.

17. Doorgiften aan derde landen en internationale organisaties

Zie formulier VTC voor protocol.

Wetgeving:

Artikel 44 e.v., AVG
Artikel 48, AVG.
Rekening houden met arrest Hof van Justitie in de zaak Schrems.

Aandachtspunten:

Het gaat meestal om de verwerker.

DEEL 3 AANVULLENDE OPMERKINGEN

Er kan voor de specifieke mededeling nog andere regels gelden.

Hier kunnen ook algemene opmerkingen worden opgenomen.

DEEL 4 BIJLAGEN

Duidt aan welke bijlagen worden toegevoegd.

Standaard wordt de bijlage inzake informatieveiligheid toegevoegd.

De bijlagen moeten niet mee gepubliceerd worden tenzij ze de opsomming van de categorieën van persoonsgegevens betreffen (of andere essentiële elementen).

DEEL 5 BESLUIT

18. Voorwaarden

Zie formulier VTC voor protocol.

De meldingsplichten zoals voorgesteld door de juridische werkgroep AVG van het stuurorgaan Vlaams Informatie- en ICT-beleid (sjabloon versie 20180718) kunnen hier opgenomen worden:

"*Partijen engageren zich in het licht van artikel 33 van de algemene verordening gegevensbescherming om elkaar [via de functionarissen voor gegevensbescherming] zonder onredelijke vertraging op de hoogte te stellen van elk gegevenslek dat zich voordoet betreffende de meegedeelde gegevens met impact op beide partijen en in voorkomend geval onmiddellijk gezamenlijk te overleggen teneinde alle maatregelen te nemen om de gevolgen van het gegevenslek te beperken en te herstellen. De partijen verschaffen elkaar alle informatie die ze nuttig of nodig achten om de beveiligingsmaatregelen te optimaliseren.*"

"*De ontvangende partij brengt mededelende partij onmiddellijk op de hoogte van wijzigingen van wetgeving met impact op voorliggend protocol, zoals de finaliteit, proportionaliteit, frequentie, duurtijd enz. en in voorkomend geval van wijzigingen omtrent de verwerkers*."

19. Sancties

Op zich is dit enkel een zaak tussen de betrokken partijen.

Een mogelijke en logische sanctie zou zijn dat de mededeling van de persoonsgegevens wordt gestopt als niet of niet meer aan de voorwaarden van dit protocol wordt voldaan. Dit gebeurt dan aanmaning en het bieden van een redelijke termijn om de mededeling conform te maken tenzij het risico voor de betrokkenen te groot is.

20. Handtekeningen

Zorg ervoor dat bij digitale handtekening minstens bij publicatie van het protocol het rijksregisternummer niet zichtbaar is.