De privacytoets als leidraad in de wisselwerking tussen DPO en EC post GDPR

Griet Verhenneman, VLIR – GDPR en het onderzoeksbeleid, Brussel, 6 November 2019

UZ Leuven | Herestraat 49 B - 3000 Leuven | www.uzleuven.be tel. +32 16 33 22 11 | UNIVERSITY HOSPITALS LEUVEN

Medisch Ethische Commissie UZ Leuven

- Erkende Ethische Commissie Onderzoek UZ/KULeuven
  - onderzoeksprojecten aangaande medisch-wetenschappelijke en gezondheidszorg gerelateerde onderwerpen (klinisch onderzoek)
  - 24 leden
  - Net geen 1300 adviezen + net geen 1200 amendementen in 2018

Functie DP

- Informeren en adviseren
- Toezicht op de naleving [illegible] wel beleidsmatig als in dagelijkse werking
- Advies verstrekken m.b.t. [illegible] ezien op de naleving ervan
- Contactpersoon voor d[illegible]

Kortom… awarene[illegible]DPR creëren, GDPR-compliance trachten te bereiken en je organisatie inspireren…

óók in de uitvoering van wetenschappelijk onderzoek.

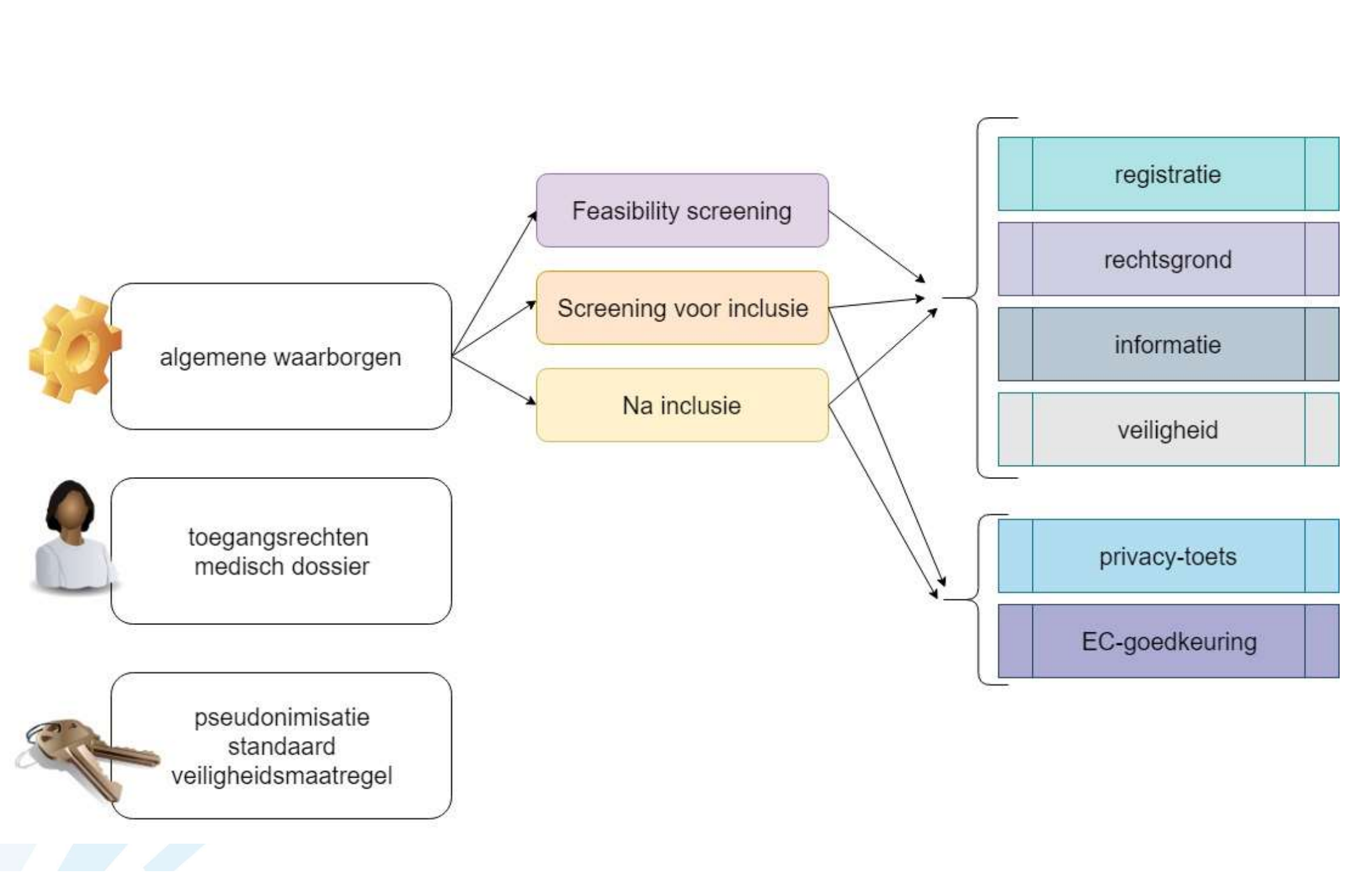
Medisch ethische commissie

(Medisch) ethische commissie is *niet* verankerd in GDPR.

EC en DPO wel deels dezelfde bezorgdheid

=> vinden elkaar in verplichting

“privacy-toets”


algemene waarborgen
toegangsrechten
medisch dossier
pseudonimisatie
standaard
veiligheidsmaatregel
Feasibility screening
Screening voor inclusie
Na inclusie
registratie
rechtsgrond
informatie
veiligheid
privacy-toets
EC-goedkeuring

Privacytoets

Wanneer vereist?

als gezondheidsgegevens worden verwerkt, privacytoets altijd verplicht onderdeel van EC goedkeuring.

→ Onafhankelijk van rol van het ziekenhuis
(controller / processor – sponsor / site)

→ Onafhankelijk van type studie
(grote klinische studie, klein onderzoeksproject, PhD thesis, Masterproef,…)

→ Onafhankelijk van type wetenschappelijk onderzoek
(prospectief / retrospectief, interventioneel / observationeel)

- In 2018 EC UZ/KULeuven 500+ studies die onder WEPM vallen,
  700+ studies die niet onder WEMP vallen.

Privacytoets

Wie beoordeelt de privacytoets?

Semiautomatisch, maar vooral een kwestie van samenwerking

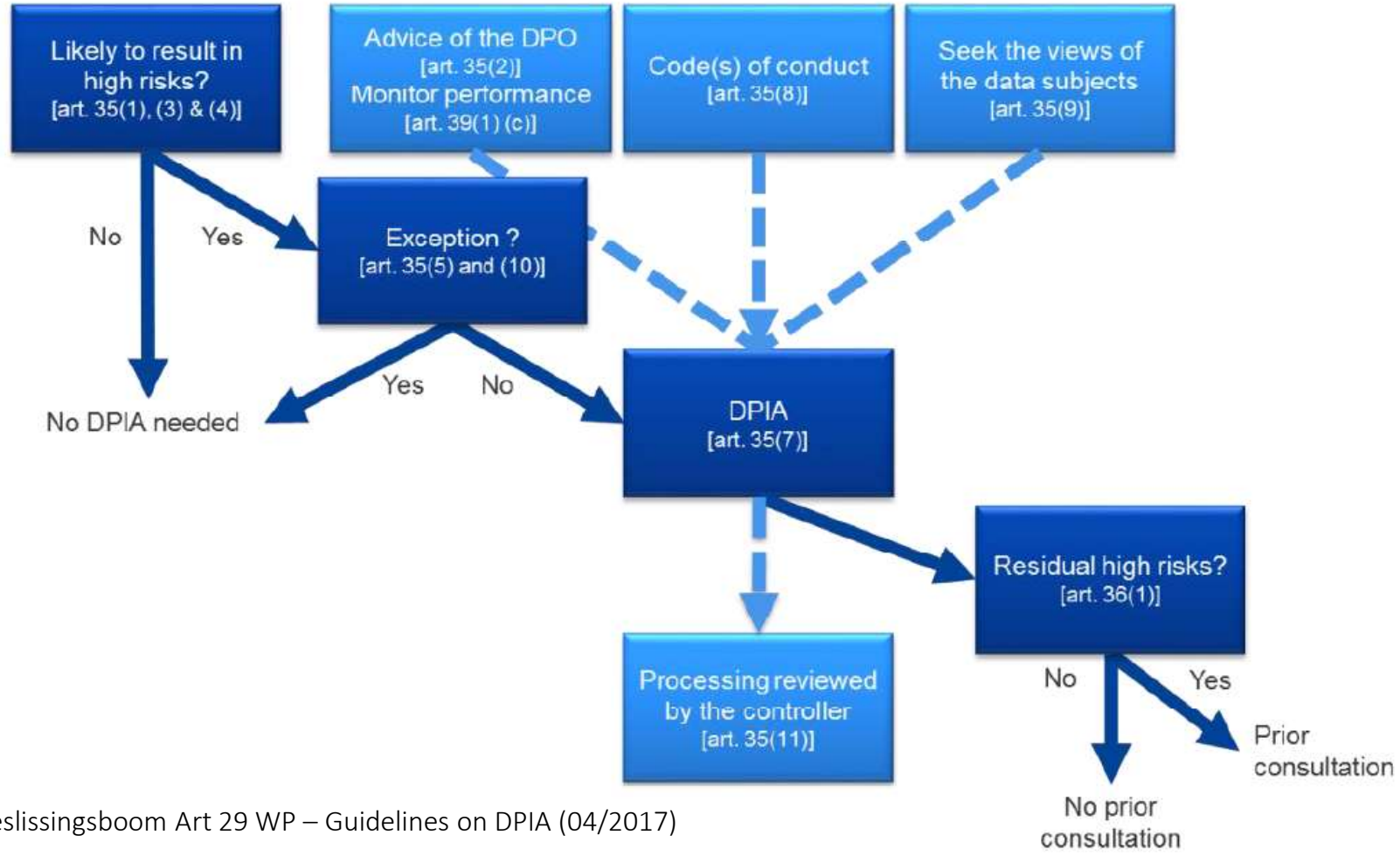
- Bepaalde antwoorden op bepaalde vragen worden bij voorafgaande toetsing gemarkeerd als **rode vlag** (bijvoorbeeld gebruik van geanonimiseerde gegevens)
- Volledig ingevulde vragenlijst = voorwaarde voor **ontvankelijkheid** bij indiening EC
- Samenwerking tussen EC, CTC en DPO
  - Jurist CTC kijkt bepaalde aspecten na (standaard of steekproefsgewijs) vóór indiening EC
  - Privacytoets = onderdeel van bespreking bij EC
  - DPO wordt niet altijd rechtstreeks betrokken, maar escalatie is mogelijk (vooraf of achteraf)

Privacytoets

Waarom gekozen voor een formele privacytoets in deze vorm? Meerdere redenen:

- **Wettelijke verplichting** voor EC om privacytoets uit te voeren (los van GDPR)
- **Register** van de gegevensverwerkingen
- **Informatieplicht** betrokkenen
  - Vertaalt zich in verplichting PI om korte omschrijving van de studie in lekentermen te voorzien die gebruikt kan worden om automatisch aan patiënt / deelnemer te bezorgen
- Verplichting tot uitvoering van een **Data Protection Impact Assessment** (DPIA / GEB)
  - Medisch wetenschappelijk onderzoek met gezondheidsgegevens bijna altijd high risk
    - Aanwezigheid van Twee factoren nog vermelden?

Privacytoets versus Data Protection Impact Assessment



Beslissingsboom Art 29 WP – Guidelines on DPIA (04/2017)

Privacytoets versus Data Protection Impact Assessment

Belangrijke elementen:

- Waarschijnlijk hoog risico?
  - In geval van medisch wetenschappelijk onderzoek gewoonlijk:
    - Gevoelige gegevens
    - Grote schaal
    - Overige factoren zie: Art 29 WP – Guidelines on DPIA (04/2017)
- Toepassing van Artikel 35? Vergeet lijsten van nationale toezichthouders met verwerkingen waarvoor DPIA verplicht is niet.

In UZ Leuven gekozen voor **"template DPIA"** als onderdeel van de privacytoets:

- PI kan zich conformeren aan maatregelen opgenomen in de template DPIA
- PI kan afwijking op template DPIA vragen door escalatieprocedure op te starten (JUR, CTC, DPO & IT worden betrokken)
  - Typisch wanneer het doel of opzet van het onderzoek een aanpassing vereist aan de voorgestelde maatregelen
- Opgemaakt voor retrospectief onderzoek enerzijds, prospectief onderzoek anderzijds
  - vanuit de PIA tool CNIL (i.s.m. verschillende leden RUZB)

Privacytoets

Wat houdt de privacytoets in?

Dynamische vragenlijst in te vullen door onderzoeker

- Deel van het registratieproces bij Clinical Trial Center
- Noodzakelijke voorwaarde voor ontvankelijkheid bij EC

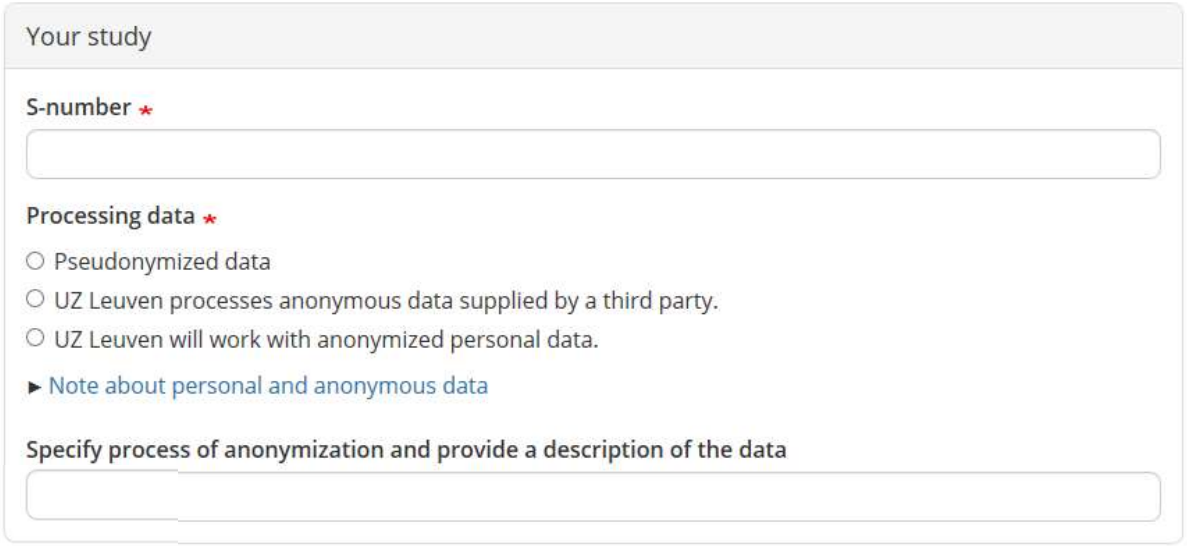
Inhoud is gebaseerd op vragenlijst voor wetenschappelijk onderzoek zoals opgemaakt binnen de VLIR

→ Kleine aanpassingen louter te maken met toespitsing op medisch wetenschappelijk onderzoek

Privacytoets – Inhoudelijk belangrijkste aspecten

- Anonimisatie en pseudonimisatie
- Proportionaliteit van de gegevensverwerking
- Rechtsgrond voor de gegevensverwerking
- Recht op informatie van de betrokkene

Anonimisatie en pseudonimisatie



Strikte interpretatie GDPR zorgt (nog steeds) voor verwarring

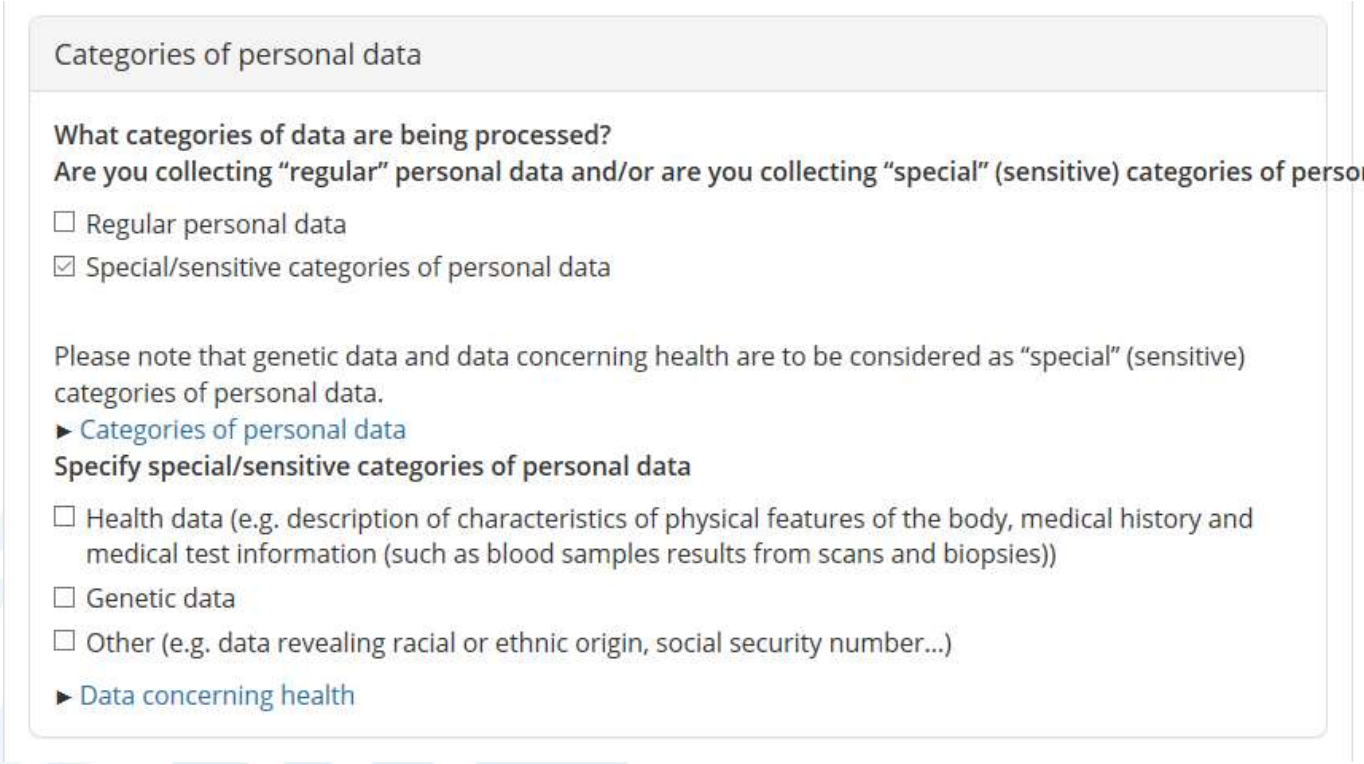
Grootste misvattingen:

- anoniem voor u, maar niet voor mij
- anonimisatie = de-identificatie in HIPAA

Heel vaak geen anonimisatie, maar pseudonimisatie → GDPR wel van toepassing

N.B. HIPAA identificatoren goede maatstaf voor pseudonimisatie

Proportionaliteit van de gegevensverwerking



Categories of personal data

What categories of data are being processed?
Are you collecting "regular" personal data and/or are you collecting "special" (sensitive) categories of personal data? *

☐ Regular personal data
☑ Special/sensitive categories of personal data

Please note that genetic data and data concerning health are to be considered as "special" (sensitive) categories of personal data.
► Categories of personal data
Specify special/sensitive categories of personal data

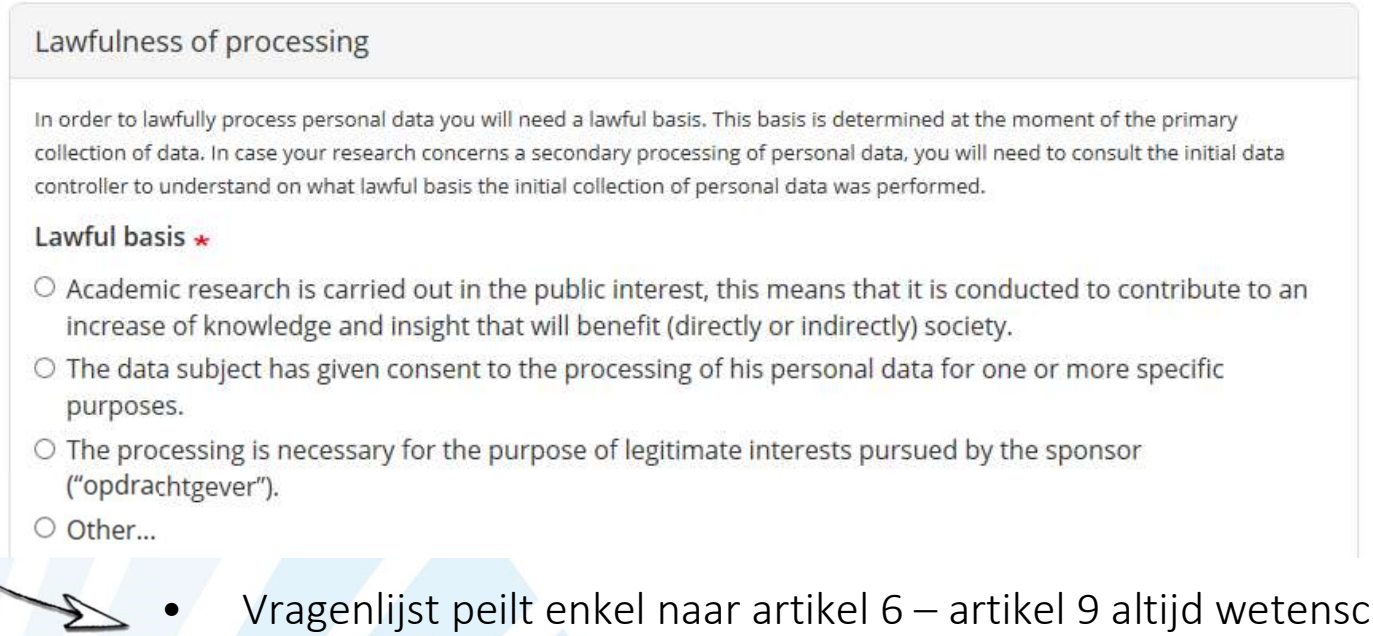
☐ Health data (e.g. description of characteristics of physical features of the body, medical history and medical test information (such as blood samples results from scans and biopsies))
☐ Genetic data
☐ Other (e.g. data revealing racial or ethnic origin, social security number...)

► Data concerning health

Vragenlijst registreert enkel types van gegevens. Proportionaliteit moet blijken uit protocol.

→ Interdisciplinaire blik nodig om bv. inhoud van eCRF te beoordelen

Rechtsgrond voor de gegevensverwerking



Lawfulness of processing

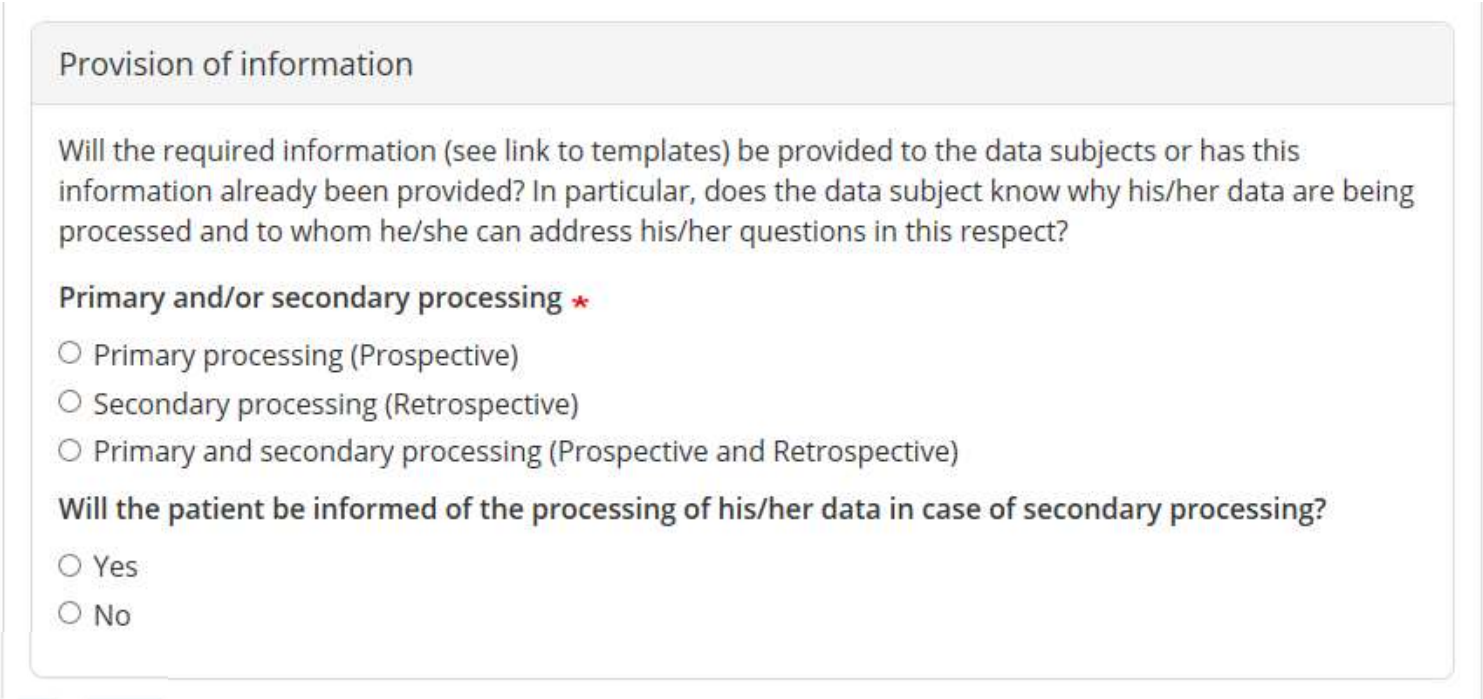
In order to lawfully process personal data you will need a lawful basis. This basis is determined at the moment of the primary collection of data. In case your research concerns a secondary processing of personal data, you will need to consult the initial data controller to understand on what lawful basis the initial collection of personal data was performed.

Lawful basis *

- ○ Academic research is carried out in the public interest, this means that it is conducted to contribute to an increase of knowledge and insight that will benefit (directly or indirectly) society.
- ○ The data subject has given consent to the processing of his personal data for one or more specific purposes.
- ○ The processing is necessary for the purpose of legitimate interests pursued by the sponsor ("opdrachtgever").
- ○ Other...

- Vragenlijst peilt enkel naar artikel 6 – artikel 9 altijd wetenschappelijk onderzoek
- Peilt altijd naar rechtsgrond van de primaire verwerking
- Rechtsgrond wordt altijd bepaald door data controller
  - Maakt dat we hier verschillende opties moeten aanbieden
  - Als UZ Leuven data controller, keuze voor public interest

Recht op informatie voor de betrokkene



Provision of information

Will the required information (see link to templates) be provided to the data subjects or has this information already been provided? In particular, does the data subject know why his/her data are being processed and to whom he/she can address his/her questions in this respect?

Primary and/or secondary processing *

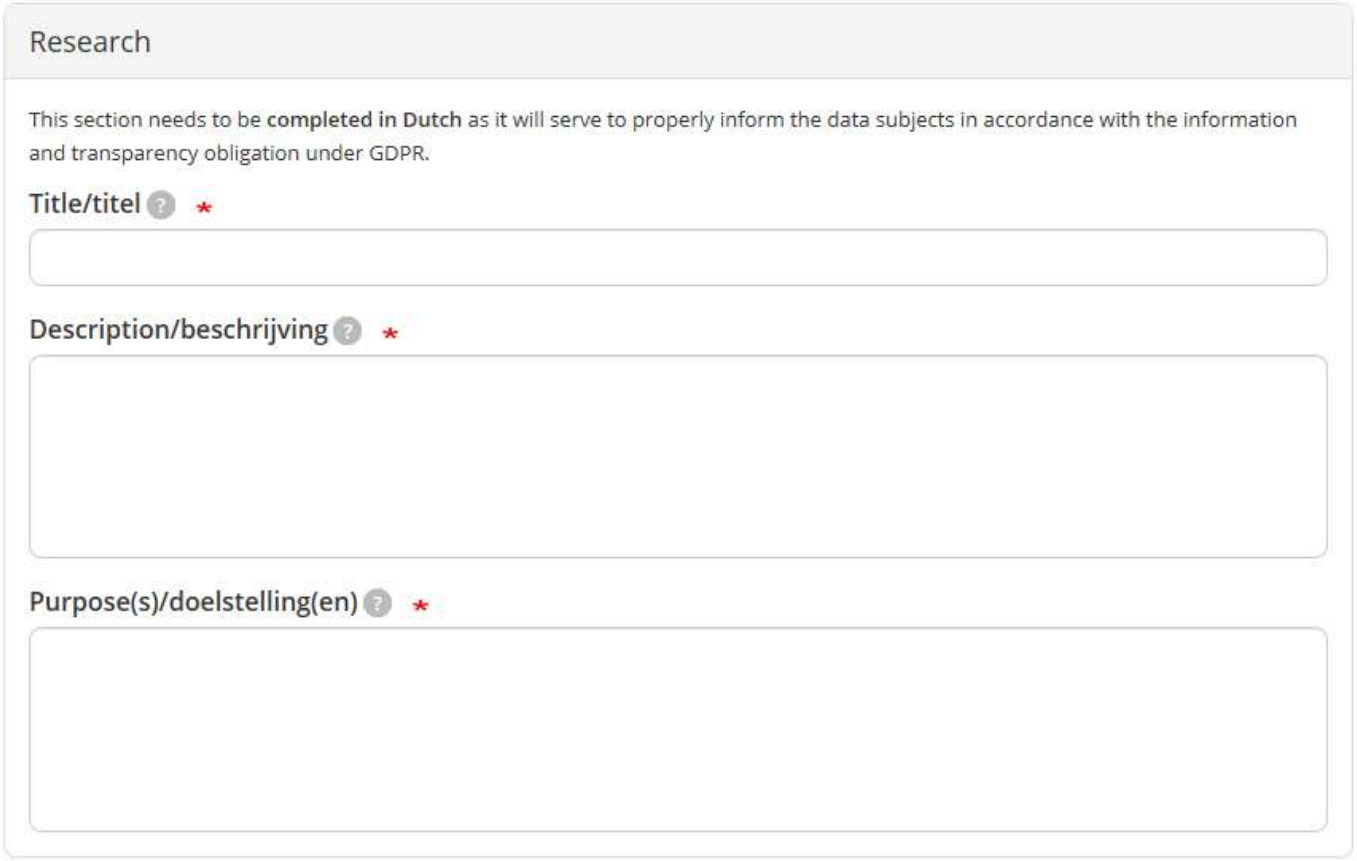
- ○ Primary processing (Prospective)
- ○ Secondary processing (Retrospective)
- ○ Primary and secondary processing (Prospective and Retrospective)

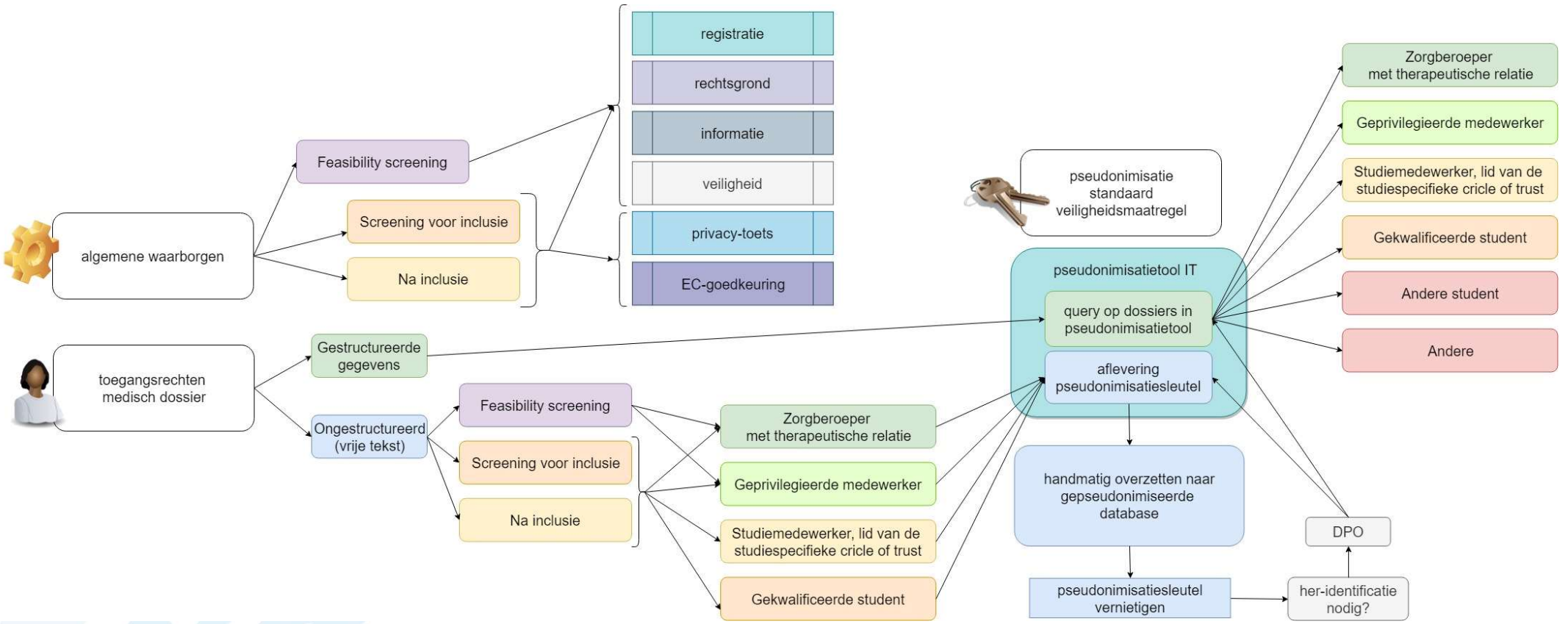
Will the patient be informed of the processing of his/her data in case of secondary processing?

- ○ Yes
- ○ No

Transparantie als allerbelangrijkste waarborg naast pseudonimisatie.

Recht op informatie voor de betrokkene




algemene waarborgen
Feasibility screening
Screening voor inclusie
Na inclusie
registratie
rechtsgrond
informatie
veiligheid
privacy-toets
EC-goedkeuring
pseudonimisatie
standaard
veiligheidsmaatregel
toegangsrechten
medisch dossier
Gestructureerde
gegevens
Ongestructureerd
(vrije tekst)
Feasibility screening
Screening voor inclusie
Na inclusie
Zorgberoeper
met therapeutische relatie
Geprivilegieerde medewerker
Studiemedewerker, lid van de
studiespecifieke cricle of trust
Gekwalificeerde student
pseudonimisatietool IT
query op dossiers in
pseudonimisatietool
aflevering
pseudonimisatiesleutel
handmatig overzetten naar
gepseudonimiseerde
database
pseudonimisatiesleutel
vernietigen
DPO
her-identificatie
nodig?
Zorgberoeper
met therapeutische relatie
Geprivilegieerde medewerker
Studiemedewerker, lid van de
studiespecifieke cricle of trust
Gekwalificeerde student
Andere student
Andere

Griet Verhenneman
DPO – UZ Leuven
Affiliated Researcher Centre for IT and IP Law, KULeuven
griet.verhenneman@uzleuven.be