



UZ
LEUVEN

Verwerken van persoonsgegevens in wetenschappelijk onderzoek conform GDPR

Michèle Dekervel
Clinical Trial Center (CTC)
9 februari 2024

SAMEN
GRENZEN
VERLEGGEN

GDPR in het kort



GDPR staat voor 'General Data Protection Regulation' of in het Nederlands 'Algemene Verordening Gegevensbescherming' of AVG

- Europese wetgeving sinds 25 mei 2018:
 - rechtstreeks toepasselijk in alle landen van de Europese Economische Ruimte (EER) (dit zijn de landen van de EU + Noorwegen, IJsland en Liechtenstein)
 - aangevuld met de Belgische wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens
- bepaalt de principes die van toepassing zijn wanneer we omgaan met gegevens over natuurlijke personen o.a.:
 - algemene beginselen van de vorige wetgeving
 - toelatingsgronden om persoonsgegevens te mogen verwerken
 - rechten van de betrokkene
 - meldingsplicht van een datalek aan de Gegevensbeschermingsautoriteit (GBA) en de betrokkene binnen 72 uur na de ontdekking
 - GBA kan hoge boetes opleggen (20.000.000 EUR of tot 4% van de globale jaaromzet)
 - aanstelling Data Protection Officer (DPO) in grote organisaties
- Meer informatie: [intern] <https://wiki.uz.kuleuven.ac.be/display/uzl/GDPR>, [extern] <https://www.uzleuven.be/nl/privacy-en-uw-dossier>

Wanneer je persoonsgegevens gebruikt, moet je je telkens **vijf basisvragen** stellen: waarom, wat, waar, wie en hoe lang?

1. Waarom verwerk ik de persoonsgegevens? Doelbinding en toelatingsgrond
2. Wat mag ik verwerken? Minimale gegevensverwerking, need-to-know, not nice-to-know principe
3. Waar mag ik persoonsgegevens verwerken en bewaren? Zie [afsprakennota Excel gebruik](#)
4. Wie mag toegang hebben tot persoonsgegevens? Zie [KWS toegang beleid](#)
5. Moet ik de verzamelde persoonsgegevens vernietigen en zo ja, wanneer? Opslagbeperking, bewaartermijn in studies minstens 25 jaar

GDPR en wetenschappelijk onderzoek



GDPR-vragenlijst voor onderzoekers

GDPR-vragenlijst: <https://www.uzleuven.be/nl/clinical-trial-center/ctc-gdpr-questionnaire>

Na toekenning S-nummer bij het CTC verzoek om GDPR-vragenlijst zo snel mogelijk in te vullen

Let op ✓ **ontvankelijkheidsvereiste EC Onderzoek**
ook vereist voor CTR/MDR/IVDR studies

3 finaliteiten:

- register van alle verwerkingsactiviteiten (transparantie)
- informatieplicht (transparantie)
- privacy check door CTC/EC/DPO

Dynamische vragenlijst

Fundamentele begrippen

Verwerking	Technische en organisatorische maatregelen	Rechten van betrokkene
Persoonsgegevens	Toelatingsgrond	Anonieme gegevens
Pseudonimisering	Informatie	Verwerkersovereenkomst/DPA
Verwerkingsverantwoordelijke	Primaire verwerking	DPO
Verwerker	Secundaire verwerking	Transparantie
Inbreuk in verband met persoonsgegevens/datalek	Categorieën van persoonsgegevens	Doorgifte aan derde landen
Toezichthoudende autoriteit /GBA	Gegevensbeschermingseffectbeoordeling (GEB/DPIA)	Algemeen belang

Toepassingsgebied: verwerking van persoonsgegevens

Your study

S-number *

S-number (enter in format SXXXXX, e.g. S12345)

Processing data *

UZ Leuven will process pseudonymized data.

UZ Leuven will process anonymous data supplied by a third party.

UZ Leuven will work with anonymized personal data.

KU Leuven will process data without UZ Leuven being data controller or processor for the purpose of the study (eg. KU Leuven acting as sponsor).
[KU Leuven GDPR questionnaire to be filled in](#) (only available for KU Leuven personnel)

► [Note about personal and anonymous data](#)

Specify process of anonymization and provide a description of the data

Voor een studie met s-nummer moet je steeds de GDPR-vragenlijst invullen maar de volgende gegevens vallen **buiten het GDPR toepassingsgebied:**

- **anonieme/geanonimiseerde gegevens**
- **gegevens van rechtspersonen**
- **gegevens van overleden personen**

Anonieme en gepseudonimiseerde gegevens

- **Persoonsgegevens** =

alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('betrokkene')

Enkele voorbeelden: naam, adres, e-mailadres, code van een staal, IP-adres, gezondheidsgegevens, medisch beeld, ...

Let op ✓ ook gepseudonimiseerde gegevens zijn persoonsgegevens en vallen onder de GDPR

- **Gepseudonimiseerde gegevens** =

gegevens die niet kunnen worden gelinkt aan een individuele persoon zonder het gebruik van aanvullende gegevens

⇒ wanneer de onderzoeker een link behoudt tussen de identiteit van de deelnemer en de gegevens (codelijst)

⇒ wanneer het de bedoeling is dat er nadien nog kan worden teruggegaan naar het medisch dossier van de deelnemers

⇒ wanneer de gegevensverzameling een combinatie van gegevens betreft die de deelnemer indirect identificeerbaar kunnen maken zoals locatiegegevens, persoonlijke karakteristieken, uniek na combinatie databanken,...

■ **#Anonieme gegevens** =

gegevens die op geen enkele wijze – door niemand en nooit meer – terug te leiden zijn tot een bepaald individu
moeilijk te bereiken want:

- gegevens zijn enkel anoniem wanneer ze niet toelaten om een individu te selecteren
- anoniem voor u, maar niet voor mij, bestaat niet
- tijdelijke anonimiteit bestaat niet
- medische beelden zijn nooit anoniem
- uitzonderlijke voorbeelden in het kader van onderzoek:
 - ⇒ eenmalige anonieme vragenlijst met enkel een informatiebrief (vb. Qualtrics anonymous link met de optie waarin het IP adres van de deelnemer niet wordt bijgehouden)
 - ⇒ firma bezorgt ons een anonieme dataset

Gepseudonimiseerde gegevens = standaard in wetenschappelijk onderzoek (zie 1.58 GCP: Subject identification code)

⇒ meest voorkomende antwoord op de eerste vraag zal dus zijn:

Processing data *

UZ Leuven will process pseudonymized data.

Tenzij:

- Je werkt met anonieme gegevens
maar **Let op** ✓ **dit is zeer uitzonderlijk in het kader van onderzoek:**
 - anonimisatie is steeds onomkeerbaar
 - ≠ pseudonimisatie of codering
 - ≠ de-identification in HIPAA (US privacy law voor gezondheidssector)
- KU Leuven studie

Let op ✓ **Identificatie door één partij in de ketting is voldoende** → niet anoniem

Voorbeeld 1

In het kader van commerciële klinische proef vult onderzoeker het eCRF in waarbij een studiecodel wordt gebruikt voor de studiedeelnemer, de sponsor ontvangt de gecodeerde data zonder de studiedeelnemer direct te kunnen identificeren

Voorbeeld 2

Er worden medische beelden zonder directe identifier bezorgd aan een collega-onderzoeker van een ander ziekenhuis voor zijn/haar studieprotocol, op basis van de beelden kan de collega-onderzoeker de patiënten niet direct identificeren

Voorbeeld 3

Een tijdschrift eist dat de onderzoeker de onderzoeksdata in het kader van menselijk genomonderzoek deelt via een genoomdatabank/'repository', op basis van de dataset zijn de studiedeelnemers niet direct identificeerbaar

Voorbeeld 4

Een onderzoeker stuurt gecodeerde bloedstalen (verplichte traceerbaarheid) met minimale data van de donor (leeftijd en geslacht) naar een buitenlands labo voor analyse, op basis van de code en data is de donor voor het labo niet direct identificeerbaar

Tips om goed te pseudonimiseren:

- bewaar het **sleutelbestand** altijd op een andere plek dan het **gepseudonimiseerd bestand**
- beperk de **toegangsrechten** voor de plaats waar je het sleutelbestand bewaart tot 2 à 3 personen
- de pseudonimisering moet **uniek** zijn per project
- **sleutels** mogen op geen enkele manier inhoud hebben in relatie tot de identiteit van de betrokken personen (bv. patiënten)
- gebruik nooit EAD-nummers, EMD-nummers, rijksregisternummers of geboortedata in de codering
- in gepseudonimiseerde gegevens staan **geen direct herleidbare gegevens**. Om goed te pseudonimiseren, de 18 HIPAA identificatoren coderen, generaliseren of weglaten zoals naam, woonplaats, geboortedatum, ...
- maak gebruik van de [pseudonimisatietool](#) om gestructureerde data uit KWS te halen

- KU Leuven will process data without UZ Leuven being data controller or processor for the purpose of the study (eg. KU Leuven acting as sponsor).
[KU Leuven GDPR questionnaire to be filled in](#) (only available for KU Leuven personnel)

= KU Leuven verwerkt persoonsgegevens zonder dat UZ Leuven de verwerkingsverantwoordelijke of verwerker is voor de studie

- KU Leuven is de opdrachtgever van de studie
- Mynexuzhealth patiëntvriendelijke samenvatting en van wie de persoonsgegevens worden verwerkt wel nog invullen in de GDPR-vragenlijst
- KU Leuven Eenheid Privacy en Ethiek (PRET)-vragenlijst in te vullen:
<https://idp.kuleuven.be/idp/profile/SAML2/Redirect/SSO?execution=e2s1> (alleen beschikbaar voor KU Leuven personeel)

- **Verwerkingsverantwoordelijke ('controller')** =

bepaalt doel ("waarom") van en middelen ("hoe") voor verwerking van persoonsgegevens

in principe de opdrachtgever/sponsor van de studie want de opdrachtgever is diegene die de verantwoordelijkheid op zich neemt voor het starten, het beheer en/of de financiering van het onderzoek = van wie het protocol uitgaat

- **Verwerker ('processor')** =

verwerkt persoonsgegevens ten behoeve van verwerkingsverantwoordelijke

in principe de site/deelnemend centrum

Dus de eerste vraag: **Is er naast UZ Leuven een derde partij betrokken in de studie?**

Zo niet: monocentrische studie binnen UZ Leuven zonder betrokkenheid van een derde partij

⇒ UZ Leuven is de opdrachtgever van de studie en verwerkingsverantwoordelijke

Verwerkingsverantwoordelijke en verwerker

Data controller versus data processor

Is there (next to UZ Leuven) another university, research institution or partner involved in the study? *

- No, it is a monocentric study within UZ Leuven without third party involvement and UZ Leuven is the sponsor of the study and hence data controller
- Yes

Who determines the purposes and means of the study? (this means solely financing is insufficient) ? *

- This is solely determined within UZ Leuven (UZ Leuven is sponsor of the study and hence data controller; another university, research institution or partner involved in the study is acting as data processor, or is acting as separate data controller)
- UZ Leuven determines this together with someone outside of UZ Leuven (joint controllership)
- UZ Leuven executes on behalf of someone outside of UZ Leuven (UZ Leuven is data processor)
Also in case UZ Leuven would take on the role of national coordinator for Belgium, UZ Leuven would in principle act as data processor.
- This is solely determined by someone outside of UZ Leuven and UZ Leuven does not act as data processor (controller-to-controller transfer)

Has a data processing agreement or "DPA" been drafted between the controller and the processor or another type of data processing arrangement between the parties (in function of parties's roles under GDPR, for example a joint controllership agreement or a controller-to-controller transfer agreement)?

- Yes
- No

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Tweede vraag indien ja: wat is de GDPR rol van UZ Leuven en deze derde partij

Let op ✓ GDPR rollen=breekpunt juridisch groen licht voor CTC validatie flow naar EC Onderzoek en naar FAGG (CTR/MDR/IVDR academisch onderzoek)

Optie 1: UZ Leuven is verwerkingsverantwoordelijke, de derde is verwerker of afzonderlijke verwerkingsverantwoordelijke

Optie 2: UZ Leuven en de derde zijn gezamenlijke verwerkingsverantwoordelijken

Optie 3: UZ Leuven is verwerker en de derde is verwerkingsverantwoordelijke

Optie 4: UZ Leuven is geen verwerker en de derde is verwerkingsverantwoordelijke (controller-to-controller)

⇒ wanneer UZ Leuven opdrachtgever is van een studie is UZ Leuven de verwerkingsverantwoordelijke

⇒ in alle andere gevallen is UZ Leuven in principe de verwerker

- Monocentrische UZ Leuven studie zonder betrokkenheid van een derde partij

Is there (next to UZ Leuven) another university, research institution or partner involved in the study?

- No, it is a monocentric study within UZ Leuven without third party involvement is and UZ Leuven is the sponsor of the study and hence data controller

- UZ Leuven onderzoeker zet een multicentrische studie op

Who determines the purposes and means of the study? (this means solely financing is insufficient) ?

- This is solely determined within UZ Leuven (UZ Leuven is sponsor of the study and hence data controller; the other university, research institution or partner involved in the study is acting as data processor))

- Buitenlandse academische organisatie Y vraagt residuaire stalen van UZ Leuven patiënten voor studie in het buitenland

optie 3

- UZ Leuven executes on behalf of someone outside of UZ Leuven (UZ Leuven is data processor)
Also in case UZ Leuven would take on the role of national coordinator for Belgium, UZ Leuven would in principle act as data processor.

Specify someone outside of UZ Leuven

Organisatie Y

- Commerciële klinische proef van firma X waaraan UZ Leuven deelneemt

optie 3

- UZ Leuven executes on behalf of someone outside of UZ Leuven (UZ Leuven is data processor)
Also in case UZ Leuven would take on the role of national coordinator for Belgium, UZ Leuven would in principle act as data processor.

Specify someone outside of UZ Leuven

Firma X

- Optie 2 ‘gezamenlijke verwerkingsverantwoordelijke’ en optie 4 ‘controller-to-controller’ = uitzonderingssituaties
- DPA moet in principe worden voorzien door de juristen van het CTC dus op deze vraag mag bij contract of DPA annex aan het protocol ‘ja’ worden geantwoord

Has a data processing agreement or “DPA” been drafted between the controller and the processor or another type of data processing arrangement between the parties (in function of parties’s roles under GDPR, for example a joint controllership agreement or a controller-to-controller transfer agreement)?

Yes

No

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Data description and collection

Primary versus secondary collection

Are new data being collected (primary processing – prospective study)?

And/or are only already collected data being processed (secondary processing – retrospective study)? 

*

Primary processing (Prospective study) and/or

Secondary processing (Retrospective study)

het kan zeker ook beiden zijn voor een studie

- **primaire verwerking – prospectieve studie =**

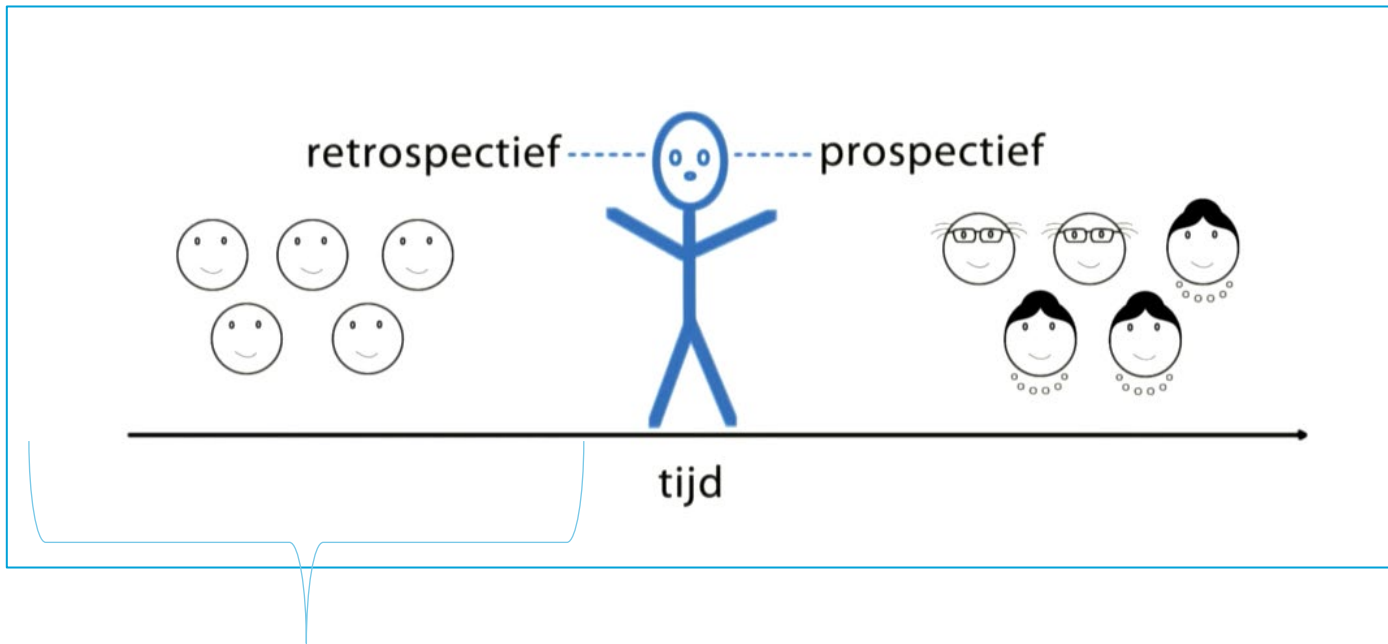
verzameling van nieuwe gegevens (experiment, klinisch onderzoek, klinische proef)

- **secundaire verwerking – retrospectieve studie =**

verwerking van eerder verzamelde gegevens

ook secundair gebruik van gecodeerd lichaamsmateriaal

Retrospectieve studie ↔ prospectieve studie



retrospectieve studie =

- een studie op basis van gegevens uit het verleden die zich in bestaande patiëntendossiers, medische dossiers of administratieve dossiers of bestanden bevinden
- voor zover voor deze studies op geen enkele wijze nieuwe gegevens met betrekking tot deze patiënten worden bekomen

Verwerking (zoals het verzamelen, bekijken, opslaan, doorgeven, analyseren, wissen) van persoonsgegevens

→ toelatingsgrond nodig (keuze uit 6)

Lawfulness of processing

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...

► [European Data Protection Board Opinion regarding consent as legal basis](#)

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.

- studies met UZ Leuven opdrachtgever: **algemeen belang/wetenschappelijk onderzoek**

Let op ✓ : onderscheid tussen deelname aan de studie (Belgische wetgeving rond onderzoek) en verwerking van persoonsgegevens (GDPR)

⇒ **voor deelname aan een experiment/klinisch onderzoek/klinische proef wel nog altijd toestemming nodig conform Belgische wet: ICF**

- studies met andere opdrachtgever: keuze toelatingsgrond aan de opdrachtgever

Let op ✓ : **voor commerciële retrospectieve studies een toestemmingsvereiste**

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)

Please, note that the data subject always has to be informed in case of primary processing! In case UZ Leuven is the sponsor of the study, the data subject will be informed of his/her data being processed for research purposes through the MyNexuzHealth application.

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

- Yes
- No

Export of data

Will the collected personal data be transferred to or shared with persons/institutions outside UZ Leuven?

- No
- Yes

Verplichte GDPR vermeldingen aan de betrokkene:

- de identiteit en de contactgegevens van de controller
- de contactgegevens van de DPO
- de toelatingsgrond voor de verwerking
- de ontvangers of categorieën van ontvangers van de persoonsgegevens
- de doorgifte aan derde land
- de periode gedurende welke de persoonsgegevens zullen worden bewaard
- de uitoefening van de GDPR-rechten
- dat de betrokkene het recht heeft klacht in te dienen bij de GBA

wanneer UZ Leuven opdrachtgever is van monocentrische retrospectieve studie/art.21 WLM wordt door het vlaggen van de patiënten in KWS automatisch aan de informatieplicht voldaan via de Mynexuzhealth- app

Research


Title/titel *

Name of data controller/Naam van verwerkingsverantwoordelijke ? *

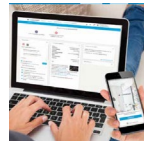
Description/beschrijving ? *

Purpose(s)/doelstelling(en) ? *

Link to website(s) with additional information/ Link naar website(s) met bijkomende informatie

- patiëntvriendelijke samenvatting: beschrijving van de doelstellingen van het onderzoek voor de patiënten
- automatisch informeren van de patiënten door het vlaggen van de patiënten in KWS met s-nummer 

Let op ✓ in alle studies: ook in retrospectieve studies moeten de patiënten gevlagd worden



Klinische studies

Een overzicht van uw actieve en afgelopen klinische studies.

- in het Nederlands, beknopt (niet te lang), volledig en begrijpelijk → het moet de patiënt informeren maar niet leiden tot extra vragen van de patiënt

Informatieplicht UZ Leuven studie (UZ Leuven = controller):

Prospectieve studie

- ICF (gebruik de [UZ Leuven templates](#))
- Ontvangstbrochure
- UZ Leuven privacy statement
- Mynexuzhealth

Retrospectieve studie

- Ontvangstbrochure
- UZ Leuven privacy statement
- Mynexuzhealth
- (Informatiebrief)

Mynexuzhealth app:

- monocentrische studie met UZ Leuven als opdrachtgever
 - ✓ patiënten UZ Leuven
- multicentrische studie met UZ Leuven als opdrachtgever
 - ✓ patiënten UZ Leuven
 - ✓ patiënten van andere Nexuzhealth ziekenhuizen
 - X patiënten van andere sites die geen gebruik maken van Mynexuzhealth

Categorieën van persoonsgegevens

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](#)

Data subjects

Whose personal data are being processed in the framework of the research? *

- Patients of UZ Leuven
- Patients of other hospitals than UZ Leuven
- Healthy volunteers
- UZ Leuven personnel
- Only deceased persons
- Other (e.g. are personal data of UZ Leuven/ KU Leuven students the object of the research?)

gezondheidsgegevens worden beschouwd als bijzondere (of gevoelige) categorieën van persoonsgegevens in de meeste gevallen moet dit dus ook worden aangeduid

geen persoonsgegevens maar toch regels voor het gebruik ervan en GDPR- vragenlijst

Technical and organisational measures

Where are data being stored? *

- Only centrally managed tools/systems/technology such as for example KWS, LWS
- Also decentrally managed tools/systems/technology

What tools/systems/technology are being used (other than the tools/systems/technology for the processing of personal data made available by UZ Leuven) *

Hier kan je het CRF vermelden waarmee zal worden gewerkt

- UZ Leuven ⇒ REDCap

✗ Zie [CR GEN-MEM-001](#) over Excel gebruik

Agreement with the UZ Leuven principles regarding processing of personal data and data protection impact analysis (“DPIA”)

The processing of “special categories” of personal data (such as “data concerning health” or genetic data) in the framework of research constitutes a high privacy risk for the data subjects.

Is UZ Leuven data controller? Please indicate under which DPIA of UZ Leuven your research fits.

- DPIA retrospective study
- DPIA prospective study
- None of the above

The investigator hereby acknowledges review of the GDPR guidance document for clinical researchers.

- verplichting van de verwerkingsverantwoordelijke
- een instrument om vooraf de privacy risico's van de gegevensverwerking in kaart te brengen
- laat toe om zowel de risico's in te schatten als de manier waarop deze kunnen worden beheerd
- UZ Leuven: [GEB retrospectieve studies](#) en [GEB prospectieve studies](#)

- interne e-learning ‘GDPR en privacy voor de onderzoeker’ via leercentrum
- GDPR-helpdesk gdpr@uzleuven.be (DPO + multidisciplinair team)
- meld een (potentieel) datalek altijd aan de DPO van UZ Leuven via gdpr@uzleuven.be

- intern adviesorgaan en beoordelingscommissie **Data Protection Board:**

vanaf 1 september 2021 dient er vóór elk gebruik of doorgifte van persoonsgegevens van patiënten voor een doel ander dan zorg of wetenschappelijk onderzoek een dp-nummer te worden aangevraagd (voorbeeld een terugbetalingsdossier)

(Zie intern: <https://wiki.uz.kuleuven.ac.be/display/public/gg/Data+Protection+Board>)

▪ **Data Access Committee (DAC)**

DAC KU Leuven/UZ Leuven. Zie <https://www.uzleuven.be/nl/dac>

een aanspreekpunt voor KU Leuven/UZ Leuven onderzoekers in volgende situaties:

- onderzoekers dienen data in bij European Genome-phenome Archive (EGA)
 - onderzoekers ontvangen verzoeken van derden om toegang te bekomen tot hun datasets met eigen humane genetische data
 - onderzoekers vragen toegang tot externe genetische/genomische datasets in repositories (onder andere EGA, NIHdbGAP)
 - onderzoekers willen genetische/genomische data indienen bij een andere domeinspecifieke databank dan EGA
-
- ## ▪ **Opt-out (in de toekomst)**

Extra informatie over het invullen van de vragenlijst kan u in het GDPR guidance document (met Q&A) terugvinden:
https://gbiomed.kuleuven.be/english/ctc/intern/quality-management/procedural-documents-1/legal/cr-leg-ug-001-1-0_gdpr-for-clinical-research-at-uz-leuven

Clinical Trial Center

ctc@uzleuven.be

Tel. +32 (0)16 34 19 98

<https://gbiomed.kuleuven.be/english/ctc/intern>

Michèle Dekervel

michele.dekervel@uzleuven.be

Tel. +32 (0)16 34 59 37

CTC OFFICE

1st Tuesday and the 3rd Friday of each month > maak uw afspraak via onze website

<https://gbiomed.kuleuven.be/english/ctc/intern/ctc-office/CTCOffice>

Bedankt voor uw aandacht!