



# Personal data protection in R&D collaborations

*Vincent Wellens*

avocat à la Cour (Luxembourg) / avocat (Bruxelles)

● **NautaDutilh**

International Law Firm | Amsterdam · Brussels · London · Luxembourg · New York · Rotterdam

# Correct personal data protection compliance in R&D collaboration depends on the right qualification of all stakeholders :

## single controllers

- Full GDPR compliance by each of the stakeholders
- Specific national research provisions to be followed by each stakeholders for its country of establishment
- Some national legislations require a data sharing agreement (good practice anyway)

## joint controllers

- Full GDPR compliance by each but tasks can be distributed
- Cumul of specific national research provisions impacting the whole project!
- Joint controllership agreement
- Data subjects to be informed about the key elements and can exercise their rights against each of the joint controllers !

## data processor

- Only compliance with specific provisions of the GDPR aimed at processors (security measures, DPO, processing record, etc.)
- Data processing agreement (standard clauses !)

## Zoom on national specific provisions on research



- derogations from some data subjects' rights
- safeguards
  - special record of processing activities (justification for exception to data subjects' rights ...),
  - information on anonymisation or not
  - data sharing agreement with initial controller ...



- derogations from some data subjects' rights
- safeguards
  - DPIA
  - DPO
  - trusted third party for anonymisation/ pseudonymisation
  - privacy enhancing technology
  - access restrictions
  - data management plan



- derogations from some data subjects' rights
- safeguards
  - prior authorisation or consent
  - increased confidentiality for special category data
  - encryption
  - ...

## Qualification of R&D stakeholders

Joint  
controllers

- **Determine jointly** the purposes (why) and the means (how)
- **EDPB** : converging decisions = complementing decisions having a tangible impact on the determination of purposes and means of the processing -> would the processing not be possible without both parties' participation (processing by each party is inseparable, i.e. inextricably linked) ?

Single  
controllers

- Determines alone the purposes and the means (especially « essential » means, which data, which persons, ...)

Data  
processor

- Acting on behalf and on exclusive instruction of controller
- Decision on non-essential means possible (which software)

## Qualification of stakeholders – EDPB example for R&D

### **Example: Research project by institutes**

Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.

## Qualification of stakeholders – outstanding questions < Luxembourg National GDPR Working Group for Research

For instance, it might be possible that a party determines the purpose and with another party, they jointly define the means. Such a situation could actually apply in the example of the clinical trial. It often happens that the sponsor, e.g. a pharmaceutical company, determines the purpose of the clinical trial – the test of a newly developed drug candidate. They would then engage a contract research organisation or a clinical partner with whom they jointly develop the means – the protocol of the clinical trial. The gain of the contract research organisation is purely financial. However, they will largely define the research protocol as their experience will be key for the development. Such situation is currently not solved with the criteria provided in the guidelines.

Another extreme can be that one party determines the purpose while another party determines solely the means. As such, no party fulfils the criteria defining the controller. This could be the case in policy development. A ministry selects a public research organisation, on the basis of a financial offer, to provide them with information on the socio-economic situation and the corresponding influences in the population. If the ministry selects the research organisation purely based on the financial offer without influencing the methodology, the subject recruitment or the analysis. All the means will be defined by the research organisation that, on the other hand, has not defined the purpose.

# Take aways from the CJEU judgment in C-40/17 Fashion ID

CJEU decision on the roles of a website operator and Facebook when embedding a Facebook “Like” social plugin:

*also in case of “joint” controllers, each must have its own basis of lawful processing (important for health data) !*

*no access to data required to qualify as a data controller (cf. earlier case law)*

*not all controllers must have the same level of implication*

*joint controllership : mutual commercial benefit*

*but joint controllership only at the level of data collection and transmission*

*in case of joint controllership: consent (if required) and information obligations preferably to be performed at the time of first contact*

*further processing under “single” controllership: idea of phased approach in data protection*

*each must ensure own compliance (information, consent (if required), ...*

# Correct reflection of roles in data management plan



6	Gestion et suivi de la clientèle	Traitement de la clientèle sur la base des schémas, des transactions commerciales ou autres relations professionnelles Suivi de la relation client (registrar de réservation, gestion des réservations et services après-vente) Elaboration de profil de la clientèle existante et la prospection de nouveaux clients	Les clients de l'organisation	Identification Identification électronique Données financières	Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de services précontractuellement liés à la demande de celle-ci	18 ans	Gestion des accès sur le principe du "Need to know" Tenue d'un journal des accès aux dossiers Protection contre les logiciels malveillants Sécurité du périmètre réseau
7	Gestion des fournisseurs	Gestion et administration des fournisseurs et les commandes aux fournisseurs	Fournisseurs en relation avec l'organisation	Identification Identification électronique	Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de services précontractuellement liés à la demande de celle-ci	18 ans	Protection contre les logiciels malveillants
8	Marketing direct	Constitution d'un fichier client en vue d'une exploitation de marketing direct Envoi de newsletters	Clients de l'organisation Prospects	Identification Identification électronique Préférence et opt-out Caractéristiques personnelles Localité et télépho	Consentement de la personne concernée		Durée de la relation entre les personnes concernées et le responsable de traitement Retrait du consentement de la personne concernée Minimisation des données transférées vers les sous-traitants Protection contre les logiciels malveillants Sécurité du périmètre réseau/Protection contre les intrus(es) d'Internet
9	Gestion des cartes de fidélité des clients	Programme de fidélité destiné aux clients	Clients de l'organisation	Identification Caractéristiques personnelles Composition du ménage Habitudes de consommation	Consentement de la personne concernée	Jusqu'à retrait du consentement de la personne concernée Après 6 mois d'inactivité de la carte de fidélité Jusqu'à l'expiration de la carte de fidélité	Gestion des accès sur le principe du "Need to know" Anonymisation des données dès que possible pour des fins statistiques Protection contre les logiciels malveillants Sécurité du périmètre réseau/Protection contre les intrus(es) d'Internet

## Privacy notice Consent



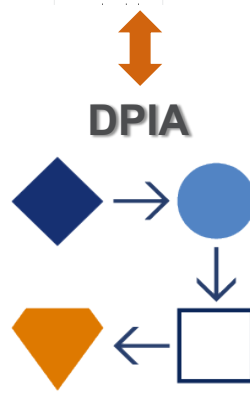
## Contracts (DPAs, joint controllership...)



## BCRs / SCC



## Record



## DPIA



## Interesting sources

- [GDPR](#)
- [Luxembourg Law of 1 August 2018](#)  
(complementing the GDPR and with specific provisions on research)
- [EDPB guidelines on the notions of « controller » and « processor »](#)
- EU Standard contractual clauses for a data processing agreement ([draft](#))
- [Horizon 2020 Data Management Plan](#)

# Contact details



## Vincent Wellens

Partner, IP, Technology Law & Data Protection  
T. +352 26 12 29 34  
E. Vincent.Wellens@nautadutilh.com



## Sigrid Heirbrant

Associate, Technology Law & Data Protection  
T. +352 26 12 29 74 50  
E. Sigrid.Heirbrant@nautadutilh.com



## Carmen Schellekens

Senior Associate, Technology Law & Data Protection  
T. +352 26 12 29 74 06  
E. Carmen.Schellekens@nautadutilh.com



## Antoine Petronin

Associate, IP litigation & Data Protection  
T. +352 26 12 29 74 51  
E. Antoine.Petronin@nautadutilh.com



## Lindsay Korytko

Senior Associate, Technology Law & Data Protection  
T. +352 26 12 29 74 22  
E. Lindsay.Korytko@nautadutilh.com



Questions?  
At your disposal!

# A brief presentation of our firm

## Firm profile

Number of partners, associates and other legal staff.

- An international law firm practising Dutch, Belgian, Luxembourg and Dutch Caribbean law, founded in 1724.
- One of the largest law firms in the Benelux region:
  - 388 lawyers including 72 partners, including 14 female partners.
  - 10 of our lawyers are also university professors.
- Spread across 6 offices and 5 country desks: Offices in Amsterdam, Brussels, London, Luxembourg, New York and Rotterdam.
- Our country desks focus on: Germany, France, India, China and Japan. We also monitor growth markets such as Brazil, Mexico, Indonesia, South Korea and Turkey.
- An independent firm with non-exclusive relations with the top law firms in more than 80 countries.

## Office locations

