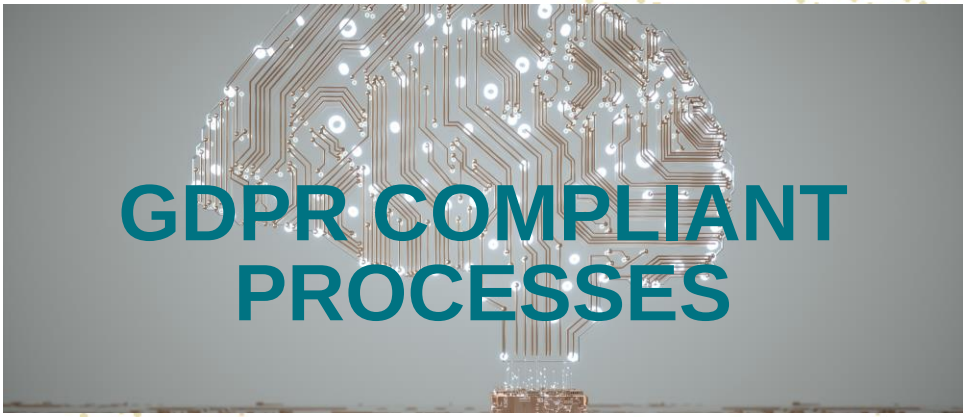
AXON
science based lawyers



GDPR COMPLIANT PROCESSES

CSMD2024
30 May 2024

health
food
technology

Cécile van der Heijden
www.axonadvocaten.nl

Disclaimer

This presentation contains my own opinions about the discussed legislation and not those of my employer or clients. This presentation cannot be relied on to make decisions about your specific situation.

AXON
science based lawyers

Introduction

- Welcome to the department of no?
  - 100% compliance is a myth and so are perfect processes
- What do I see go wrong?
  - “It’s not personal data”
  - “The other party, who coincidentally decides everything, is a processor”
  - “We signed this template that we got”
  - “The processor does not want to an audit”
  - “GDPR is a hassle and we have not allotted any time to data compliance”
  - “’Please review this agreement, but we don’t want to consider any related data protection issue”.
  - “Data security requirements does not need to be in line with MDR security requirements”
  - “This is the obligation of the site”
  - Etc….

AXON
science based lawyers

BACK TO BASICS

Back to basics – territorial scope

Bron: https://en.wikipedia.org/wiki/European_Economic_Area#/media/File:European_Economic_Area_members.svg

AXON science based lawyers

Extraterritoriale reikwijdte

"*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

- *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
- *the monitoring of their behaviour as far as their behaviour takes place within the Union*." (article 3(2) GDPR).

Relevant questions:

- What offer are we speaking of?
- What is monitoring of behaviour?
- Where are the data subjects?

AXON science based lawyers

Back to basics

Is it personal data?

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (article 4(1) GDPR)

Leads to a lot of discussion, especially with US parties

AXON science based lawyers

Back to basics

Recital 26

"*The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.*

To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

AXON science based lawyers

Back to basics

No, it's probably not anonymized data

Case law is decisive

1. Breyer (CJEU, 19 October 2016, C-582/14, ECLI:EU:C:2016:779, r.o. 45-49)

- Does the recipient have the means to identify?
  - i.e. via additional data.
    - If identification is prohibited by law or practically impossible, due to the disproportionate effort required in terms of time, cost and man-power, the risk of identification is considered insignificant in reality.

AXON science based lawyers

Back to basics

2. SRB (CJEU, 26 April 2023, ECLI:EU:T:2023:219):
- Confirms Breyer
- The party that provides the data needs to assess whether the data has the means to identify the data subjects.
  - Are there any legal and practical means that allow for access to the data?

AXON science based lawyers

You'll never walk alone…

The GDPR is not a standalone regulation.

That means
- Compliance with additional and national legislation
  - ICFs have to meet multiple requirements.
    - Address medical confidentiality in the agreements
- Further use under other regulations
  - development?
  - Separate use by processors for their own purposes?
  - PMS?

These are not only issues with respect to your collaboration / site agreement / MSA, but have consequences for your data processing relationship as well.

AXON science based lawyers

GDPR (I) – security

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

AXON science based lawyers

GDPR II – Pbd/Pbd

Article 25

Data protection by design and by default

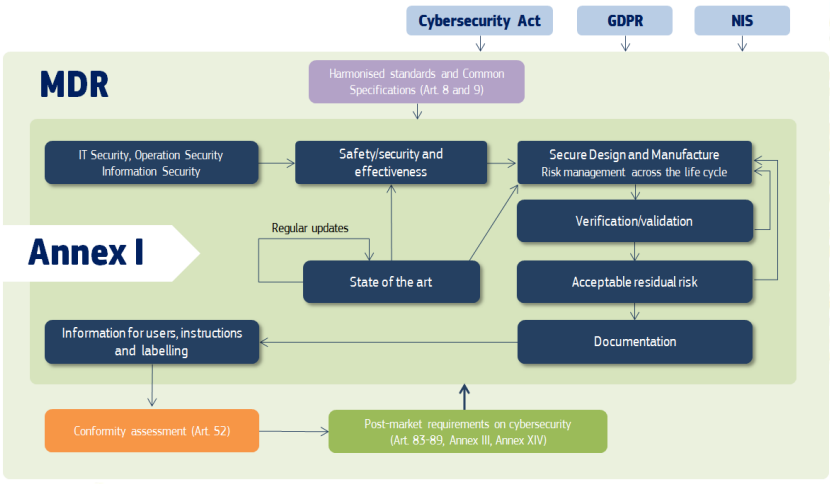
1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

AXON science based lawyers

Overview legislative framework



Source: MDCG 2019/16 rev. 1, p. 6.

AXON science based lawyers

Who are you working with and who needs the data for what?

CRO's
Service providers (IT, analytics, etc)
Labs
Sites
Ethics committees
Notified bodies
Competent authorities
Patients / participants
Study personnel, including principal investigators
Investors
Collaboration partners

➔ All with their own interests.

Controller vs. Processor (III)

Essential vs non-essential means

" "Essential means" are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller. Examples of essential means are the type of personal data which are processed ("which data shall be processed?"), the duration of the processing ("for how long shall they be processed?"), the categories of recipients ("who shall have access to them?") and the categories of data subjects ("whose personal data are being processed?"). "Non- essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on.

Bron: Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 14.

AXON
science based lawyers

Joint controllers

Article 26(1) GDPR:
"*Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation*."

Questions to ask:
- Do we take joint or converging decisions about the means and purposes of the processing?
- Are the processing activities of each party inextricably linked?

To be a controller, you do not need to have access to the full dataset.

JCA requires that you actually determine what you are going to do together with that party, and what you will not be doing jointly.

AXON science based lawyers

Agreements

- Data processing agreement
- Joint controller agreement
- Joint controller arrangement
- SCC
- "Data transfer agreement"
- Etc.

Contents of the data processing agreement and SCC are regulated. You can play with the other categories.

Be careful with data protection clauses in other agreements (i.e. collaboration agreements).

AXON science based lawyers

What follows?

So you have an agreement, what is next?

While an agreement is important, compliance is key

AXON
science based lawyers

Where is the data going?

- Data transfers
- Onward transfers
- LIA
- Adequacy decisions
- Self-certification

AXON
science based lawyers

Other things to consider

New EU-legislation + national deviations
- EHDS
- Data Governance Act
- Data Act
- NIS II Directive

Different procedures various supervisory authorities – they have their own opinions

Decisions by courts – especially CJEU

Decisions by EC (adequacy decision)

New EDPB guidance – the EDPB has been promising clinical research guidance for years.

AXON science based lawyers

Tips and tricks

Use your own templates or very carefully review those of other parties
Take special note of the liability clauses
Consider whether the agreed upon procedures are actually practical and in line with GDPR.

Be aware that things have not yet been reviewed in case-law (national and European level).

Do however not treat each regulation as a separate obligation to comply with, but instead try to achieve an overarching approach.
- Include overarching topics (i.e. security) in development and maintenance processes

Make sure IT, developers and GDPR / compliance teams speak with each other on.

Be aware of overlap (i.e. a personal data breach is often an security incident)

AXON science based lawyers

AXON
science based lawyers

THANK YOU FOR YOUR ATTENTION

www.axonlawyers.com

Cécile van der Heijden
Axon Lawyers

Piet Heinkade 183
1019 HC Amsterdam
T +31 88 650 6500
M +31 6 126 15 604

E cecile.vanderheijden@axonadvocaten.nl