Big data in Life Sciences and Healthcare and GDPR

Bird & Bird

Marc Martens

24 November 2017

Agenda

- Introduction – The GDPR
- Example or case study – Video on patient Recruitment Software
- Big Data and AI in the GDPR – Profiling (P) and Automated Decision-Making (ADM)
- General provisions and principles on P and ADM
- Specific Rules for ADM

Bird & Bird

Introduction

GDPR Context and Challenges

What?

- **New** European regulation 2016/679 reshaping the European framework on the protection of personal data
- Replaces Directive 95/46 and 28 national Data Protection laws
- Directly applicable in each Member State
- **New obligations** imposed on companies
  New rights for individuals

Who is concerned?

Any organization established in the EU or receiving EU data,
Any organization offering goods and services to EU residents

When?

25 May 2018 — GDPR entry into application

Why?

Fines for non-compliance up to 4% of worldwide global turnover

Bird & Bird

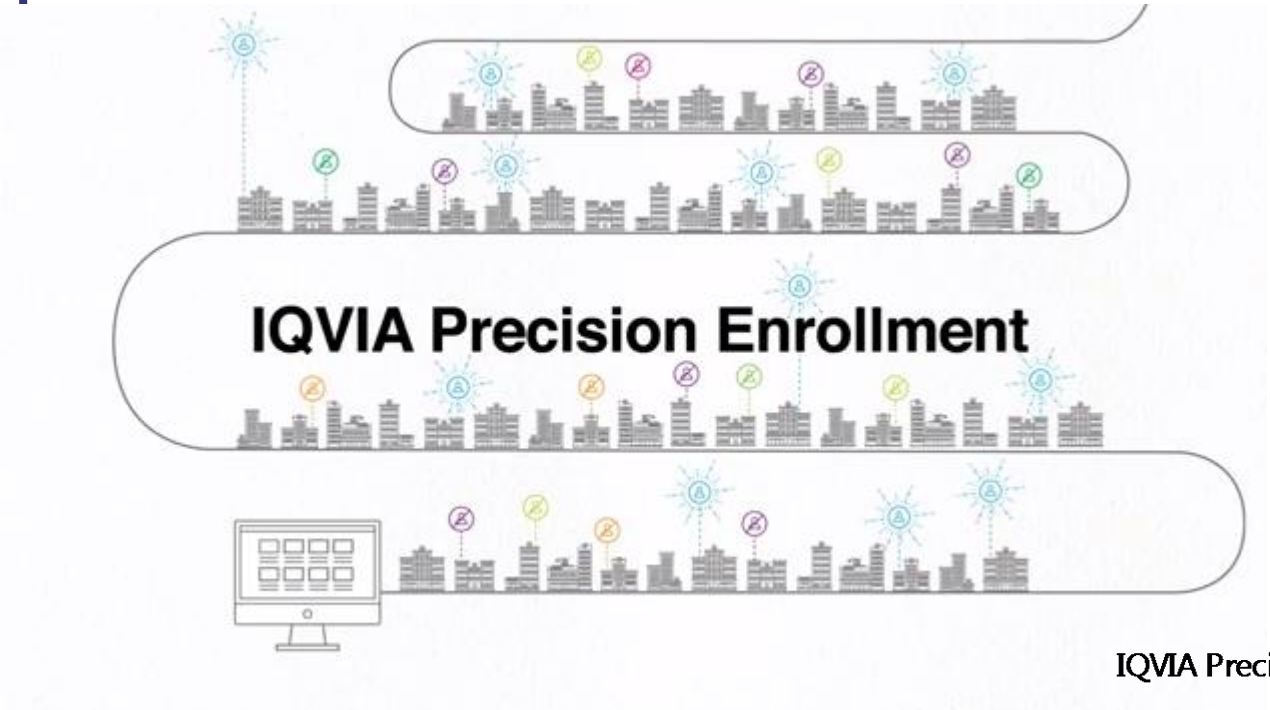
Personal Data

- Any information relating to an identified or identifiable natural person
  - directly or indirectly
  - 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
- the GDPR clarified that
  - genetic data
  - location data and
  - online identifiers may also be personal data

Example

Patient Recruitment Services

Example



IQVIA Precision Enrollment.mov

https://www.iqvia.com/solutions/research-and-development/patient-recruitment

Bird & Bird

Big Data and AI in the GDPR

Profiling and automated decision-making

Automated decision-making and profiling – different legal frameworks

Profiling Art. 4(4) means any form of automated processing of personal data consisting of the use of personal data to evaluate, analyse or predict aspects concerning individual's

- performance at work
- economic situation
- **health**
- personal preferences
- interests
- reliability
- behaviour
- location or movements

Principle

Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles." GDPR – Recital 72 "

Bird & Bird

Automated decision-making and profiling – different legal frameworks

What is automated decision-making?

(1) Processing is based *only* on automated processing,

(2) Without human intervention and

(3) Processing produces a legal effect or a similarly significant effect on the individual

What are the principles - Art. 22 ?

1. As a rule: prohibition
2. There are exceptions
3. There should be measures in place to safeguard the data subject's rights and legitimate interests

Bird & Bird

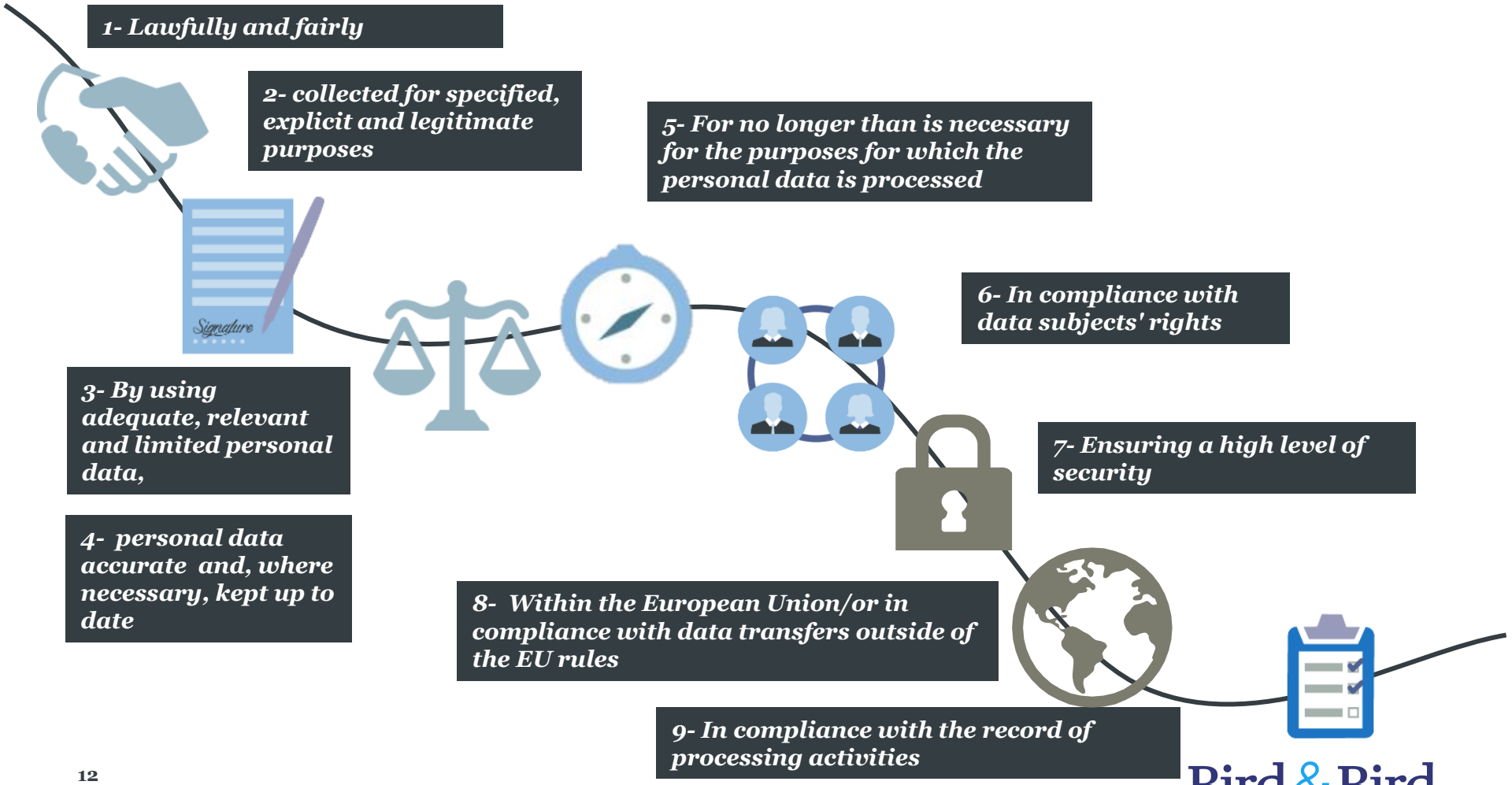
Principles applicable on Profiling and Automated Decision-making

See ARTICLE 29 DATA PROTECTION WORKING PARTY

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 – adopted on 3 October 2017

Data Protection Principles

Obligation to process personal data:



Bird & Bird

Anonymous or pseudonymous data?

- **Anonymous data**
  - Data rendered anonymous in such a way that the person is not or no longer identifiable
  - Does not relate to an identified or identifiable person

    (not personal data)
  - De-anonymisation through combination with other sources

- **Pseudonymous data**
  - the GDPR recognises for the first time
  - Processing in such a way that the data can no longer be attributed to a specific data subject without the use of additional information
  - Still personal data
  - Risk mitigation tool

Lawful processing

Processing only lawful if:

- Data subject has given consent
- Necessary for the performance of contract or to take steps prior to entering into a contract
- Necessary to protect vital interests of data subject
- Necessary for legitimate interests of controller or 3rd party (balance against the interests and fundamental rights of data subject)

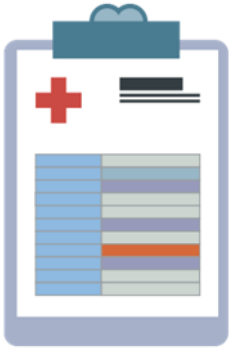
- Necessary for compliance with legal obligation to which the controller is subject
- Necessary for task carried out in the public interest or exercise of official authority

MS are allowed to maintain or introduce national provisions to further specify the application of these rules (Recital 8)

- Special regime for "Sensitive data"

Bird & Bird

Processing of **Sensitive (incl. Health) data is prohibited**



Unless

- Data subject has given explicit consent
- Necessary for obligations/rights in employment, social security & social protection law
- Necessary to protect vital interests of data subject
- Data manifestly made public by data subject
- Necessary for establishment, exercise or defence of legal claims
- Necessary for substantial public interest (under EU or Member State law)
- Necessary for preventive or occupational medicine, assessment of working capacity, medical diagnosis, healthcare (MSL or C with HCP)
- Necessary for public health (MSL)
- Necessary for archiving, scientific/historical research or statistical purpose (MSL + art 89 safeguards)

- MS may introduce further conditions for processing genetic, biometric or health data
- Profiling can create sensitive data by inference from and combination / correlations of non-sensitive data

New rights for individuals

Data subjects are given new rights pursuant to the GDPR

- Right to portability of data *(under conditions)*
- Right to restriction of data processing
- Right to erasure / "Right to be forgotten
- Right to object to profiling

In addition to existing rights:

- Right of access
- Right of rectification
- Right of information

- **Controllers** must respond within 1 month from receiving the individual's request + 2 months in case of a complex request (Art.12-3, but then the data subject must be informed of this and of the reasons why the request is complex
- **Processors** must assist the Controller for responding to requests from data subjects: access, rectification, suppression, restriction, objection, portability

GDPR & research
Rights of individuals and exceptions

- **Information obligations** (Art 13 and 14)
  - Exception for scientific research if data not obtained directly from data subject impossible
    - Proves impossible (e.g. deceased data subject)
    - disproportionate
    - likely to render impossible or seriously impair objectives
  - Controller takes appropriate measures – safeguards art 89
- Principle : **right to object** to processing for scientific research (Art.21(6))
  - Exception – processing of a task of public interest
- Right to be **forgotten**, right of **access**, right to **rectification** and **erasure**, **restriction** of processing, right to **data portability**

Bird & Bird

Data Protection Officers under the GDPR

- The GDPR obliges certain organisations to appoint a DPO:

- Other organisations **may** appoint a DPO.
- Groups of undertakings may appoint a **single** DPO providing they are **accessible** from each establishment.
- A **single** DPO may also be designated for multiple public authorities/bodies.

Bird & Bird

Specific framework for Automated decision-making

Automated decision-making and profiling – different legal frameworks

What is automated decision-making?

(1) Processing is based *only* on automated processing,

(2) Without human intervention and

(3) Processing produces a legal effect or a similarly significant effect on the individual

What are the principles - Art. 22 ?

1. As a rule: prohibition
2. There are exceptions
3. There should be measures in place to safeguard the data subject's rights and legitimate interests

Bird & Bird

Rights in relation to automated decision making – Exceptions to prohibition

The right	Unless processing is.....	For sensitive data...
• *"Not to be subject to decision based solely on automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"*	Necessary for entering into / performance of contract between controller & subject ; **or** Data subjects explicitly consents; **and** Controller implements measures to safeguard data subject rights, freedoms and legitimate interests **OR** Authorised by MS law which lays down safeguards for data subject rights	• Must, in addition, be suitable measures to safeguard data subject rights; and either • Data subject explicitly consents; or • Processing is necessary for reasons of substantial public interest on the basis of EU / MS law which is proportionate to the aim pursued, respect s the essence of the right to data protection and provides for ***suitable and specific measures*** to safeguard ***fundamental rights*** and data interests of subject

Bird & Bird

The right not to be subject to a decision based solely on automated processing

Data subject rights:

- Right to be informed / of access of the existence of automated decision-making, including profiling (13(2) (f) and 14(2)(g)
  - tell the data subject that they are engaging in this type of activity;
  - provide meaningful information about the logic involved; and
  - explain the significance and envisaged consequences of the processing
- Right to obtain human intervention (additional layer of protection)
- Right to express his point of view and contest the decision

Controller must establish appropriate Safeguards

- European Data Protection Board (EDPB) guidance!

Bird & Bird

Thank you & Bird & Bird

marc.martens@twobirds.com