AXON
science based lawyers

RANKED LEADERS IN THEIR FIELD
CHAMBERS EUROPE 2014

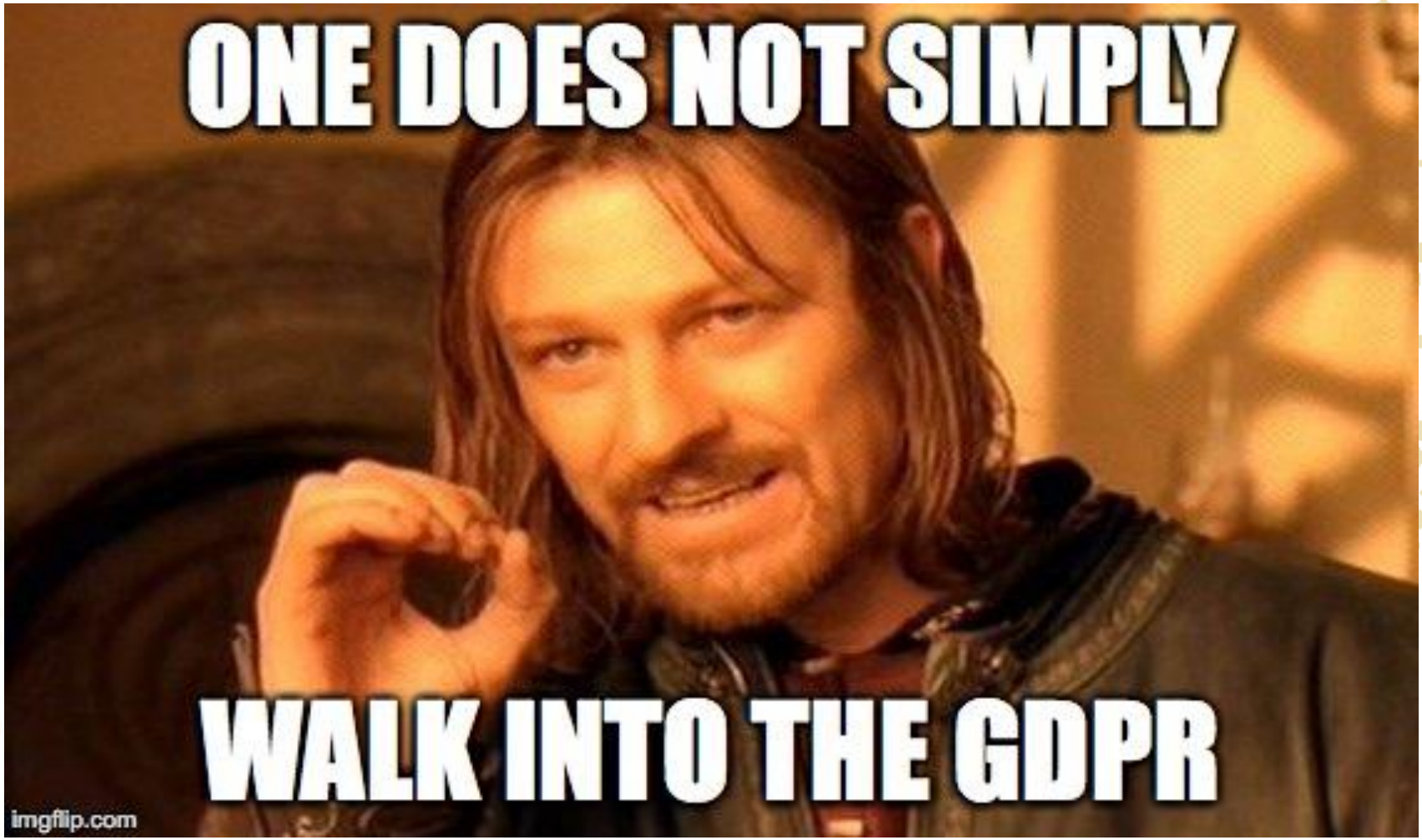
GDPR IN PERSONAL CONNECTED HEALTH: THE HATEFUL EIGHT

Die Folgen der neuen EU Datenschutz–Grundverordnung für den eHealth-Sektor - Akuter Handlungsbedarf?
23 May 2017

health
food
technology

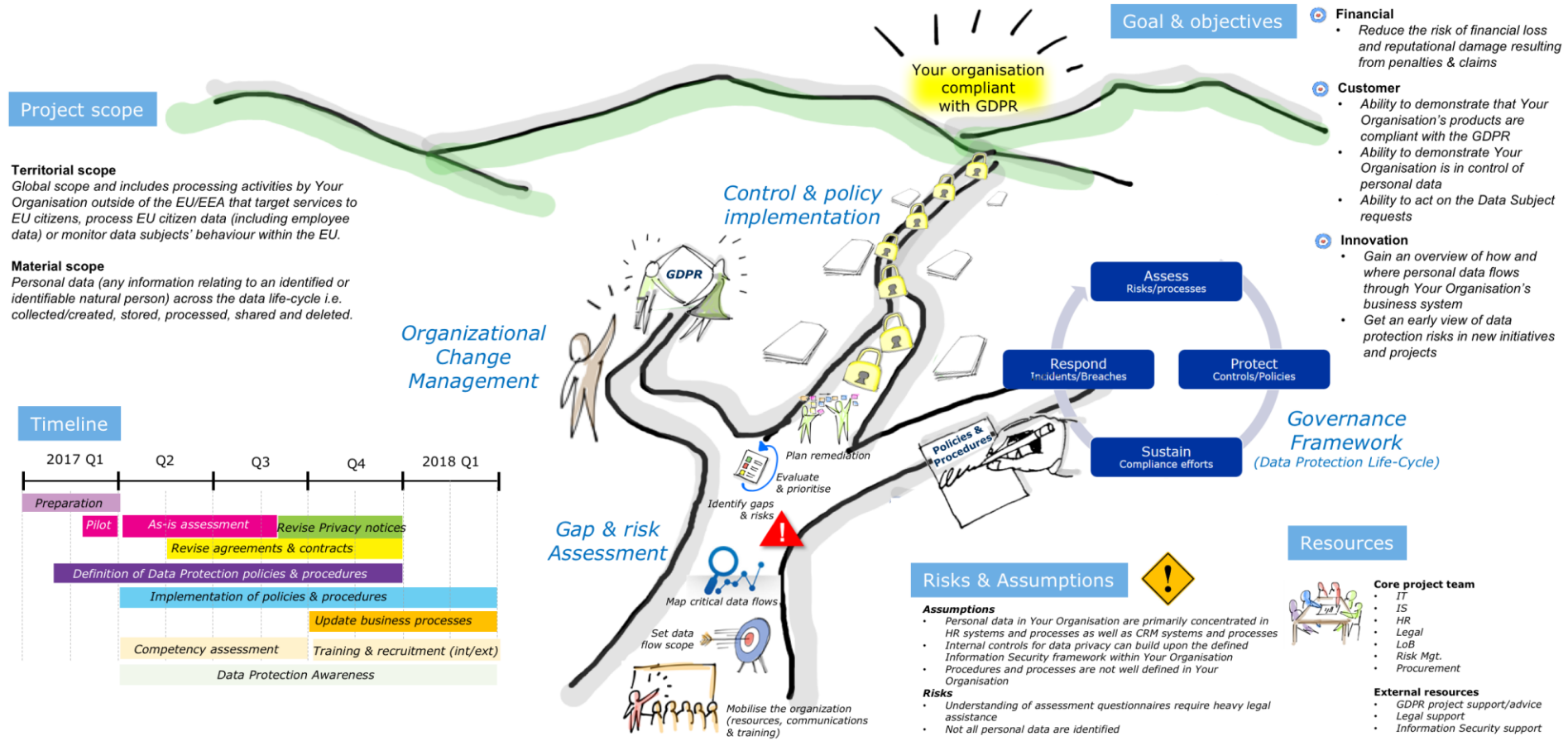
Erik Vollebregt
www.axonadvocaten.nl

“only” 88 pages, but:

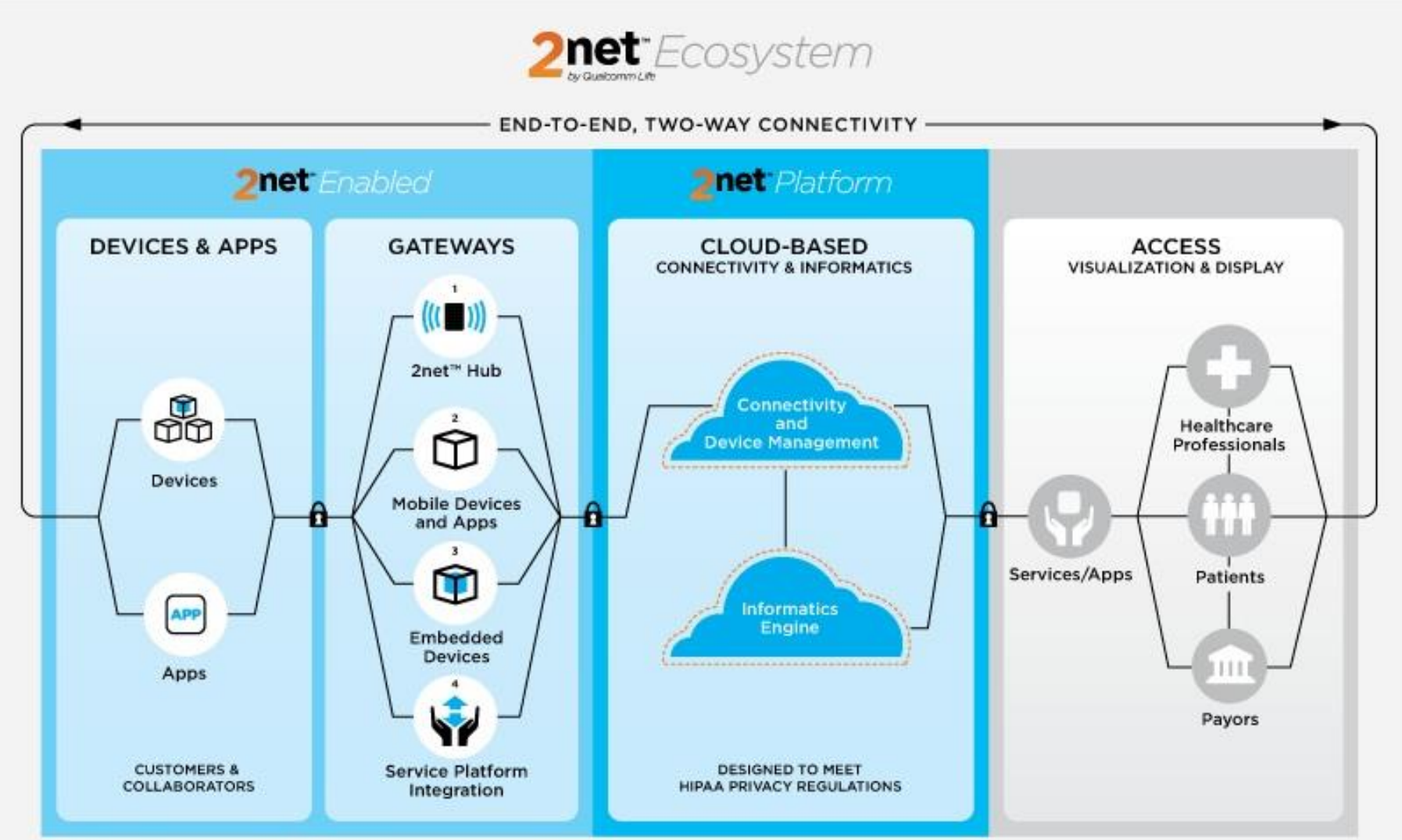


Looks familiar?

GDPR Project Game Plan



Medical device as or part of a service



Health data case study

- DPAs already take expansive view of health data
- Performance data becomes health data

Dutch DPA finds fitness app violates data protection law

The Dutch Data Protection Authority (College bescherming persoonsgegevens, hereinafter 'CBP') published a report on 11 November following an investigation into Nike's fitness app, the Nike+ Running app. The CBP found several violations of data protection law, according to its nearly hundred-page report. The report is interesting in that it provides detailed insight into how the Dutch Data Protection Authority views personal data concerning health and the thought processes behind the concept of health data, as Sofie van der Meulen and Erik Vollebregt of Axon Lawyers explain.

● Nike has no legal basis to process and use other information that is obtained from the smartphone, such as location information and contact information. Although Nike does inform users in more general terms about the processing and use of their data and asks for permission for the use of data, this information is not sufficient to establish informed consent. Based on the provided information, users are not able to determine the scope of the use of their data and cannot establish exactly what they give permission for. Therefore, there is no legally valid consent as a basis for the processing of personal data.

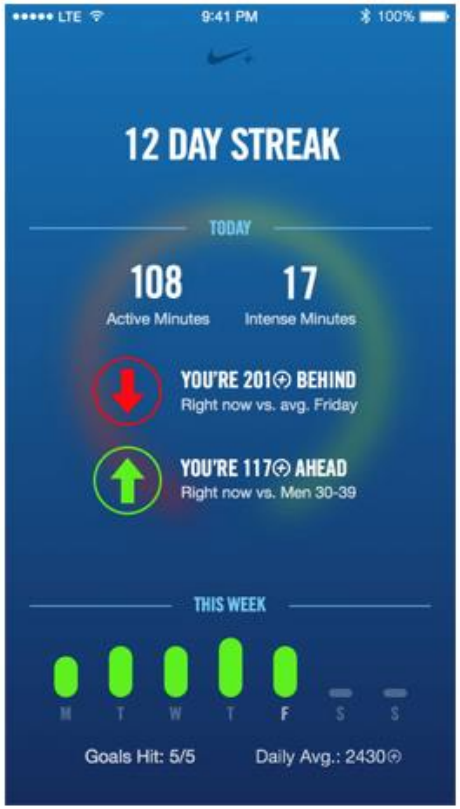
Does Nike process health data?

The Nike+ Running app is the first

time is created of all registered and calculated data for a specific user. Thus Nike has access to the sporting performance of a user over time. With this insight, Nike can conclude whether the physical condition of a user improves or deteriorates. According to the CBP, such information on a person's physical condition qualifies as health data as it provides information about the health of the user. The indefinite retention of the obtained data forms another factor to qualify the obtained data as health data because it allows a profile to be built up over time.

The deduced effect of practising sports on a person's condition: health data

Nike disagreed with the



Connected health related top 8 points of attention

1. Informed consent criteria
2. Data concerning health scope
3. Right to be forgotten (applies to commercial collection of health data)
4. Privacy by design)
   - For large scale processing of data concerning health
   - In case of profiling
5. Profiling requirements
   - including right to object if processing significantly affects data subject
6. Data portability right of user
7. Security requirements
8. Export of data to extra-EU jurisdictions

Consent-based business model tricky

‘GDPR: *‘means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’*

Recitals 32, 42 and 43 GDPR

- silence, pre-ticked boxes or inactivity do not constitute consent
- Processing for multiple purposes? Consent should be given for all of them!
- Controller must be able to prove valid consent was obtained and provide intelligible consent language
- Consent invalid “in a specific case where there is a clear imbalance between the data subject and the controller”

Future scope of ‘health data’

(15) ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council ([1]) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Research – ‘Right to be forgotten’

Article 17 (1) GDPR: The data subject has the right to obtain the erasure of personal without undue delay from the controller.

The ‘right to be forgotten’ **ONLY** does not apply if the processing takes place:

*‘for archiving purposes in the public interest, **scientific or historical research purposes or statistical purposes** in accordance with **Article 89(1)** in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing.’ (article 17 (3) (d)*

Right to be forgotten does apply in all commercial processing of health data for the purpose of services!

Privacy by design and default, PIAs

The Directive	The Regulation
	Art.25
Privacy by design and by default – General Principle: The concepts of privacy by design and by default are not explicitly addressed in the Directive.	**Data Protection by design and by default – General Principle:** When designing a processing system, and when using that system to process data, controllers must implement appropriate technical and organisational measures to protect the rights of data subjects and ensure compliance with the Regulation. Businesses must ensure that, by default, data processing activities are limited to the minimum necessary for the purpose.
	Art.35
DPIAs – General Principle: DPIAs are not explicitly addressed in the Directive, although several national DPAs recommend that a DPIA be undertaken in certain circumstances.	**DPIAs – General Principle:** The controller is required to perform a DPIA in the event that the relevant processing operations present high risks to the rights and freedoms of the data subjects. DPIAs are always required where the processing involves: • systematic evaluation of personal characteristics, including Profiling, on which decisions concerning individuals that produce legal effects are made; • processing special categories of data on a large scale; or • systematic monitoring of a publicly accessible area on a large scale.
DPIAs – Scope: DPIAs are not explicitly addressed in the Directive.	**DPIAs – Scope:** The Regulation provides a non-exhaustive list of processing activities that require a DPIA. This list includes: • systematic Profiling activities (see page 22); • processing of information in the special categories; and • large-scale surveillance in public areas. SAs can add to this list, and can require controllers to carry out a prior consultation and a DPIA.
DPIAs – Content: The content of DPIAs is not explicitly addressed in the Directive, although some national DPAs have issued guidance, and the WP29 has issued DPIA frameworks for RFID applications and Smart Meters.	**DPIAs – Content:** A DPIA should contain: • a description of the processing activities being assessed; • an assessment of the risks to data subjects; and • a description of the measures the controller will take to address these risks, including the safeguards, security measures and mechanisms that the controller will implement to ensure compliance with the Regulation.

Impact Assessment

Article 35

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

- PIA prior to processing
- Authorities will make lists of operations subject to PIA
- Prior consultation of DPA regarding residual risks (article 36)

Impact Assessment

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Profiling requirements

- Profiling based on health data -> always PIA
- 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- Data subject must be informed
- Article 22: right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, unless
    - decision is necessary for performance or entering into contract
    - decision is based on explicit consent

    - AND:
        - explicit consent in case of profiling based on health data
        - suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place

Data portability right

- Controller must inform data subject about right, and:

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

   (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

   (b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

Right to receive data

Right to have data transferred

Security

Data controllers and processors should implement appropriate technical & organizational measures to protect data from loss or any form of unlawful processing

- Article 32 defines security principles

Security measures must take into account (recital 78):

- Nature of the data to be protected and consequences of security breach
- State of the art
- Security by design
- Aim to prevent unnecessary collection and further processing of personal data
- Overriding principle: Plan-Do-Check-Act

- Data breach notification (article 33/34)
  - to DPA (<72 hours) and to data subject
  - processor must inform controller

Export

Chapter 5

Export only with legal basis:

- Adequacy decision (or Privacy Shield)
- Appropriate safeguards (BCR and SCCs) ensuring third party rights for data subjects, approved code or certification mechanism
- Specific situation
  - informed consent
  - necessary for performance of contract

Known unknowns and wide open doors

Article 9

Processing of special categories of personal data

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

- This means that member states can still require geofencing, hosting accreditation and things like that for processing of genetic, biometric and/or health data!
- Only restriction is that these cannot be contrary to the requirements of the internal market and must be proportionate

THANKS FOR YOUR ATTENTION

Erik Vollebregt
Axon Lawyers
Piet Heinkade 183
1019 HC Amsterdam
T +31 88 650 6500
M +31 6 47 180 683

E erik.vollebregt@axonlawyers.com
@meddevlegal
B http://medicaldeviceslegal.com

READ MY BLOG:
http://medicaldeviceslegal.com

AXON
science based lawyers

www.axonlawyers.com