

# MAINSTREAMING PERSONALISED HEALTH


Axon Seminar  
Amsterdam, 6 March 2019

health  
food  
technology

Karin Verzijden  
[www.axonlawyers.com](http://www.axonlawyers.com)

## Agenda

- What is Personalised Health?
- Specific GDPR requirements for data concerning health
- Interplay between CTR and GDPR
- International transfers of personal data
- EU GDPR enforcement so far



2

## What is Personalised Health?

### Why Fitbit?

See how people around the globe have changed their lives with Fitbit

Fitbit motivates you to reach your health and fitness goals by tracking your activity, exercise, sleep, weight and more.



3

## What is Personalised Health?

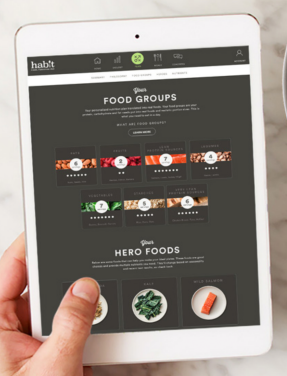
**habit**  
FOOD, PERSONALIZED

HOW IT WORKS TEST RESULTS SCIENCE FRESH MEALS SUCCESS STORIES [SHOP NOW](#)

**Find out what foods  
your body needs to  
be its best.**

Now you can get a personalized nutrition plan to match what you eat to your body's unique make-up.

[SHOP NOW](#)



4

## What is Personalised Health?

The cerascreen® Tests

Self tests for every situation!



Tests for vitamin deficiencies, food allergies, hormones and much more! Testing at home is quite simple.

**Our special offer for 1st time customers:**

Use **NEW18** at checkout and get **18%** off your first purchase! (50 £ minimum order value)

[View all tests](#)



5

## GDPR – Regulation 2016/679

**The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years.**

The regulation will fundamentally reshape the way in which data is handled across every sector, from healthcare to banking and beyond.

6

## GDPR – Regulation 2016/679

### Why has the GDPR such a large impact?

#### Broad territorial scope:

GDPR applies to any processing of personal data of data subjects by controllers/processors:

- established in the EU;
- not established in the Union:
  - in view of products or services offered within the EU (whether or not for payment)
  - who are *monitoring* behaviour of data subjects within the EU.

Increased responsibilities for data controllers, in particular regarding data concerning health



7

## Specific GDPR requirements for health data

Special categories of personal data: Data concerning health / genetic data / biometric data

Main rule: for any type of processing personal data, an appropriate legal ground is required. For processing health data *specific legal grounds* need to apply. Examples:

- **Explicit consent has been obtained for one or more particular purposes**
  - Typically the ground retained in clinical trials re. *patient data*.
  - In the context of a clinical trial, explicit consent is not necessarily applicable to processing *study staff data*.
- **Processing is necessary for scientific research purposes**
  - Applies to fundamental research, applied research and privately funded research.

NB! MS may introduce further conditions, including limitations, re. processing of health data.

Example: art. 24 Dutch Implementing Act lists 4 cumulative grounds that should be met.

8



## Specific GDPR requirements for health data

Imagine you are a CRO wanting to process (health) data for recruitment and participation in a clinical trial - **What do you need to do?**

- Processing recruitment data can be done based on contractual grounds.
- For processing health data in a clinical trial, it is advisable to obtain explicit consent.
- Operate two separate databases for volunteers for recruitment and patients / healthy volunteers actually participating in clinical trial.
- Rationale: enables you accommodating data subject requests, for instance requesting deletion of their data from the recruitment database.
- Put in place two dedicated privacy notices covering appropriate (health) data.
- When consent is requested: make sure you actually log it, for instance by a pdf form popping up when person fills in requested information.

9

## Specific GDPR requirements for health data

**Data protection impact assessment is mandatory** (amongst other grounds) **in case of:**

- processing health data on a *large scale*

**Designation of a data protection officer is mandatory** (amongst other grounds) **in case of:**

- core activities consisting of processing health data on a *large scale*

Guidance on large scale processing from Dutch DPA re. care sector (Dec. 2018)

- Hospitals, groups of GP's and healthcare insurance companies always process personal data on a large scale.
- Any other care provider processes personal data on a large scale if data of > 10.000 pp. are involved in one information system.

Can this guidance be applied to companies offering personalised health products?



AUTORITEIT  
PERSOONSGEGEVENS

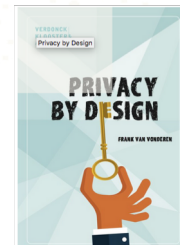
## Specific GDPR requirement for health data

When operating as a controller/processor, you need to set up **records of processing activities**.

Obligation to set up such record in principle applies to companies > 250 employees, unless the processing is **not occasional** or the processing includes **health data**.

- Name & contact details controller / its representative / DPO
- Purposes of processing
- Description of categories of data subjects / personal data / processing actions
- Categories of recipients to whom personal data will be disclosed
- If applicable, transfer of personal data to third countries
- Description of technical and organizational security measures

**Privacy by design** is of the essence here > reparation actions after Processing are hard to implement.



11

## Interplay between CTR and GDPR

### Generation of evidence

- Many evidence-based health products will be evaluated in clinical trials (food / meddev / pharma).
- The new Clinical Trials Regulation (536/2014) came into force, but is not yet applicable (expected 2020, depending on fully functional EU clinical trial portal).
- Both the CTR and the GDPR apply simultaneously; CTR containing specific provisions targeting clinical research, but *no derogations* from the GDPR.
- 23 January 2019: EDPB issued guidance on the interplay between the CTR and the GDPR



European Data Protection Board

Main focus: appropriate legal basis for processing personal data in clinical trials (primary use) & secondary use of clinical data for other scientific purposes.

12

## Interplay between CTR and GDPR

### Primary use of personal data

- Comprises all processing operations covering a specific clinical trial during its whole lifecycle.
- NB This concept has evolved: WP29 in its opinion on purpose limitation (03/2013) only considered in the initial collection of data as “primary use”.
- EDPB nevertheless distinguishes operations purely related to:

Category of processing activities	GDPR	Legal grounds for processing
(1) Research activities	Article 6	<b>Explicit consent</b> / task carried out in public interest / legitimate interest Controller
	Article 9	<b>Explicit consent</b> / public interest / scientific research purposes
(2) Protection of health	Article 6	Legal obligation of Controller
	Article 9	Public interest in public health

13

## Interplay between CTR and GDPR

### “Explicit consent” (GDPR)

- Not to be confused with “*informed consent*” under CTR.
- Should satisfy all statutory elements laid down for explicit consent:
  - (1) freely given > subject should be offered real choice; conditionality does not tick that box
  - (2) specific > subject should be made aware of impact of different choices (*granularity*)
  - (3) informed > who? / what? / right to withdraw consent (*transparency*)
  - (4) unambiguous > requires clear, affirmative action

> See WP29 Guidelines on consent, endorsed by EDPB on 25 May 2018

<b>Article 29 Working Party</b>
<b>Guidelines on consent under Regulation 2016/679</b>
Adopted on 28 November 2017
As last Revised and Adopted on 10 April 2018

14

## Interplay between CTR and GDPR

### Secondary use of clinical data

- Comprises the use of personal data for other scientific use than laid down in the Protocol.
- In principle, the use of personal data for secondary use requires an independent legal basis.
- However, EDPB seems to leave room for the application of the **principle of compatibility**: research outside the scope of Protocol could be considered compatible with initial purpose.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

15


## International transfers of personal data

### How to accommodate transfers of personal data outside EU?

- Bottomline: for any transfer outside the EU an *adequate level of protection* should be insured.
- (1) **Commission adequacy decision** covering those countries providing an adequate level of data protection. Examples: Switzerland, New-Zealand, Canada and Japan (# 18). US: only in as far as companies / organization adhere to EU/US privacy shield.
  - (2) **Binding corporate rules**: agreements applied by all members of a group / approved by competent authority / offering data subjects enforceable rights. Example: Philips.
  - (3) **Standard contractual clauses**: 3 sets of provisions agreed by the European Commission that can be implemented as such in f.i. data processor agreement.



Privacy Rules  
for Customer,  
Supplier and  
Business  
Partner Data



**EU Japan Adequacy Decision**

Fact sheet | January 2019

**Věra Jourová**  
Commissioner for Justice,  
Consumers and Gender Equality

**Directorate-General for  
Justice and Consumers**

**What happens to the personal data transferred from the EU to Japan?**

Japan has recently modernised its data protection law applicable to the private sector, bringing it closer to the European standards. Following the negotiations with the European Commission, the Japanese Government has adopted the Supplementary Rules applicable only to data transferred from the EU, thereby filling the remaining gaps.

**As a result, whenever the data travel from the EU to Japan, the same guarantees as those under the EU law will continue to apply.**

17

## International transfers of personal data

Imagine you are a health platform based in **Ireland**. You collect blood samples that are analyzed by a sub-contractor based in the **UK**. Analysis results will be sent back to Ireland.

**How to GDPR-proof this operation?**

- Data Processor Agreement needs to be concluded between Irish platform and UK sub-contractor.
- UK will become third country upon Brexit.
- As long as no adequacy decision re. the UK is in place, correct set of SCC needs to be added.

COMMISSION DECISION  
of 5 February 2010  
on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council  
(notified under document C(2010) 593)  
(Text with EEA relevance)  
(2010/87/EU)

18

## International transfers of personal data

### Contents 2010 SCC

- Define “data exporter” (Irish platform) and “data importer” (UK sub-contractor).
- To specified by the parties: categories of data subjects & data / processing operations.
- Exporter obligations: apply and specify appropriate technical & organisational security measures and see to it that data importer does the same.
- Importer obligations: process personal data in accordance with exporter’s instructions.
- Duty of information: data subject needs to be informed of transfer to third country.
- Liability: data subject is entitled to receive compensation from data exporter for damage suffered.
- Governing law: law of the country of data exporter.

19

## Information note on data transfers under the GDPR in the event of a no-deal Brexit

Adopted on 12 February 2019



When transferring data to the UK, you should:

- 1 • Identify what processing activities will imply a personal data transfer to the UK
- 2 • Determine the appropriate data transfer instrument for your situation (see below)
- 3 • Implement the chosen data transfer instrument to be ready for 30 March 2019
- 4 • Indicate in your internal documentation that transfers will be made to the UK
- 5 • Update your privacy notice accordingly to inform individuals

20



## Processing personal data



### How about GDPR enforcement so far?

- September 2018: 1<sup>st</sup> fine of € 4.800 imposed by Austrian Data Protection Authority to online gambling business monitoring large part of public space with camera attached to its premises.
- October 2018: 2<sup>nd</sup> set of fines imposed by Portuguese Data Protection Authority on hospital upon inspection for not respecting patient confidentiality (€ 300.000,00) and for the inability to ensure data integrity into its system (€ 100.000,00).
- Jan. 2019: 3<sup>rd</sup> huge fine by French Data Protection Authority directed against Google for lack of transparency, inadequate information and lack of valid consent for ads personalisation.

### **The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC**

*21 January 2019*

## EU GDPR enforcement so far



### Learnings from Google fine

- Google is offering a variety of services, including personalised ads fine based on geo-tracking.
- Complaint filed by 2 NGO's was twofold:
  - (1) Lack of transparency about personal data processing activities;
  - (2) Lack of a valid legal basis therefore.
- Ad (1) Not being transparent is a true deadly sin under the GDPR, that aims to empower citizens to take control over the processing of their personal data.
- Ad (2) Google claimed to operate on the basis of obtained consent, but this was neither specific (targeting each of the services offered), nor unambiguous (pre-ticked boxes).



## EU GDPR enforcement so far

### Enforcement in the NL

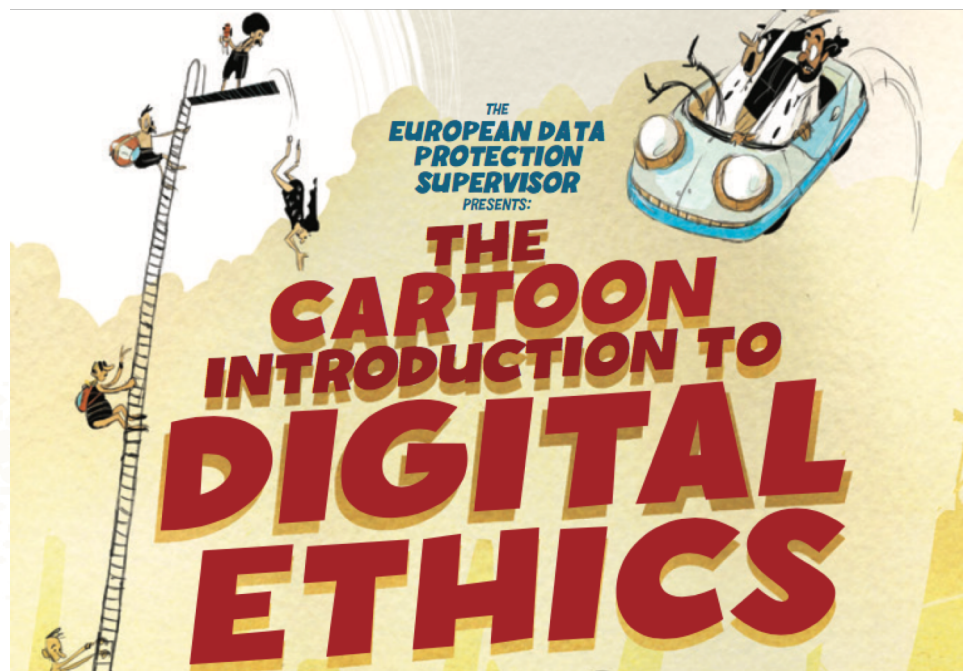
- So far, we have not seem major fines being imposed.
- Dutch DPA held a number of *exploratory investigations* re. specific items. It checked with a number of companies if they put in place a record of processing activities. And what did they exactly put into their Data Processor Agreements? How about the privacy policies of a number of hospitals (obviously dealing with data concerning health)? And did they appoint a DPO?
- November 2018: Police was received an order subject to an incremental penalty ("*last onder dwangsom*") for € 40K re. the access to a database containing Schengen data.

**Financieel Dagblad**  
31 January 2019

#### Optimistisch

De Autoriteit Persoonsgegevens zelf wil tegenover het FD niet vooruitlopen op eventuele geldstraffen. 'Er zijn zeker een aantal zaken ernstig genoeg om dieper in te duiken', zegt woordvoerder Martijn Pols. Wat passend optreden is, kan pas op termijn duidelijk worden. 'Maar is er dwang nodig, dan kan er een last onder dwangsom of boete volgen', aldus Pols.

23



24

## Conclusions



- In the field of personalised health, processing personal data in line with the GDPR is vital for your business.
- You are processing data concerning health, regarding which specific requirements apply. You are therefore under scrutiny of the competent authorities and customers get more and more demanding.
- So, do not obtain and keep more data than required for your business purposes, properly inform your client on the use of those data and put in place appropriate measures in order to safely process personal data and to be able to properly address client request.

**Appropriate data processing measures can be a competitive advantage!**



**Food Health Legal**  
legal and regulatory blog

25