

# Cybersecurity and the Law

## Introduction to Data Protection Law

Assoc. Prof. Sophie Stalla-Bourdillon, Director of Ilaws

@SophieStallaB

Blog: <https://peepbeep.wordpress.com/>

[s.stalla-bourdillon@soton.ac.uk](mailto:s.stalla-bourdillon@soton.ac.uk)

Seminar on 7 November 2016 at 11.00 B32 (level 4)  
coffee room

**“It's Too Complicated: How the Internet Upends Katz, Smith,  
and Electronic Surveillance Law”**

The paper “demonstrate(s) the urgent need for development of new rules and principles capable of regulating law enforcement access to IP-based communications data.”

# Cybersecurity and the Law

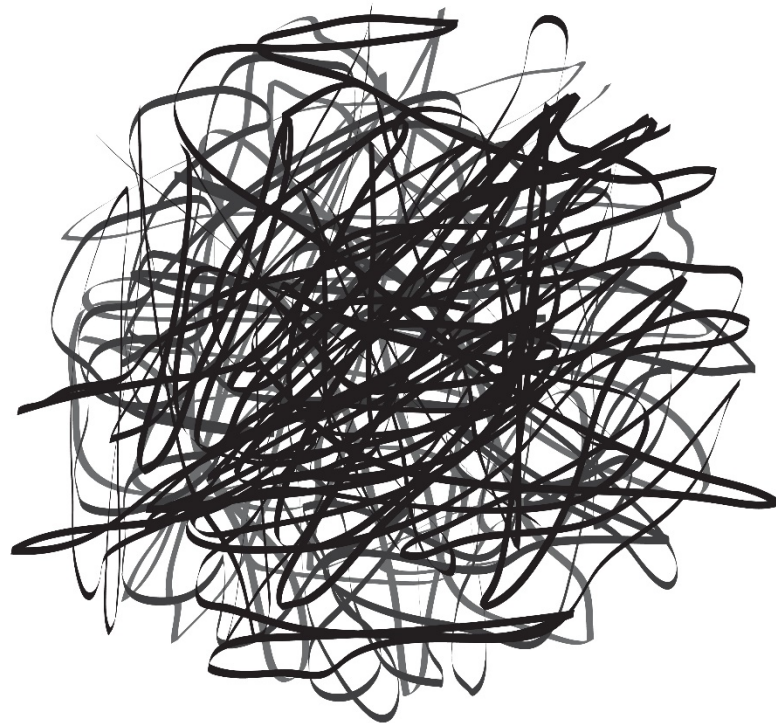
## Introduction to Data Protection Law

Assoc. Prof. Sophie Stalla-Bourdillon, Director of llaws

@SophieStallaB

Blog: <https://peepbeep.wordpress.com/>

[s.stalla-bourdillon@soton.ac.uk](mailto:s.stalla-bourdillon@soton.ac.uk)







It is better to understand  
little than to misunderstand  
a lot.

Anatole France

You have created an app to allow individuals to monitor their psychological condition. It collects information such as the time at which morning alarms are set, location of users (to determine whether they stay at the same location for a long period of time), the speed at which users speak during phone calls (but not the names, addresses or telephone numbers of users). Should you be concerned by data protection law?

# Starring: at the EU level



DP Directive 1995



Art. 29 WP



GDPR 2016



# Starring: at the UK level



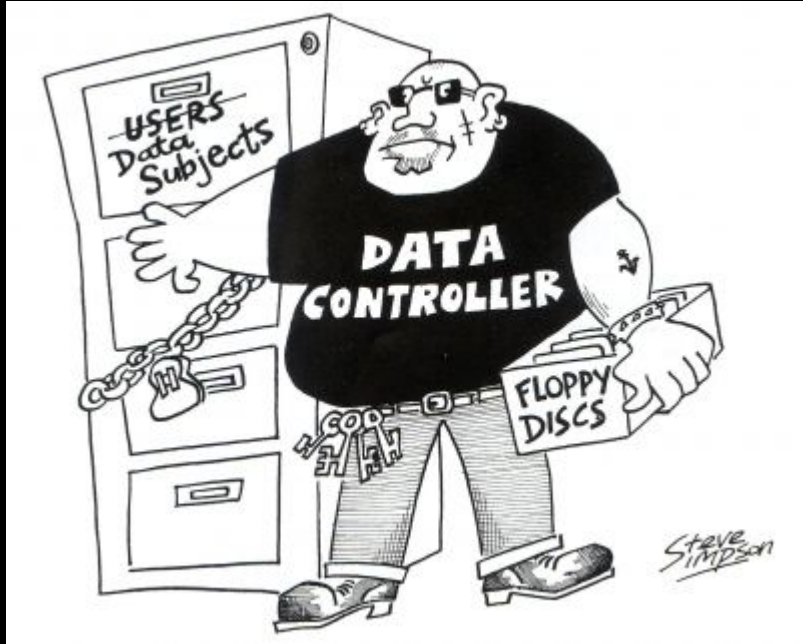
ICO



UK DPA 98

So what?

If Data Protection Law applies



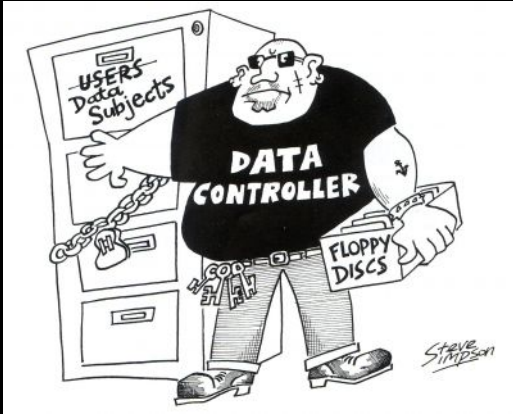
A **data controller** will have a certain number of obligations



As well as his **data processor**



A **data subject** will have a  
certain number of rights



The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data



An identified or identifiable natural person whose personal data are being processed (by the data controller)

1. You shall have a legitimate ground to process the data

2. You shall process the data for a specific and limited purpose

3. You shall only collect the data that are necessary to pursue this purpose

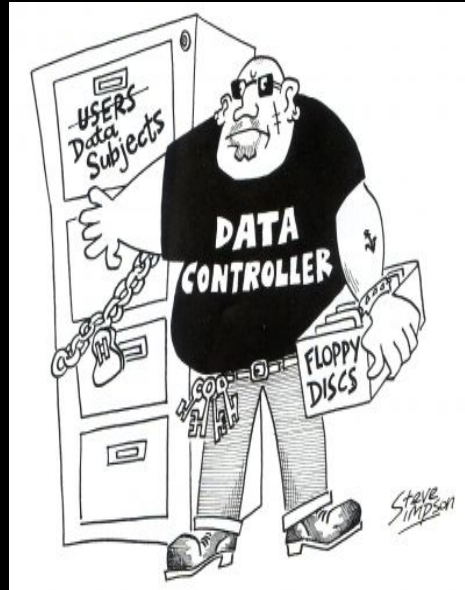
4. You shall keep the data for non longer than necessary

5. You shall only keep accurate data

6. You shall keep the data secure

7. You shall enable data subjects to exercise their rights

8. You shall notify the ICO that you are a DC



## Article 32 GDPR

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.

## Article 32 GDPR

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.



## Article 33 GDPR

1. In the case of a **personal data breach**, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
  - (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
  - (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - (c) describe the likely consequences of the personal data breach;
  - (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

1. You have a right to be informed (e.g. purpose of the processing)

2. You have a right to access data relating to you

3. You have the right to have the data rectified

4. You have the right to have the data erased if the processing is not legally compliant

5. You have a right to object to certain processing when not based on consent

6. You have a right not to be subject to a measure based on profiling

8. You have a right to data portability



When Big Data practices are applied  
to personal data....

Data protection law apply!

D'OH!







1. “Big data has been described as a phenomenon rather than a technology” (See Wiggins)
2. “Big data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making” (See Gartner)
  - “of the ‘three Vs’, **variety** is the most important characteristic of big data”

“if a company is analysing its own customer database, even if that database is particularly large, it may not necessarily raise any novel issues in terms of either analytics or data protection. However, when it combines its own information with data sourced **externally** (whether that be from a publicly accessible source or not), then it is doing something qualitatively different that can be called big data.”

ICO 2014



Ok, but what is  
personal data?

# Personal Data

any information relating to an identified or identifiable natural person ('data subject');

Ex: identification number, one or more factors specific to one's physical, physiological, mental, economic, cultural or social identity

GDPR: genetic data, biometric data, location data

to determine whether a person is identifiable, account should be taken of all **the means likely reasonably to be used** either by the controller or by any other person to identify the said person

# Personal Data

= data enabling the **singling out** of individuals

Ok, but what is  
an IP address?

Opinion of AG Campos  
Sanchez-Bordona in Breyer 12  
May 2016

It depends....

“Just as recital 26 refers not to any means which may be used by the controller (in this case, the provider of services on the Internet), but only to those that it is likely ‘reasonably’ to use, the legislature must also be understood as referring to ‘third parties’ *who, also in a reasonable manner, may be approached by a controller seeking to obtain additional data for the purpose of identification*. This will not occur when contact with those third parties is, in fact, very costly in human and economic terms, or practically impossible or prohibited by law. ” [68]



Does it really depend?

# Personal Data

→ non-sensitive

→ Sensitive



personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life

It is not because the data are publicly available that they are not personal data.



D'OH!






How many categories of personal data can you spot within this list: address, name, search terms entered into a search engine, email address, IP address, tweets, Facebook status.

- 1
- 2
- 3
- 4
- 5
- 6
- 7

Is 'John Smith' personal  
data?

# ICO



“By itself the name John Smith may not always be personal data because there are many individuals with that name”. [2012]



Is 'The tall, elderly man with  
a dachshund who lives at  
number 15 and drives a  
Porsche Cayenne' personal  
data?

# ICO



“There will be circumstances where the data you hold enables you to identify an individual whose name you do not know and you may never intend to discover”. [2012]

Is an address personal  
data?

# ICO



“if searching a public register or reverse directory would enable the individual to be identified from an address or telephone number, and this resource is likely to be used for this purpose, the address or telephone number data should be considered to be capable of identifying an individual”. [2012]

“A utility company may not record the name of the occupier of the house to which it provides water, but may simply note the address of the property and address all bills to 'the occupier’”.

Is the utility company dealing with personal data?

# ICO



“In this last example, even without a name associated with the water consumption data, this data will be personal data in that it determines what the occupier will be charged and the occupier is identified, even without a name, as the person living at the property in question and is therefore distinguished from other individuals. Also, if necessary, the water company is likely to be able to easily obtain the name of, if not the occupier, then at least the registered owner of the property. ”. [2012]

# Rephrase in your own words:

“Information about the market value of a particular house may be used for statistical purposes to identify trends in the house values in a geographical area. The house is not selected because the data collector wishes to know anything about the occupants, but because it is a four bedroom detached house in a medium-sized town”. ICO 2012

How to explain all of this?



# ICO



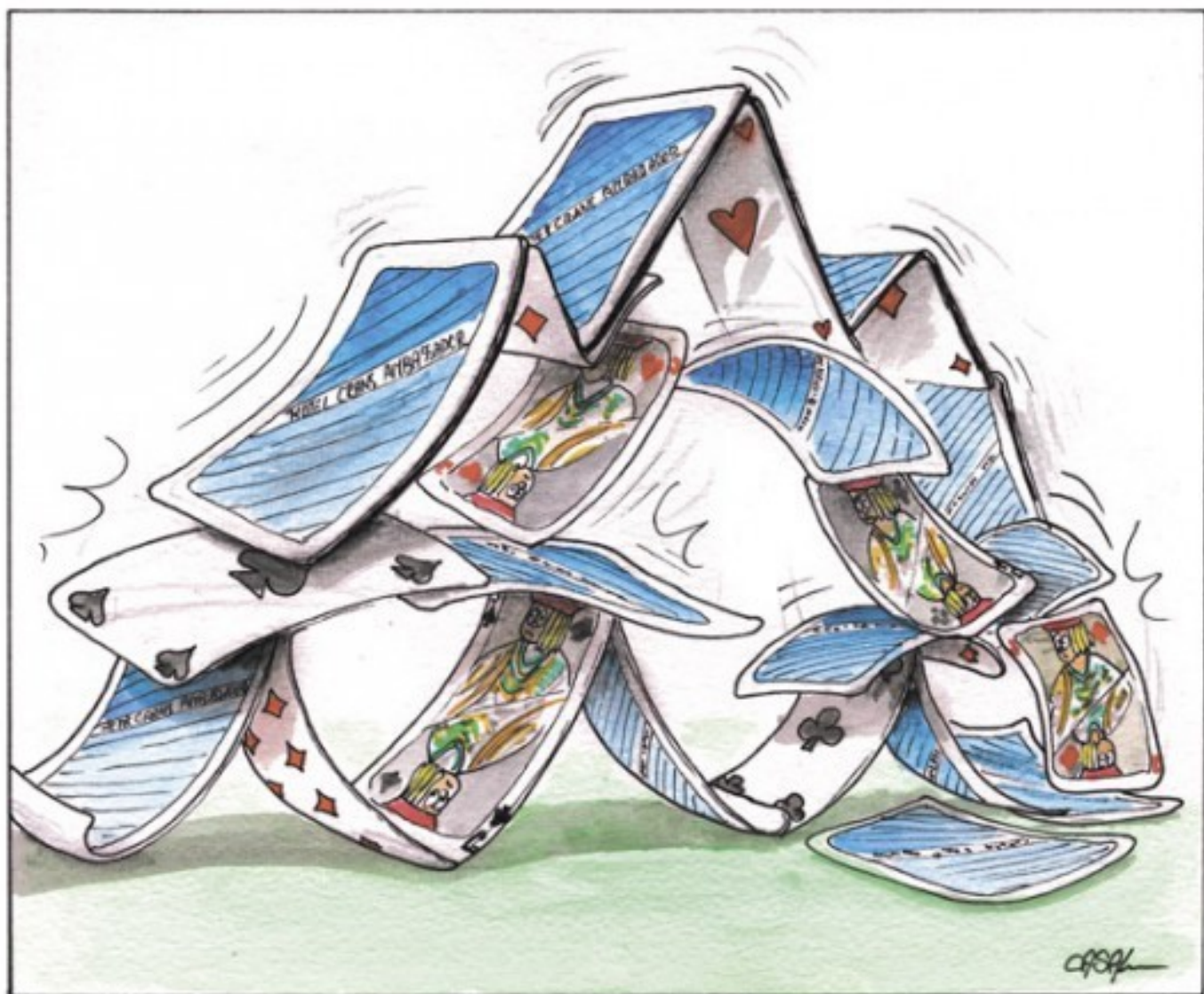
“the same piece of data may be personal data in one party’s hands while it may not be personal data in another party’s hands” [2012].

Not all hands are equal!

# ICO



“Whether information is linked to an individual, for example, **to learn something about that individual**, is the key factor in determining whether information about an object (for example, a biscuit-making machine) is personal data.  
” ICO [2012].



# ICO




“Even though the data is not usually processed by the data controller to provide information about an individual, **if there is a reasonable chance that the data will be processed for that purpose,** the data will be personal data”  
[2012].

ICO



“Though our guidance is structured differently we are satisfied that it is consistent with the approach taken by the Working Party”. [2012]



“in order to consider that the data “relate” to an individual, a **"content"** element OR a **"purpose"** element OR a **"result"** element should be present”. [2012]

Article 29 WP

# Personal Data

≠ is not anonymous data



the data subject is  
no longer  
identifiable



Is there such a thing as  
anonymous data?

The DPD in Recital 26 excludes “data rendered anonymous” from the scope of data protection law

“Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, **account should be taken of all the means likely reasonably to be used** either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous **in such a way that the data subject is no longer identifiable;**”

This means a risk-based approach,  
right?

Art. 29 WP 2014

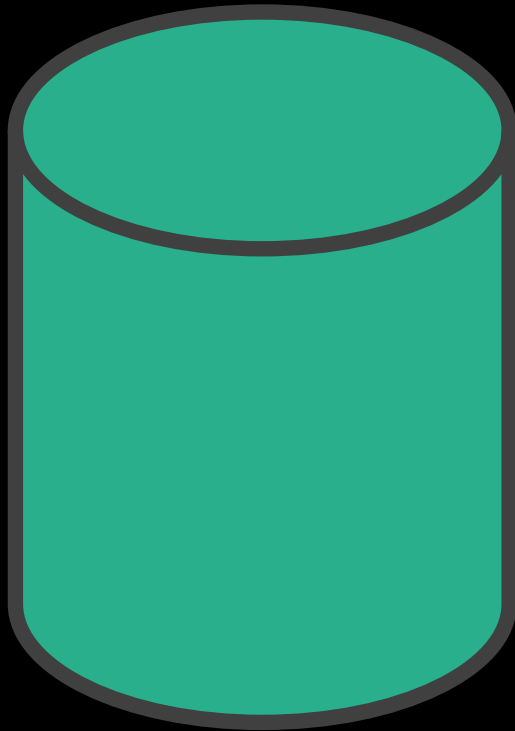
# Opinion on Anonymisation Techniques

“More precisely, the data must be processed in such a way that it can no longer be used to identify a natural person by using “all the means likely reasonably to be used” by either the controller or a third party. An important factor is that the processing must be irreversible”.

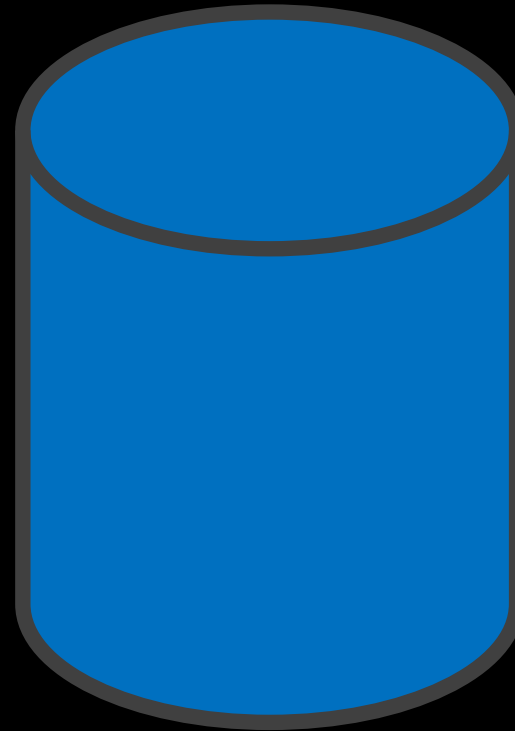
“it is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data”.

What?!?





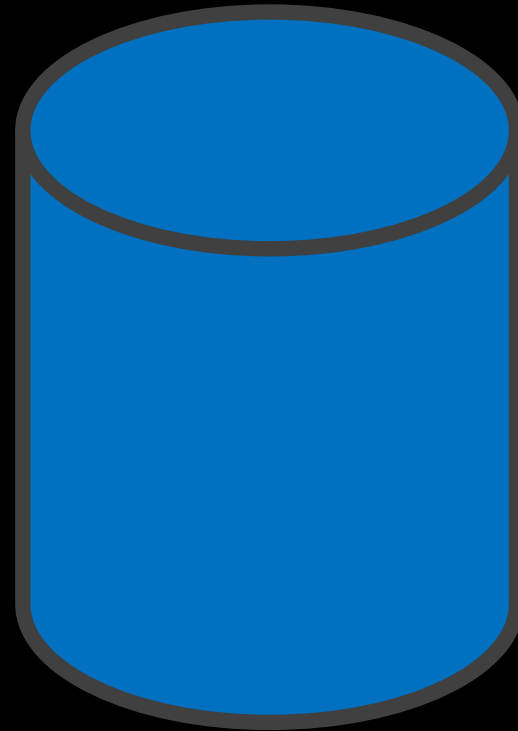
Raw dataset: identified or  
identifiable data subjects



Transformed dataset: de-  
identified data



Raw dataset: identified or  
identifiable data subjects



Anonymised dataset

Anonymous data is  
a very very rare species, is it?

Does everybody agree?

# Of course not!

- Common Services Agency v Scottish Information Commissioner [2008] UKHL 47
- ICO Code on anonymisation
- Queen Mary University of London v (1) The Information Commissioner and (2) Alem Matthees, EA/2015/0269

Does the GDPR  
solve the uncertainty/dispute?

Of course not!

The GDPR in Recital 26 excludes “anonymous information” from the scope of data protection law



“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;”

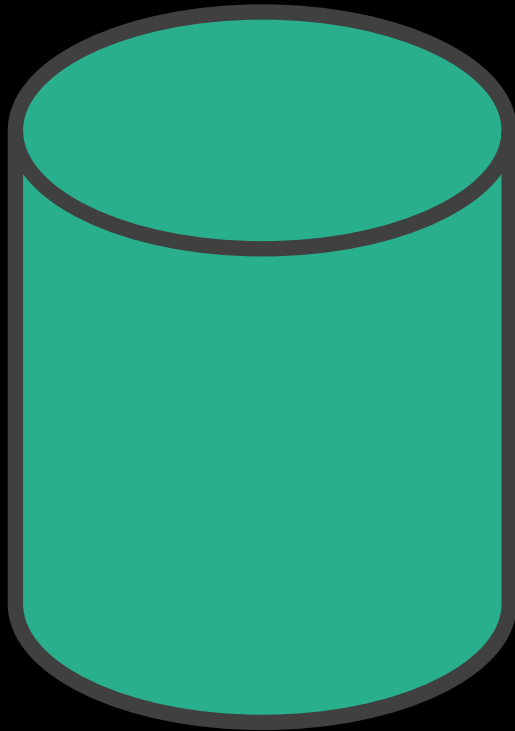
So far so good...

The GDPR equates data that has undergone  
pseudonymisation to personal data  
in Recital 26

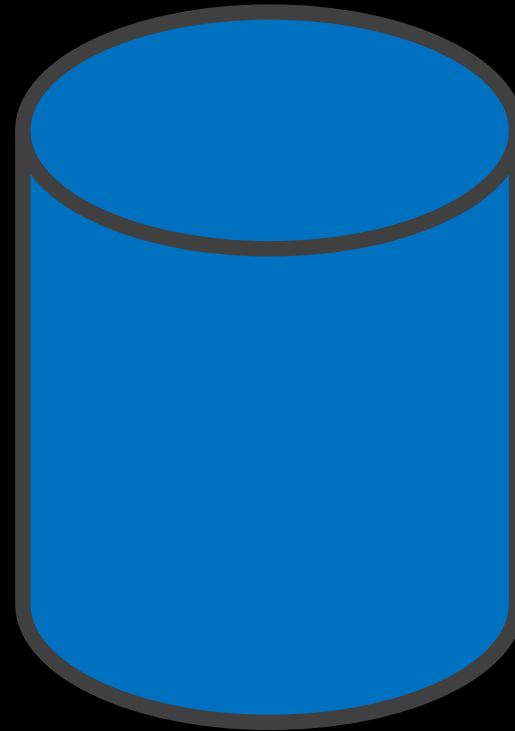
“Data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered as **information on an identifiable natural person**”.

The GDPR defines pseudonymisation in  
Article 4

“'pseudonymisation' means the processing of personal data in such a manner that the personal data **can no longer be attributed to a specific data subject without the use of additional information**, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;”



Raw dataset: identified or  
identifiable data subjects



Transformed dataset:  
Pseudonymised data

# Conclusion



# What are we protecting with data protection laws?

1. Intimate secrets
2. An ability to control one's personal data even when one interacts with others

# What is anonymised data?

1. Non-personal data
2. Personal data