

Technical consequences of data subjects' rights

**BERLIN
BUZZWORDS
2018** JUNE 10-12

Aurélie Pols – Berlin June 12th 2018

Hunt down your vendors and demand response
and capabilities early



Accountability

“un nuevo modelo que podemos decir que pasa de la gestión de los datos al uso responsable de la información”

José Luis Piñar Mañas

DERECHO ADMINISTRATIVO



**REGLAMENTO GENERAL DE
PROTECCIÓN DE DATOS**

Hacia un nuevo modelo europeo de privacidad

Data Governance & Privacy Engineer

Data is the New Electricity – Privacy is the New Green – Trust is the New Currency
Dutch nationality, French mother tongue, works in English, lives in Spain



2003:
OX2 Co-founder
Webanalytics.be
2008:
Sold to Digitas LBI
(Publicis)



- DPO for mParticle (Customer Data platform) – contractor (USA, New York)
- Chief Visionary Officer – Competing on Privacy
- Professor of Ethics & Privacy in Big Data & Business Analytics Master – Instituto de Empresa (IE), Madrid (ES); guest professor DPO certification courses Maastricht University, faculty of law (NL) & Solvay Business School Brussels (B)
- Board Member European Center On Privacy and Security, Maastricht University (NL)
- Ethics Advisory Group (EAG) – European Data Protection Supervisor (EDPS) [Towards a digital ethics](#)
- Former Vice-chair P7002 – Data Privacy Process – IEEE
- Speaker/writer/consigliere: Mobile World Congress, SWSX, Strata (+ Hadoop World), IAPP, Piwik, AT Internet, industry associations, AdTech & MarTech vendors, ...



AURELIE POLS,
DATA GOVERNANCE
& PRIVACY ENGINEER





Strata
DATA CONFERENCE

PRESENTED BY

O'REILLY

cloudera

"Start with the problem,
not with the data."

—Andreas Weigend

Which problem?

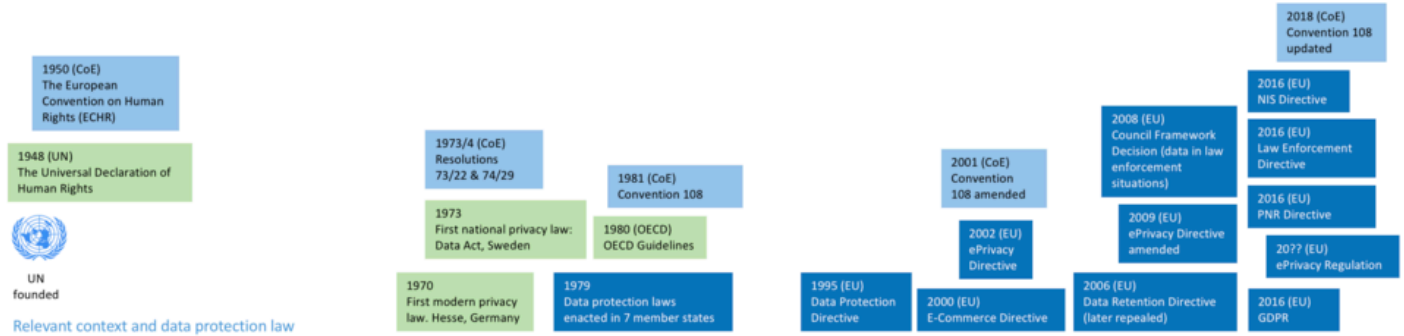
Do values influence the problems we choose to solve?

Or the society we live in, it's history...

The questions we are faced today

- Economic growth?
- What is happiness?
- Externalities to economic growth like pollution
- What is the future of work?
- Are incentives aligned to assure “human flourishing” and inter-generational solidarity?
- The rule of law is like La Sagrada Familia: eternally under construction





Relevant context and data protection law



European structural evolution



Evolution of technology

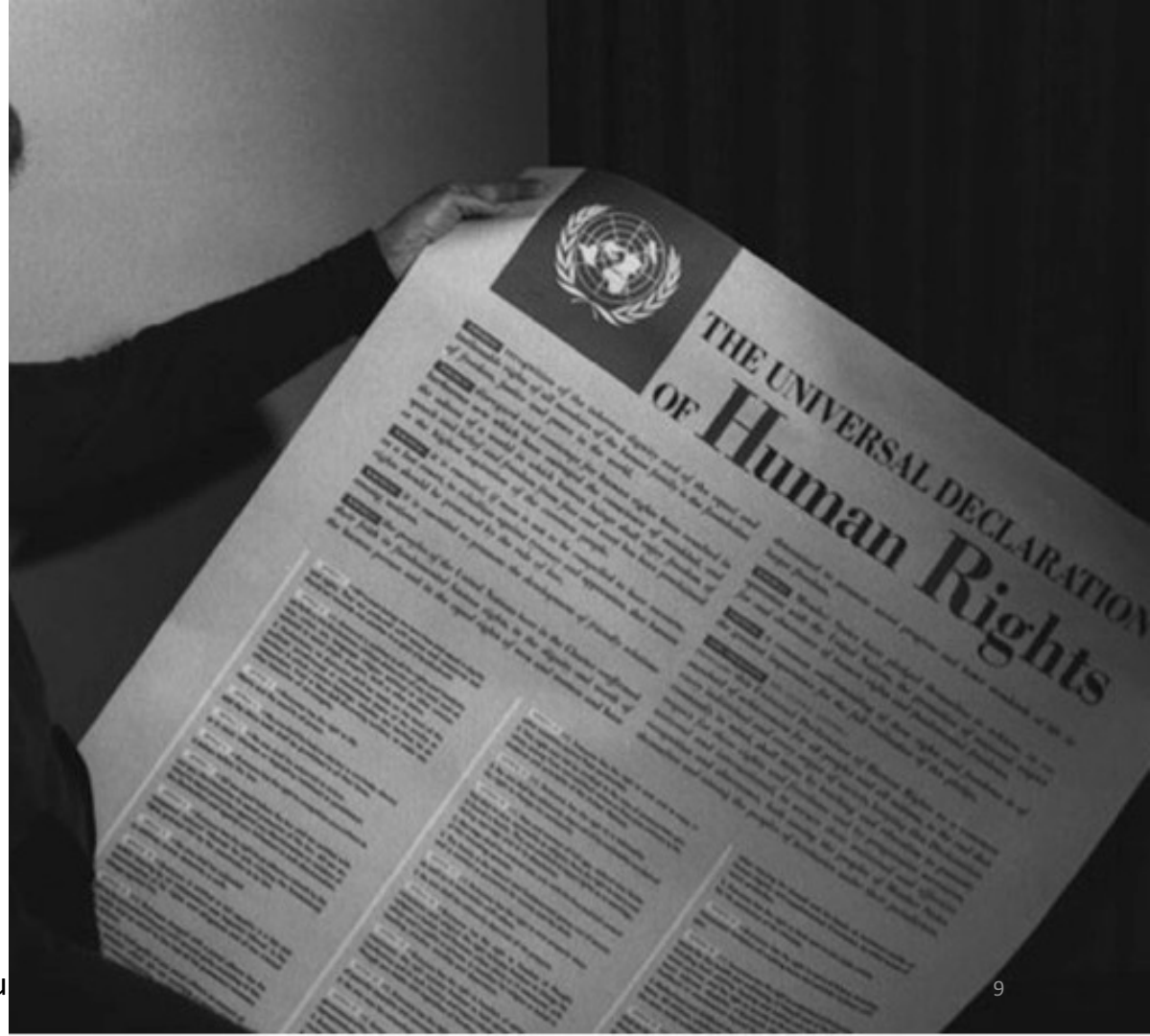


Society



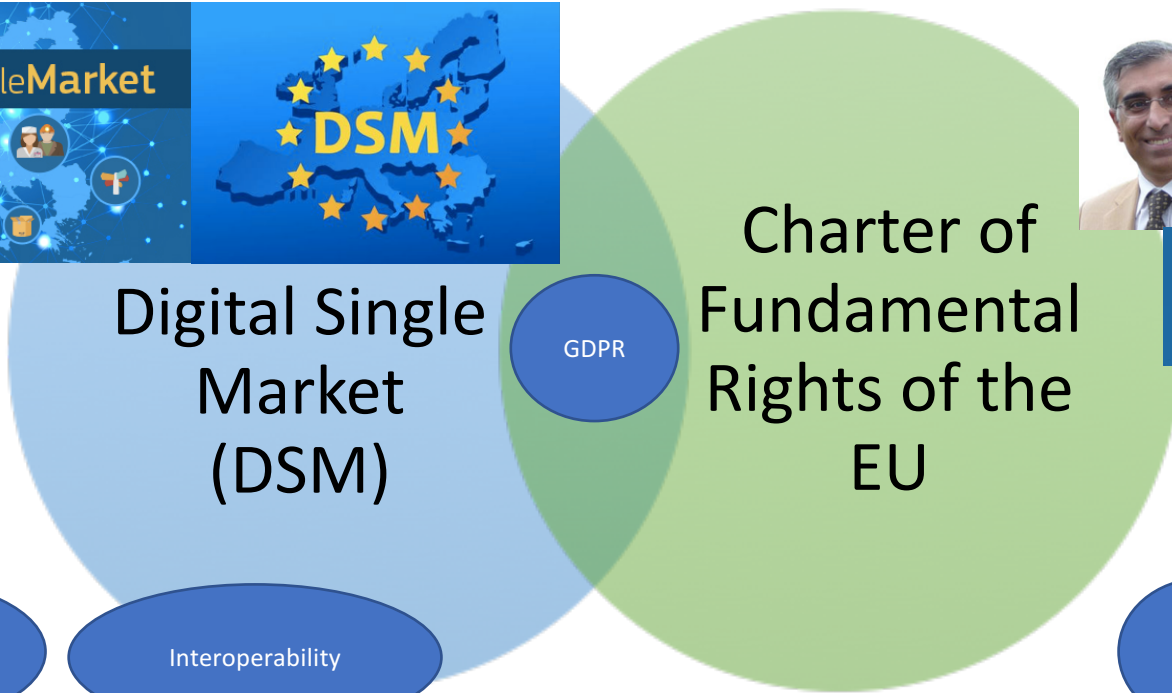
We are Data Subjects as

- Parents, Caretakers,
- Consumers, Customers,
- Citizens,
- Business Partners, Employees,
- Men and women,
- Young and old,
-



Economic development & human rights

The Right to Privacy in the Digital Age



Roaming

Geo-fencing/
copyright

Interoperability

PS2

ePrivacy

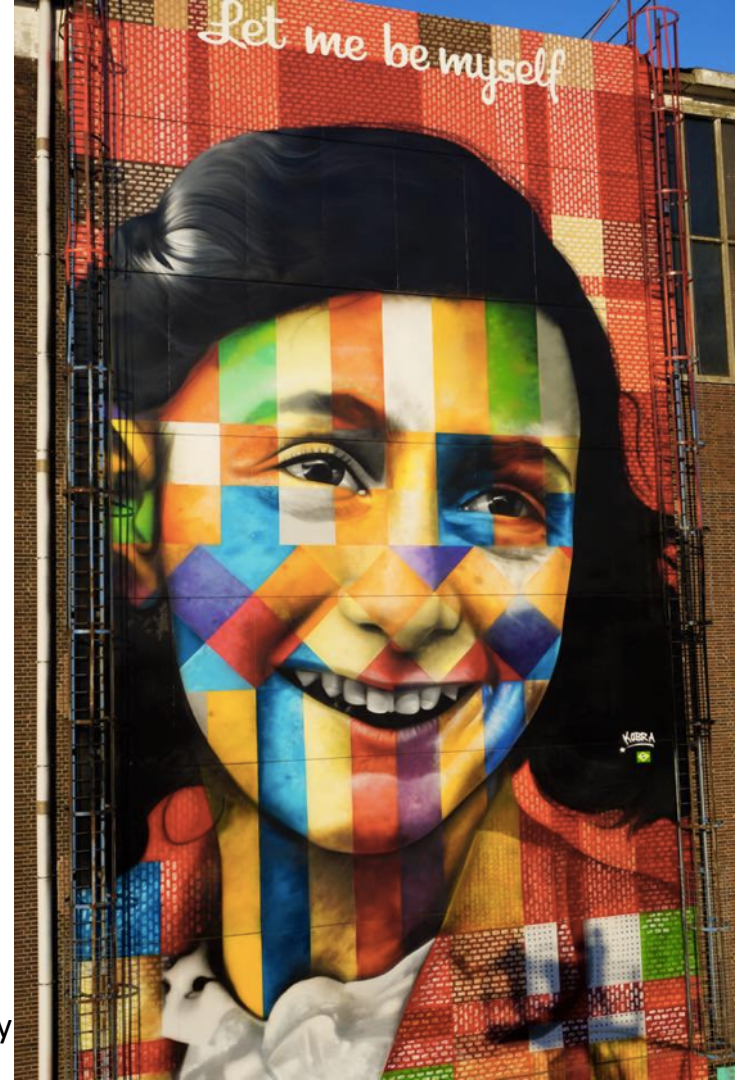
NIS

Autonomy, beyond Dignity

Charter of Fundamental Rights of the European Union

Article 1: “Human dignity is inviolable. It must be respected and protected”.

	Charter articles	Charter text
GDPR	Art. 8: Protection of personal data	<ol style="list-style-type: none">1. Everyone has the right to the protection of personal data concerning him or her.2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.3. Compliance with these rules shall be subject to control by an independent authority.
ePrivacy	Art. 7: Respect for private and family life	Everyone has the right to respect for his or her private and family life, home and communications.



“GDPR is an obstacle for technology-driven companies”

YES

- GDPR goes against key characteristics of big data, AI, block chain, etc.
- Compliance projects are costly & may constitute hindrance for technological progress
- Companies consider that a lack of knowledge on how to cost-efficiently turn collected data into business accelerating assets while complying with the GDPR = one of the biggest obstacles to the full exploitation of big data technologies
- Significant administrative burden regarding principle of accountability

NO

- One of the main goals of the GDPR is to enable a more functional and harmonized information economy within the EU
- Compliance might benefit companies' information management and create new business opportunities
- Enhancing privacy means enhancing business operations in a profound way
- Compliance with the new requirements may be turned into a commercial benefit
- New technology market providing tools & products for GDPR compliance and progress validation
- Technology as an “enabler”, recital 6

Source: borrowed from Stibbe, CPCP 2018

Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

General Data Protection Regulation, recital 6

<https://corporateeurope.org/sites/default/files/unfairbnb.pdf>



UnFairbnb

**How online rental platforms use the EU
to defeat cities' affordable housing measures**

@aureliepols

For Berlin Buzzword © Competing on Privacy

The EU vs. the US

The EU has created a privacy culture around “rights talk” that protects its “data subjects”. In the EU moreover, rights talk forms a critical part of the postwar European project of creating the identity of the European citizen.

In the United States in contrast, the focus is on a “marketplace discourse” about personal information and the safeguarding of “privacy consumers”. In the United States, data privacy law focuses on protecting consumers in a data marketplace.

Transatlantic Data Privacy Law, Paul M. Schwartz & Karl-Nikolaus Peifer

“The processing of personal data should be designed to serve mankind.

The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. “

General Data Protection Regulation (GDPR), Recital 4, par. 1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data



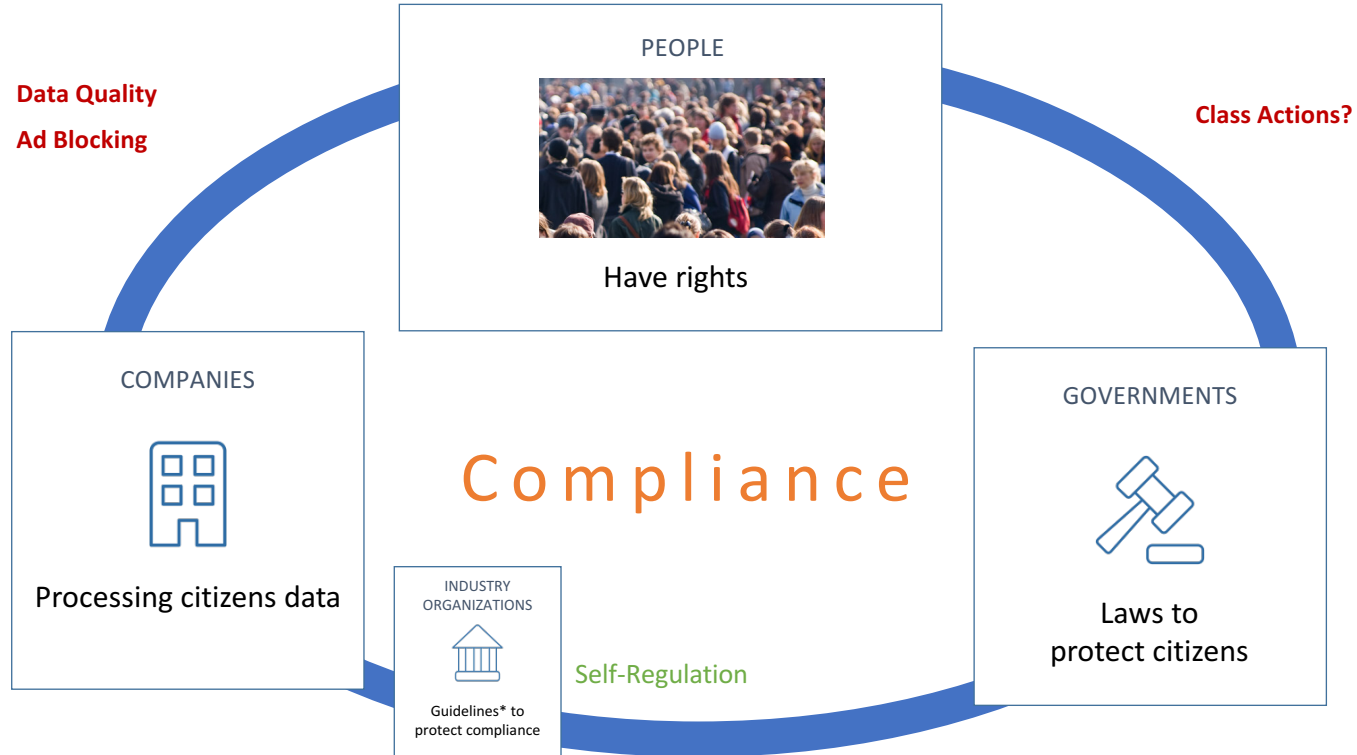
2018: GDPR enforced What is new?

A bunch of stuff!

Fines of up to
4% of global turnover
or **20 million €**,
which ever is higher
... for starters

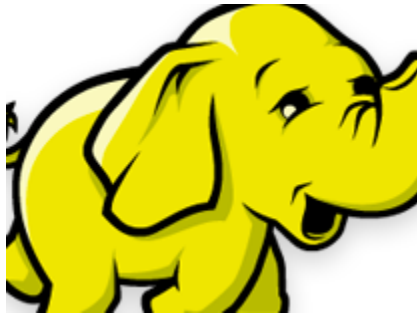
Figure 5: Crossreferencing of articles within GDPR (created by Sushant Agarwal, Institute for Management Information Systems, 2016)

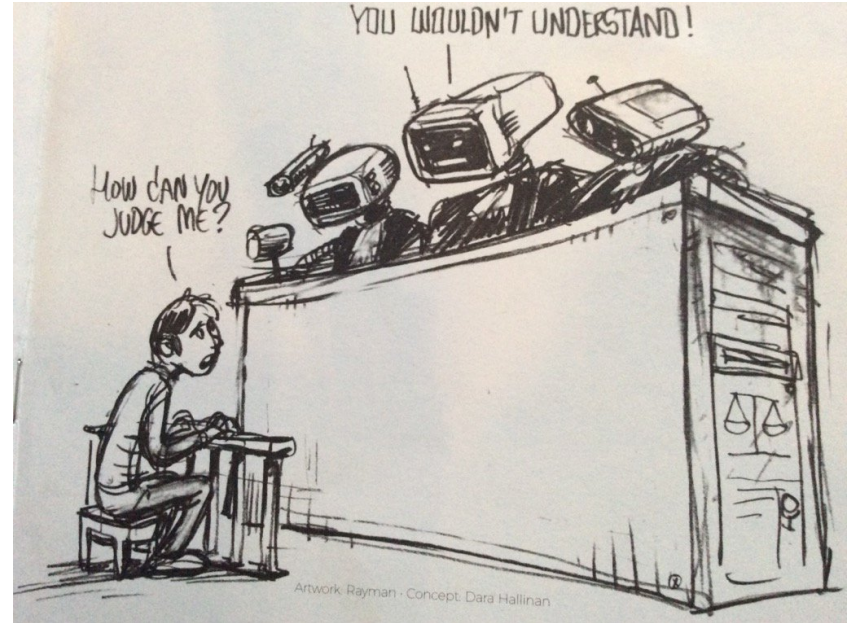
Reintroducing people into Data Privacy



The GDPR didn't happen in a vacuum

1. Legislation and it's inherent risk = an excuse to do the right thing
4% of global turn-over or 20 million €, which ever is higher!
2. Complexification of systems
3. Non linearity => this is just the beginning! (IoT)





On the need for periodical revision of models used for profiling to avoid discrimination:

“... in order to ensure that, in practice, the pre-established models and criteria, the use that is made of them and the databases used are not discriminatory and are limited to that which is strictly necessary, the reliability and topicality of those pre-established models and criteria and databases used should, taking account of statistical data and results of international research, be covered by the joint review of the implementation of the envisaged agreement (i.e. EU-Canada PNR Agreement)”. (CJEU, Opinion 1/15, EU-Canada PNR, para. 174)

People getting more savvy!



Paul-Olivier Dehay [Follow](#)

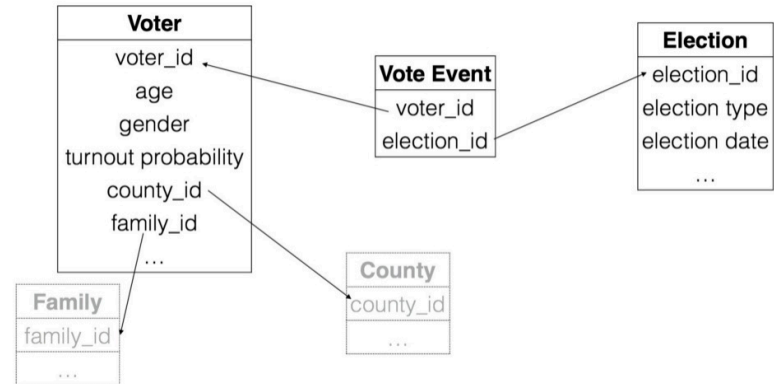
Mathematician. Co-founder of PersonalData.IO. Free society by bridging ideas. #bigdata and its #eth...
Feb 15 · 3 min read

Quick guide to asking Cambridge Analytica for your data

Cambridge Analytica has finally responded (past deadline, after some threatening emails) to requests by individuals all over Europe and the United States for a copy of their data. I give here some advice on how to go further, and offer a template for responding at the bottom.

Source: <https://medium.com/personaldata-io/quick-guide-to-asking-cambridge-analytica-for-your-data-52f9e74bd059#.ghtkcau56/>

Wondering about SARs? Visit <http://www.personaldata.io/>



Cambridge Analytica's internal database schema, as presented at a 2014 [Meetup](#).

Let's talk about the law

Now that we shared the basis for the rule of law




I am a Data Subject (Bits of Me)

The GDPR is

1. a base line for compliance,
2. re-introducing the Data Subject into the data ecosystem's equation (not new!)
3. where each actor is accountable

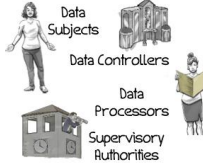
TERRITORIAL SCOPE



EU Establishments
Offer goods or services or engaging in monitoring within the EU.


Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS



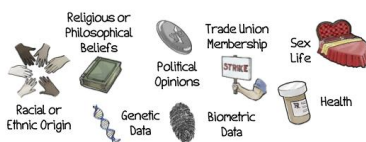
Data Subjects
Data Controllers
Data Processors
Supervisory Authorities

PERSONAL DATA



Identified Identifiable


SENSITIVE DATA



Religious or Philosophical Beliefs
Trade Union Membership
Sex Life
Political Opinions
Racial or Ethnic Origin
Genetic Data
Biometric Data
Health


RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

SECURITY




Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.

RECORD OF DATA PROCESSING ACTIVITIES




Maintain a documented register of all activities involving processing of EU personal data.

DATA PROTECTION BY DESIGN



built in starting at the beginning of the design process


DATA IMPACT ASSESSMENT



For high risk situations


GDPR

CONSENT



Consent must be freely given, specific, informed, and unambiguous.


RIGHTS OF DATA SUBJECTS



Automated Decision Making
Transparency
Access and Rectification
Right to Erasure
Purpose Specification and Minimization
Right to Data Portability

Right not to be subject to a decision based solely on automated processing, including profiling.


ENFORCEMENT



Fines
Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies:
compensation for material and non-material harm.


DATA BREACH NOTIFICATION



A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."


If likely to result in a high privacy risk → notify data subjects
Notify supervisory authorities no later than 72 hours after discovery.

INTERNATIONAL DATA TRANSFER




Adequate Level of Data Protection


BINDING CORPORATE RULES (BCRs)




PRIVACY SHIELD



MODEL CONTRACTUAL CLAUSES



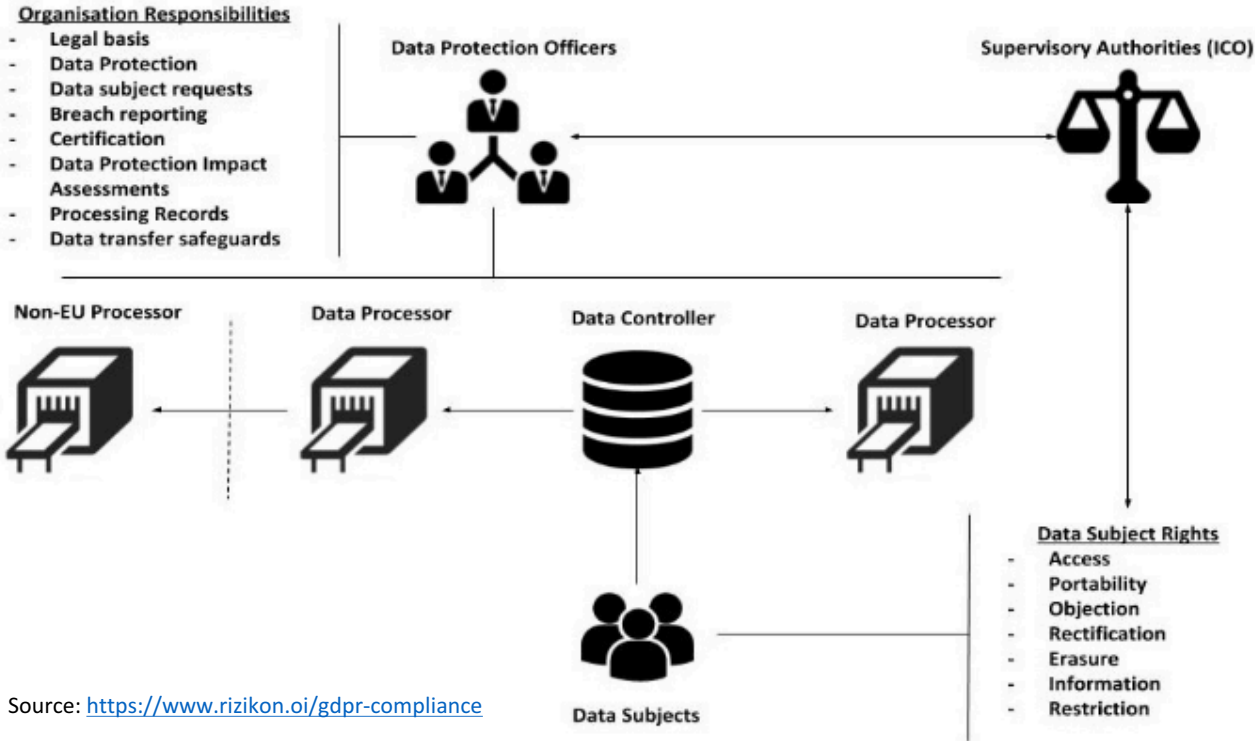


www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

Please ask permission to reuse or distribute.

Obligations under the GDPR data ecosystem



Source: <https://www.rizikon.oj/gdpr-compliance>

Appointing a DPO – Data Protection Officer – or not? Described in section 4 of the GDPR, art. 37: Designation of a data protection officer. Following articles talk of position and tasks.

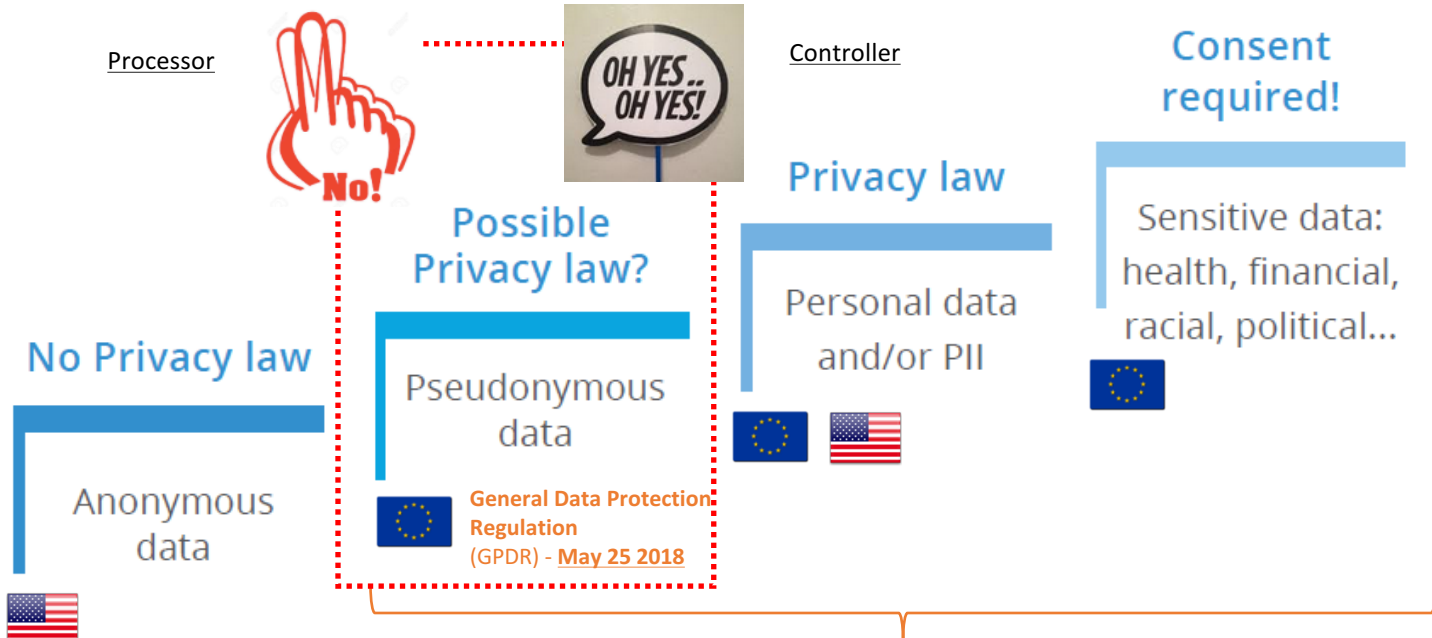
The choice remains to appoint one even if not directly required: moving beyond compliance!

Data Subjects Rights

- Article 15: Right of access by the data subject
- Article 16: Right to rectification
- Article 17: **Right to erasure (“right to be forgotten”)**
- Article 18: **Right to restriction of processing**
- Article 20: **Right to data portability**
- Article 21: Right to object
- Article 22: **automated individual decision-making, including profiling**

Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing

Articles 16 & 17: Rectification & deletion



General Data Protection Regulation (GDPR) - May 25 2018

Which variables or combination exactly?

The inevitable question! (≠ PII!)

Personal data in the GDPR (article 4.1)

‘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 15: Data Subject Access Requests

Exemptions



Controllers may be able to refuse to comply with a SAR where:

- Third party personal data is involved;
- Protection of intellectual property rights and trade secrets;
- No personal data is involved.

However, result should not be the refusal to provide information to the data subject.



Controllers can ask the data subject to specify the information or processing activities to which the request relates where a large amount of data is involved.



Remember: you cannot refuse to comply with a SAR on the basis that it would be costly and/or time consuming. Be prepared to make extensive efforts to be ready to provide a copy of the personal data undergoing processing by May 2018.

Source: DataGuidance GDPR Essentials: Data Subject Rights

Take note of

- Article 12.4 to develop communication around your stance:
“if the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within **one month of receipt of the request** of the reasons for not taking action and on the possibility of lodging a complaint with the supervisory authority and seeking judicial remedy”.
- Recital 63
- Article 15.4, which shows it’s about
 1. The right to obtain certain information on the activities a company performs
 2. The right to obtain a copy of the data undergoing processing

Practical steps for SARs:



Develop a SAR procedure involving Privacy and product teams to identify the personal data they will have to return upon request



Develop authentication procedure



Consider the various options for returning the data – consumer-facing portals, returning information via emails, online forms







Develop standard response

Source: DataGuidance GDPR Essentials: Data Subject Rights

Article 16: Right to Rectification

Requirements

	An individual can require a data controller to rectify inaccuracies in personal data held about them
	In certain circumstances, the data subject shall have the right to have incomplete personal data completed, which may involve recording a supplementary statement
	A controller will also need to communicate the rectification of personal data to any third parties to which the data has been disclosed
	In practice: organizations should enhance self-service options for individuals to make updates to their personal information directly, or provide for granular options in relation to data returned to individuals as part of an SAR request

See also recital 65 which provides examples and links rectification to erasure

Source: DataGuidance GDPR Essentials: Data Subject Rights

The right to erasure (article 17)

It typically requires a balancing test as it's not an absolute right

Example: employee data needed for compliance &/or establishment, exercise or defense of legal claims => keep the data & tell data subject why her data is not deleted

Can apply if:

- Data is no longer necessary
- No more legal basis for processing: consent is withdrawn, legitimate interests not accepted, objection to direct marketing

Depend upon

- Recognition of compliance obligation
- Linkability of data, even pseudonymized, and possibility to decouple
- Available options: typically deletion probable (Adobe)

Article 18: Restriction of processing. When?

- Data accuracy
- Unlawful processing, typically 6.1(f) legitimate interests
- Internal process flow!

Note that

- Erasure applies to all systems: includes back-ups, copies leans & extends to 3rd parties!
- Applicable when individuals have removed their consent for processing activities based on consent (no other legal ground) or have objected to processing based on legitimate interests or they have objected to direct marketing activities
- Refusal for deletion doesn't mean access should not be granted!
- Automated deletion? Unlikely!

Erasure is a similar process to SARs

Practical Steps



Privacy should guide the product and business teams within the organization to identify personal data in scope of deletion requirement



Clean up retention policies – identify business need to retain the data for each specific business unit. Often, the business wants shorter retention!



Ensure that systems containing personal data are able to delete personal data. Deletion must be hard deletion and apply to any duplicative database, including back-up systems



Requirement to take reasonable steps to notify others who are processing that data with details of the request unless it is impossible or would involve disproportionate effort



Privacy must review each and every deletion request.

Source: DataGuidance GDPR Essentials: Data Subject Rights

Art. 18: Restriction of processing

Practical Steps



Ensure your organisation has in place systems to enable the identification of restricted personal data as well as restricting access to and further processing of this data. Undertake development work if needed



For example, moving the data to a separate system; temporarily blocking the data on a website or otherwise making the data unavailable



Be prepared for potential “combination requests” i.e. simultaneously asking the data controller to stop processing the personal data and to, for example, erase it. Such requests may be more difficult to deal with

Source: DataGuidance GDPR Essentials: Data Subject Rights

Article 20: Data Portability

Requirements



An individual can only exercise the **Right to Data Portability** when:

- a business is processing personal data either based on their consent; or
- where the processing is necessary for the performance of a contract with the individual; and
- the processing is carried out by automated means (i.e. performed by a computer)

Applicability



Applicable to data provided by the data subject including:

- Data submitted via an online form; and
- Data generated and collected from activities of users

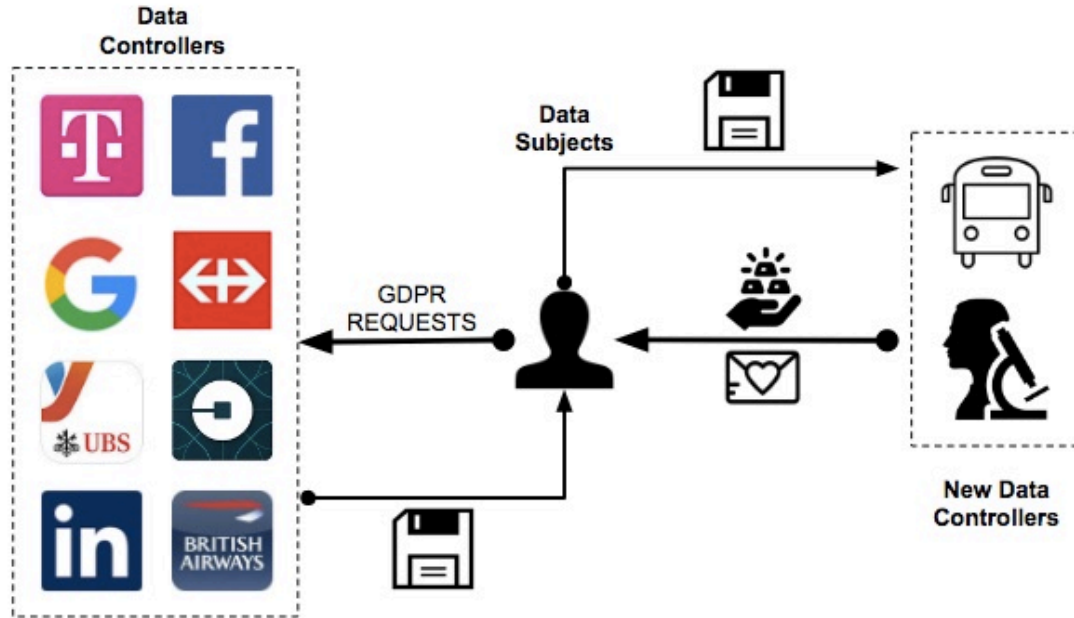


The right is **not** applicable to personal data *derived* or *inferred* from the data provided by the data subject

Source: DataGuidance GDPR Essentials: Data Subject Rights

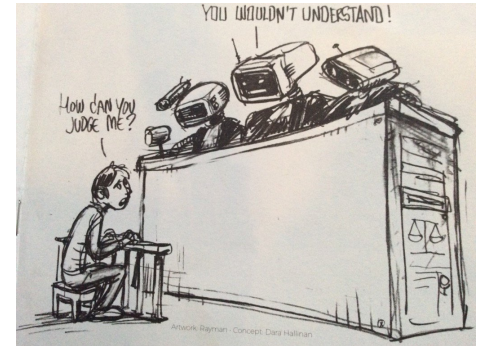
The coming of age of Transparency Wars?

Portability rights



Art. 22 : The right not to be subject to a decision based solely on automated processing, including profiling

1. The data subject shall have the 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.
2. Paragraph shall not apply if:
 - a) It is **necessary** for entering into, or performance of, a contract between the data subject and a data controller;
 - b) ... Authorised by Member state Law...
 - c) It is based on the data subject's **explicit consent**.



3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and **legitimate interests**, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and **legitimate interests** are in place.

Where 9 (1): Special categories of personal data also called sensitive data: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Profiling

Requirements



“Profiling” is defined broadly under GDPR as “a procedure which may involve a series of statistical deductions...often used to make predictions about people”



GDPR applies restrictions to **automated decision making** that involves **profiling**: “a data subject shall have the 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”



GDPR also applies to general profiling (e.g. the use of personal data to evaluate certain personal aspects relating to a natural person) by requiring a **privacy impact assessment** to be carried out if general profiling takes place

Interpretation



“Legal effects” will include **impingements on the freedom to associate with others, vote in an election, or to take legal action or an effect on legal contractual status or rights**



“Similarly significantly” effects need not be legal ones. The threshold is the **significant of the decision’s impact on the data subject**

Source: DataGuidance GDPR Essentials: Data Subject Rights

Assuring compliance with profiling activities

Practical Steps



Conduct a **Privacy Impact Assessment** in relation to the profiling activity



Additional measures:

- **Determining** which of your business activities involve profiling which constitutes automated decision making or non-automated profiling
- **Informing** data subjects of the existence and logic involved in the automated decision-making process
- **Explaining** the significance and envisaged consequences
- **Providing** data subjects with the means to oppose a decision
- **Having in place**, procedures, guidance and training so relevant staff know how to deal with profiling issues

Source: DataGuidance GDPR Essentials: Data Subject Rights

Applicability of automated decision making

- Typical examples are scoring solutions to come to a decision
 - Credit scoring for loans, mortgages... (Google ban on PayDay loans)
 - Educational scoring to get into colleges...
- It's based on this idea that:
 - Discrimination is not allowed
 - You shouldn't keep paying for past errors
 - Someone should take responsibility for wrong data (false positives/negatives)
=> acceptable levels?
- Applicable for agencies?
 - Activation of data by DMP & CDPs is a risk
 - Eg. Price discrimination

Reality check

At least in my digital world

Technology stacks

Digital Transformation is as much a buzz word as GDPR



Some numbers

Since the enforcement of the GDPR:

- The Dutch supervisory authority received 170 complaints in the 1st week of the GDPR
- The Irish supervisory authority 1.300 in the last week of May
- The Spanish SA estimates their annual complaints at 10.000 (multiplied by 5 since 2008)
- Some of our clients have received over 2.200 deletion requests
- We solved 12% of these requests

Hands up: how many of you know

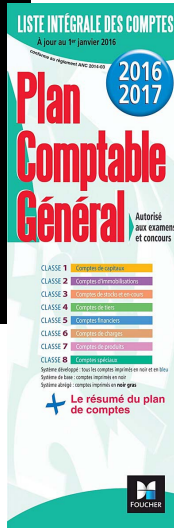
- What an IDFA is?
- What an AdID?
- Where to find it?
- Where to find the ID of a specific app?
- How to fill in a SAR?
- How to complain to the supervisory authority?

What privacy engineers should focus on

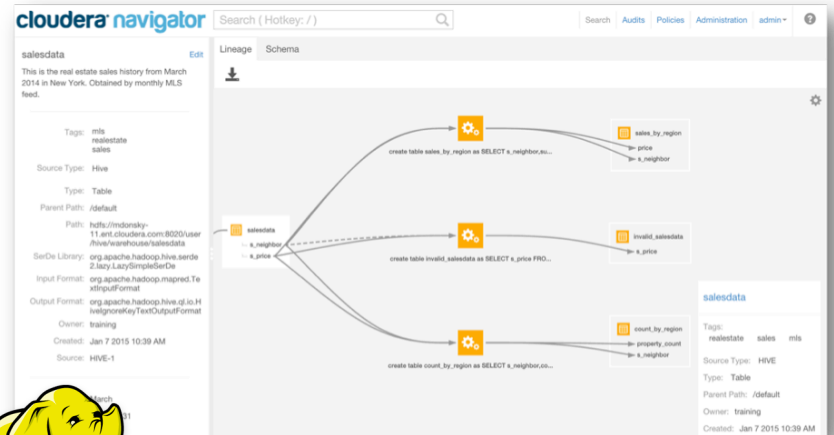
- Purpose classification

If Not, You'll Crash and 🔥

```
2016-05-12 13:40:54.161036 DiscoTime[12103:588848]
This app has crashed because it attempted to
access privacy-sensitive data without a usage
description. The app's Info.plist must contain an
NSHomeKitUsageDescription key with a string value
explaining to the user how the app uses this data.
```

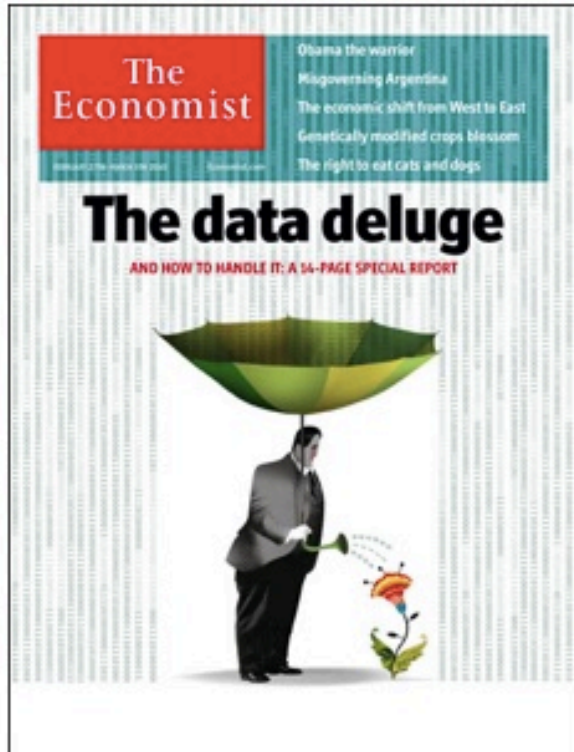


- Consent trails and traceability (including reverse engineering between parties/legal entities)



What are we solving for?

@aureliepols



@aureliepols

For Berlin Buzzword © Competing on Privacy

Thank you for
your attention

aurelie@mindyourprivacy.com

@aureliepols

For Berlin Buzzword © Competing

**ANYTHING YOU
SAY OR DO CAN
AND WILL BE
USED AGAINST YOU
IN A TARGETED
ADVERTISEMENT**

think privacy