

Privacy and the General Data Protection Regulation

Dominik Huth, 4.12.2019, Guest lecture Computational Methods for Social Sciences

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
www.matthes.in.tum.de

Introduction

Who is talking to you? (Professional version)

2006 – 2012

Dipl. Math. oec. @ TUM

2012 – 2016

SAP CRM Consultant & Developer @ Reply

Since 2016

PhD student in Information Systems @ TUM Informatics faculty,
working on personal data and the implementation of the general
data protection regulation





Introduction – another perspective

Who is talking to you? (More private version)

1986 Privacy awareness: zero

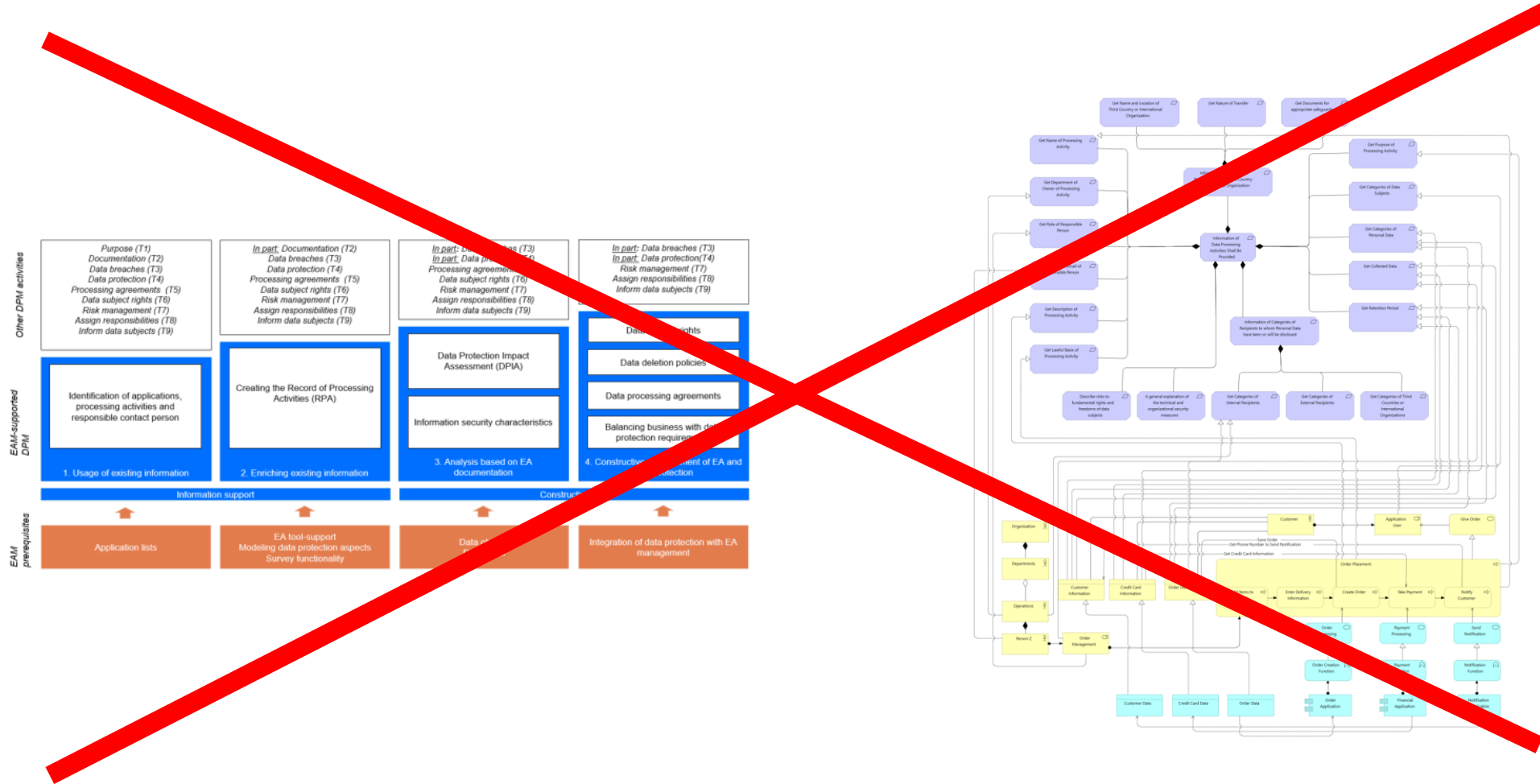
2000 Why do my teachers voluntarily put embarrassing pictures of themselves online?

2006 Joined StudiVZ, for some reason

2012 (Do not) find me on  !



What are we going to talk about?



POWEEEEERRRR!



Privacy definition

Motivation for privacy legislation

The GDPR

Practical advice

What is privacy? – some famous definitions

„Privacy is the right to be let alone“

Warren & Brandeis, 1890

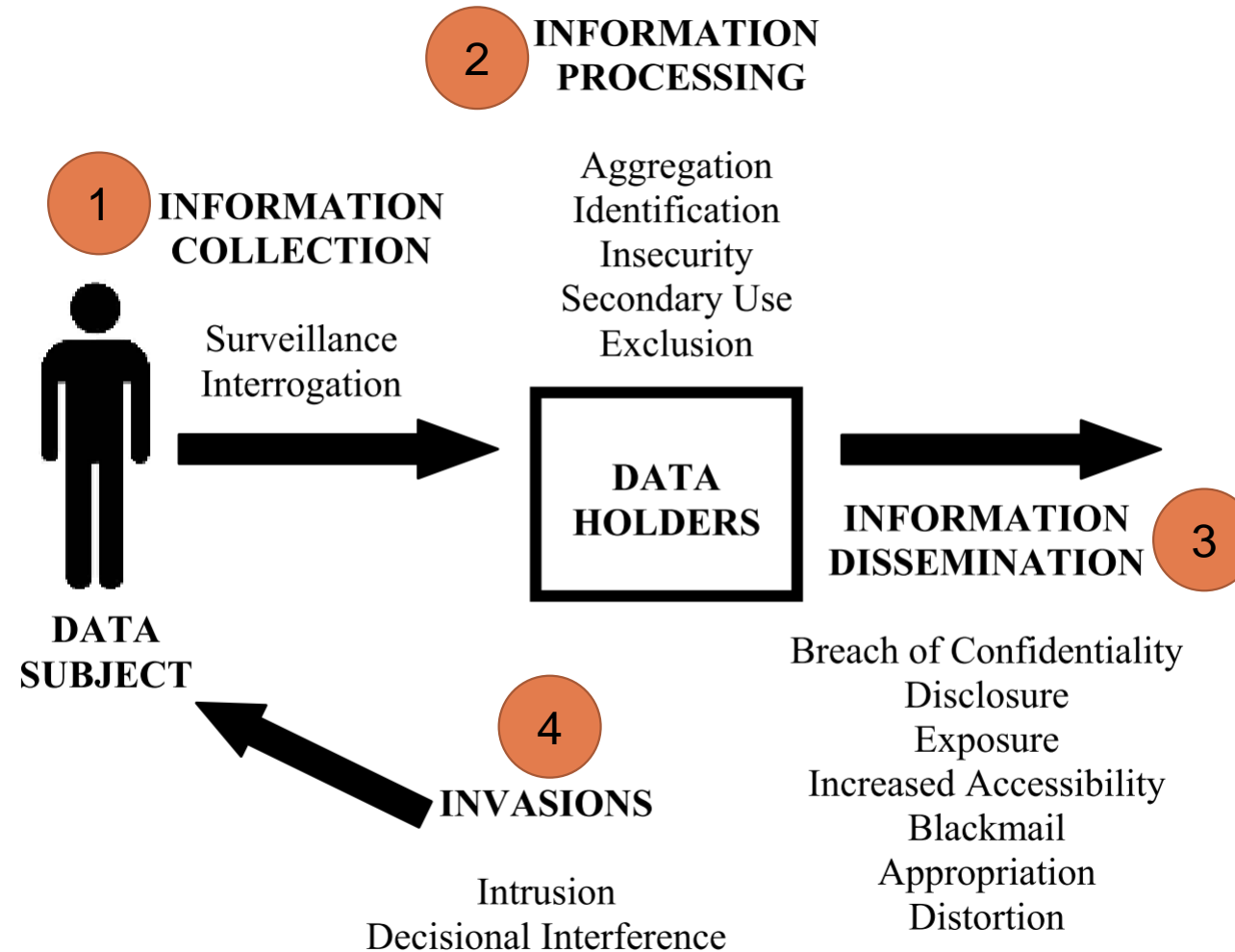
„Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others“

Westin, 1967

„Privacy is a set of protections against a related set of problems. These problems are not all related in the same way, but they resemble each other. There is a social value in protecting against each problem, and that value differs depending upon the nature of each problem.“

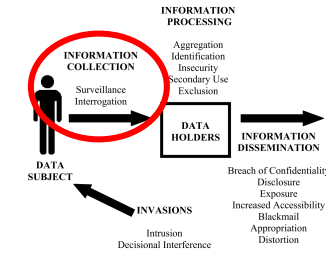
Solove, 2007

Solove's Taxonomy of Privacy



Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), p. 477. (<https://doi.org/10.2307/40041279>).

1st group of activities: Information collection



Surveillance

- Awareness of surveillance can make people feel uncomfortable
- People might even change behavior: self-censorship and inhibition, self-imposed mainstream behavior
 - Even more so if there is a *possibility* of being watched (Panoptic effect - based on Panopticon Prison design by Jeremy Bentham)
- Being unaware of surveillance is not any better: If watched long enough, *something* compromising could be found (Martin Luther King example)

“If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him.”

Cardinal Richelieu (supposedly)

- There are also private actions in the public space – conversations, interactions as customers, ...
- However, surveillance can also convey a sense of security

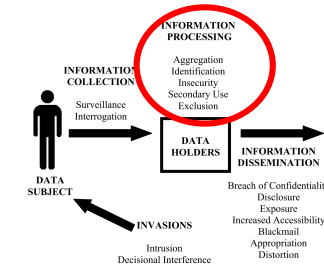
Interrogation

- Census outcry, e.g. in Germany 1987: (year of birth, gender, religion, state of employment...)
- Refusal to answer vs. the „nothing to hide argument“



2nd group of activities: Information processing

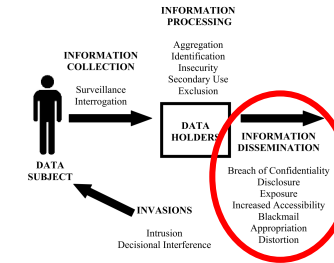
„How is data handled?“



- Aggregation: One data point is not very telling, but combination with others can make it revealing
 - Shopping history, credit history – what if the information is not complete?
- Identification
 - Once a link to an individual is established, it is possible to link all future (and past) actions to a person
- Insecurity
 - Like in aggregation, there is a risk of downstream harm - what if an attacker uses the data in a malicious way?
- Secondary use: use of data for purposes unrelated to the ones it was originally collected for
- Exclusion: the inability to participate in the maintenance and use of one's information

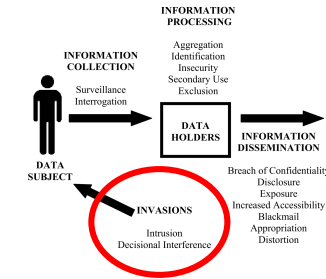
3rd group of activities: Information dissemination

- Abuse of trust
- There is information that you do not want to be published to everyone: address, health status, sexual orientation
- According to our common social norms, we conceal „animal-like“ behaviour
- However, dissemination of information is necessary in some cases (e.g. criminal investigation)



4th group of activities: Invasion

- Intrusion
 - Interference with people's solitude
 - „time thieves“ (spam mails, telemarketing) can also be intrusive
- Decisional interference
 - US Supreme Court Decision *Roe vs. Wade* ruled that the right to privacy „encompass[es] a woman's decision whether or not to terminate her pregnancy“
 - Other rulings regarding the right of consenting adults to enter into relationships



Not mentioned in the article, but incredibly scary (and true):
 What if the knowledge about your preferences and intimate fears were used to
 influence your decision in an election?

Summary of Solove's privacy taxonomy

- The taxonomy is heavily based on Supreme court decisions in government vs. citizen rulings
- Solove doesn't describe the „citizen vs business“ case, but the taxonomy holds for business interactions as well

What about its relation to computer science?

	(Mutually exclusive) Action	Relevant GDPR Personal Data Processing Examples
Processing	Operate	Adaptation; Alteration; Retrieval; Consultation; Use; Alignment; Combination
	Store	Organization; Structuring; Storage
	Retain	opposite to (Erasure; Destruction)
Collection	Collect	Collection; Recording
Dissemination	Share	Transmission; Dissemination; Making Available; opposite to (Restriction; Blocking)
Invasion	Change	unauthorized third party (Adaptation; Alteration; Use; Alignment; Combination)
	Breach	unauthorized third party (Retrieval; Consultation)

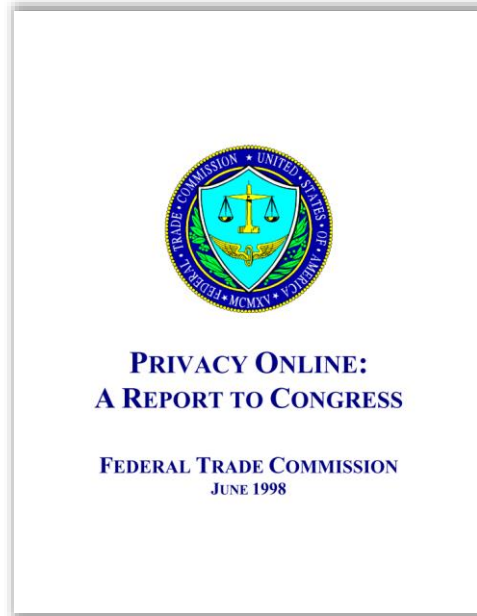
Privacy definition

Motivation for privacy legislation

The GDPR

Practical advice

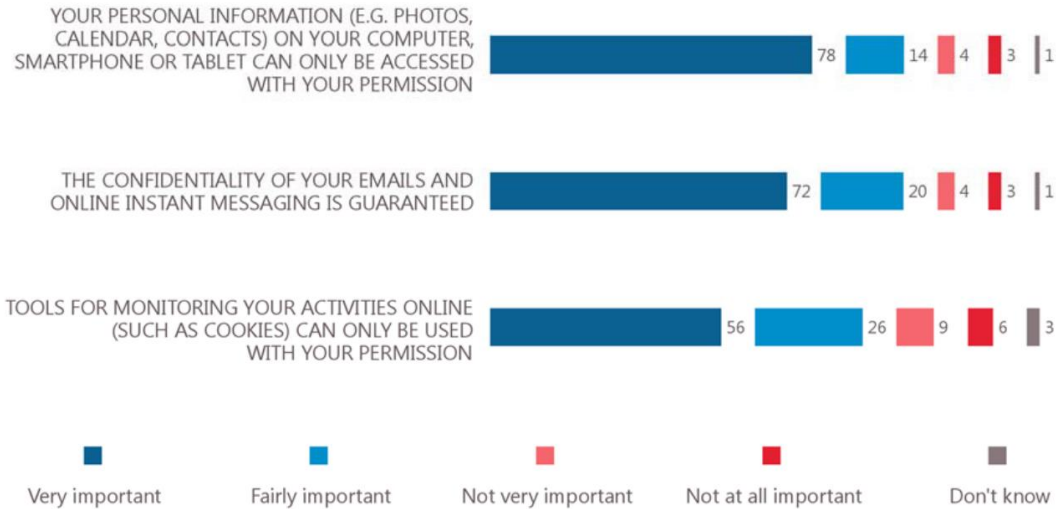
People value privacy... concerns in 1998



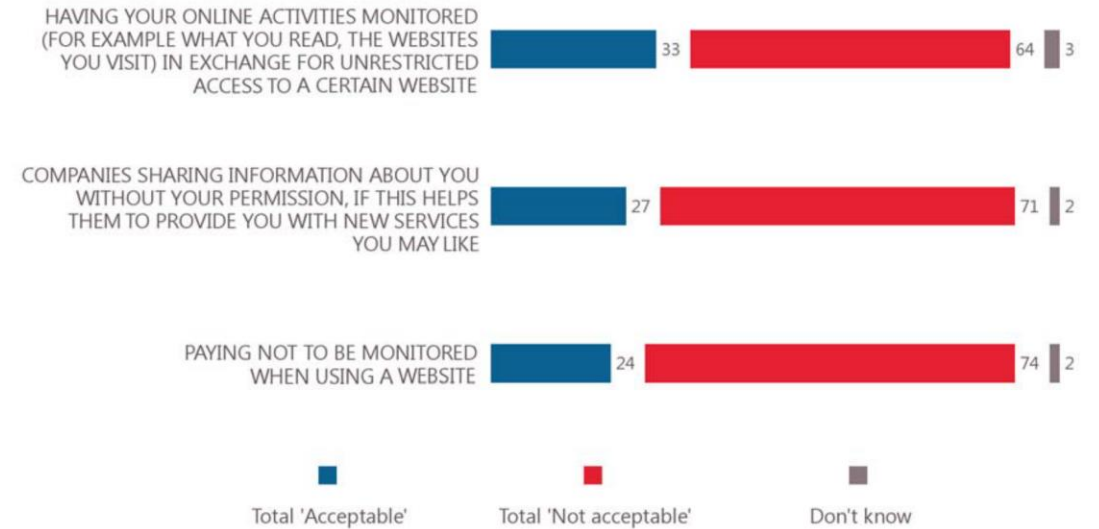
„If growing consumer concerns about online privacy are not addressed, electronic commerce will not reach its full potential.“

People value privacy...

How important for you is each of the following things?
(% - EU)



To what extent do you find each of the following things acceptable or not?
(% - EU)



What is personal data „worth“? (Jentzsch 2016)

Based on market valuation

- 1. Financial results per data record:** Aggregated market cap of a company divided by number of customers
Facebook (Q3/2019): \$570bn / 1.6bn -> 350\$ per user
- 2. Market price of data:**
Asking for your credit score: €25 at Schufa
Average additional sales from a new email address: \$15 (Privy 2019, take with caution)
- 3. Cost of data breach:** Insurance against identity theft: ~\$60
- 4. Data prices in illegal markets**
\$10 - \$60 for stolen accounts (Airbnb, Verizon, banks – Krebs 2017)

Based on individual valuations

- 5. Surveys and economic experiments:** see next slides
- 6. Willingness to pay:** see next slides

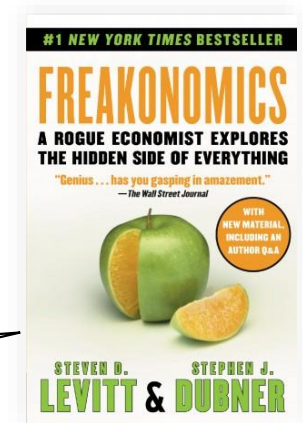
People value privacy... really? The privacy paradox

- „Hypothetical statements [about the value of private data] are often not associated with real valuations.“ (Jentzsch 2016)
- “25 cents is a price that lies within the set of values at which people are willing to sell, but does not lie within the set of values that people are willing to spend to protect” (Grossklags 2007)
- „The authors conclude from their research that individuals are not willing to pay one Euro for their privacy.“ (Jentzsch 2012, lab experiment with online shops)

How about you?

- How many privacy statements have you read lately?
- Do you use „free“ services?

„sociology is how the world should work, economics is how it actually works”



Jentzsch, N., Preibusch, S., and Harasser, A. 2012. “Study on Monetising Privacy An Economic Model for Pricing Personal Information,” *Agenda*, p. 76. (http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy/at_download/fullReport).

Jentzsch, N. 2016. “State-of-the-Art of the Economics of Cyber-Security and Privacy.” (<https://doi.org/10.1007/s10273-011-1262-2>).

Grossklags, J., Hall, S., and Acquisti, A. 2007. “When 25 Cents Is Too Much : An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information,” *Information Security*, pp. 7–8. (<https://doi.org/10.1.1.137.696>).

People value privacy... really?



Google +3.000% since IPO



Facebook +523% since IPO

Motivation Summary

- We all have a need for privacy (though it might mean something different for each of us)
- The nature and perception of privacy changes over time
- We have difficulty in assigning a value to our personal data.
- A range of factors lead us to choices that are not privacy-aware.
 - Network effects
 - Unwillingness to pay
- Privacy is an important prerequisite for freedom of speech. There is societal value in the protection of this right.

Outline

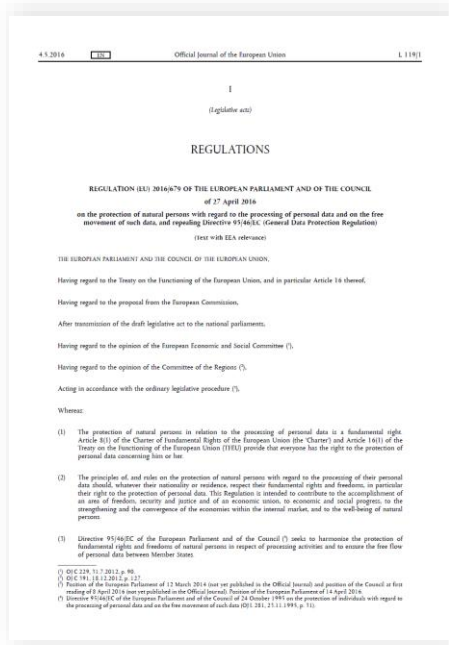


Privacy definition

Motivation for privacy legislation

The GDPR

Practical advice



GDPR key elements

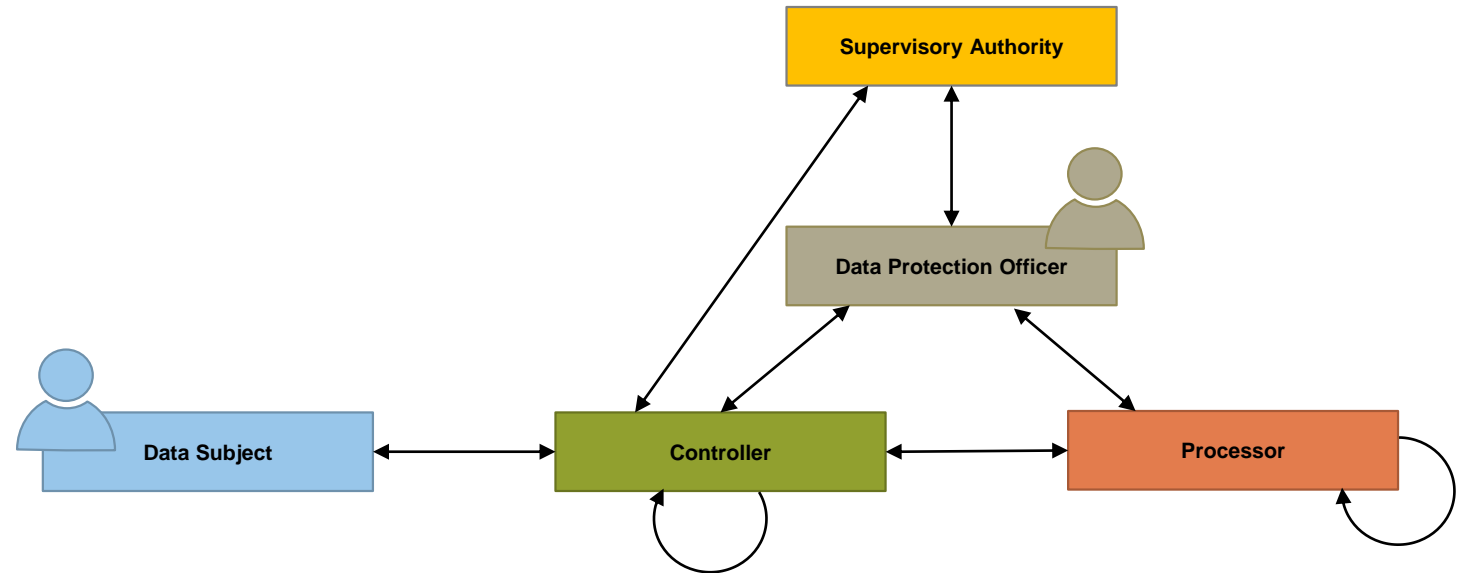
- Initiated 2012, passed 2016, in force since 2018
- Updated definitions (what is personal information?)
- Applies to all organizations who handle data of European citizens
- Sets the rules for data exchange between organizations and across borders
- Extended rights for data subjects: transparency, portability, objection, notification of data breach, rectification, erasure
- Principle of accountability, data protection by design and default
- Records of processing activities, Data protection impact assessments
- Designation of Data Protection Officer, certification mechanisms
- **Fines of up to 4% revenue / €20m for non-compliance**

Data protection regulation has existed before in Europe and elsewhere! The GDPR updated the definitions given in the 1995 EU directive (a time when less than 1% of the world population used the internet) and catches up with technological and economic development. Most importantly, its dramatic fines have urged companies to take data protection seriously.

Stakeholders in the regulation

Another recipient
Association
Certification body
Child
Controller
Court
Data protection officer
Data subject
European Data Protection Board
Member State
National accreditation body
Natural person
Not-for-profit body
Processor
Representative
Supervisory authority
Third party

Main stakeholders (three or more relationships)



Examples of fines

CNIL.
To protect personal data, support innovation, preserve individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL | Q |

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

A⁻ A⁺ Print

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

21 January 2019

On 21 January 2019, the CNIL's restricted committee imposed a financial penalty of 50 Million euros against the company GOOGLE LLC, in accordance with the General Data Protection Regulation (GDPR), for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization.

„Lack of transparency, inadequate information, lack of valid consent“

ico.
Information Commissioner's Office
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home Your data matters For organisations Make a complaint Action we've taken

About the ICO / News and events / News and blogs /

Intention to fine British Airways £183.39m under GDPR for data breach

Date 08 July 2019
Type News

Statement in response to an announcement to the London Stock Exchange that the ICO intends to fine British Airways for breaches of data protection law.

Following an extensive investigation the ICO has issued a notice of its intention to fine British Airways £183.39M for infringements of the General Data Protection Regulation (GDPR).

The proposed fine relates to a cyber incident notified to the ICO by British Airways in September 2018. This incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers were compromised in this incident, which is believed to have begun in June 2018.

The ICO's investigation has found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information.

Information Commissioner Elizabeth Denham said:

“People's personal data is just that – personal. When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights.”

Data of 500,000 customers compromised due to poor security measures

ico.
Information Commissioner's Office
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home Your data matters For organisations Make a complaint Action we've taken

About the ICO / News and events / News and blogs /

Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach

Date 09 July 2019
Type Statement

Statement in response to Marriott International, Inc's filing with the US Securities and Exchange Commission that the Information Commissioner's Office (ICO) intends to fine it for breaches of data protection law.

Following an extensive investigation the ICO has issued a notice of its intention to fine Marriott International £99,200,396 for infringements of the General Data Protection Regulation (GDPR).

The proposed fine relates to a cyber incident which was notified to the ICO by Marriott in November 2018. A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million related to UK residents.

It is believed the vulnerability began when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems.

339m guest records exposed over five years

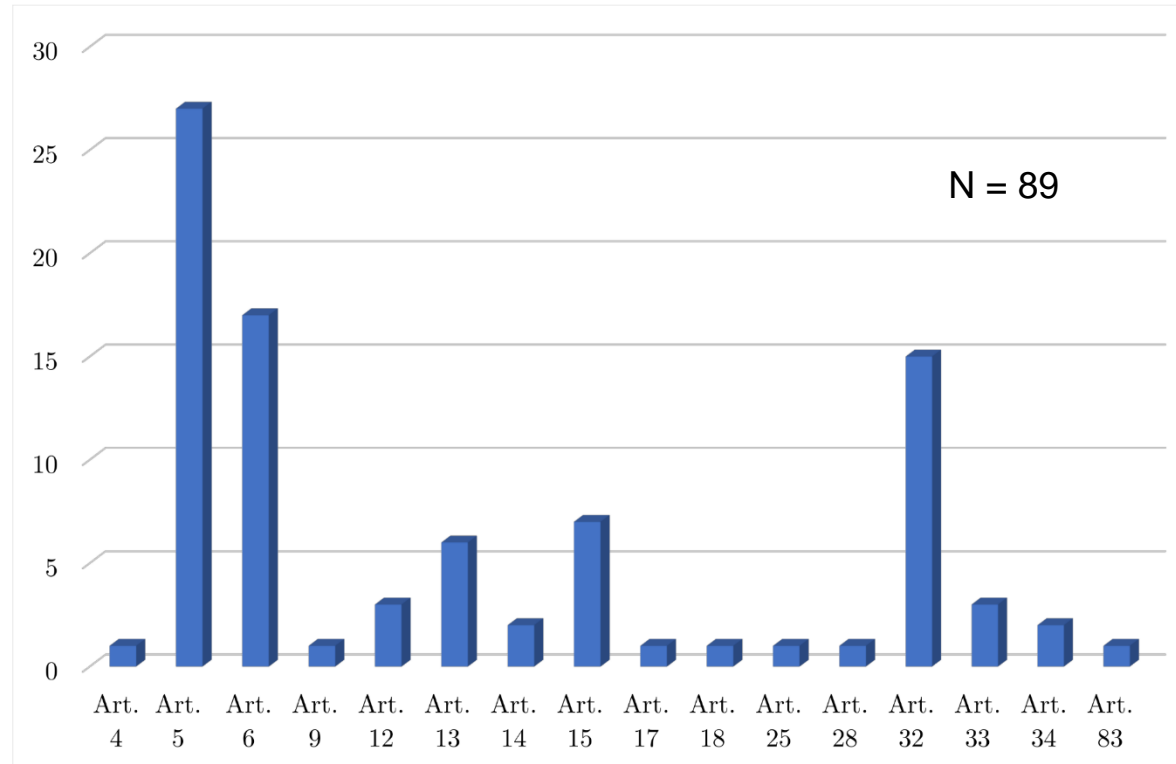
<https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc> accessed 19/11/2019

<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/> accessed 19/11/2019

<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/> accessed 19/11/2019

Analysis of issued fines

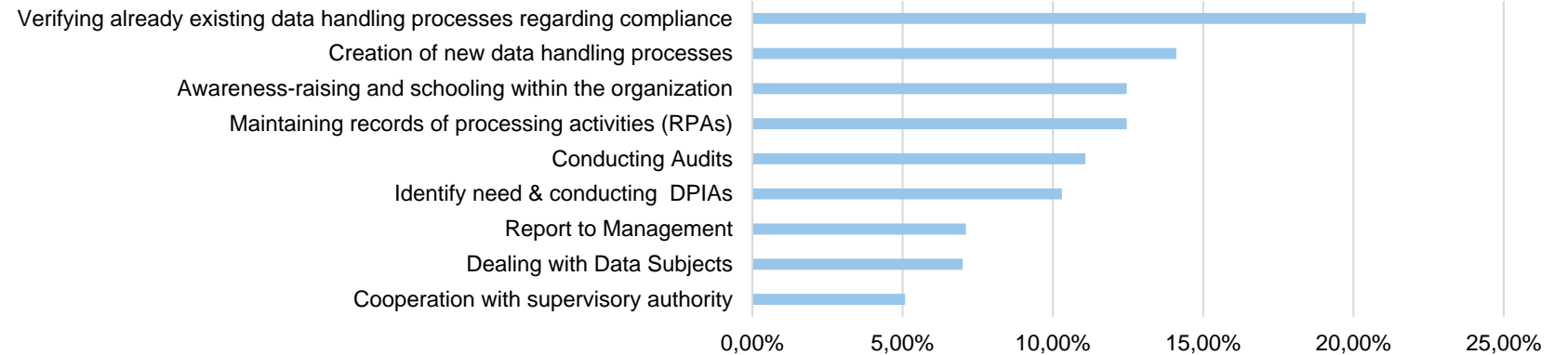
What are companies being fined for?



- Art. 5: Processing principles
- Art. 6: Legal basis for processing
- Art. 13: Right to information
- Art. 15: Right of access
- Art. 32: Security of processing

How much time is spent on these tasks and what are perceived difficulties?

What is the proportion of this activity from your total worktime as DPO?



Please select the two most severe challenges for this activity

	Legislation	Tools/Tech	Personnel	Guidelines	Contact persons	Authority	Holistic view	Single process
Awareness-raising and schooling within the organization	12%	10%	26%	17%	5%	9%	10%	10%
Verifying already existing data handling processes regarding compliance	9%	11%	17%	16%	17%	6%	9%	14%
Creation of new data handling processes	10%	10%	18%	13%	15%	8%	8%	17%
Identify need & conducting DPIAs	14%	14%	14%	19%	12%	4%	9%	14%
Cooperation with supervisory authority	6%	3%	23%	29%	20%	11%	6%	3%
Maintaining records of processing activities (RPAs)	8%	14%	14%	20%	8%	2%	16%	16%
Conducting Audits	9%	13%	20%	26%	9%	7%	11%	7%
Dealing with Data Subjects	20%	20%	7%	7%	7%	7%	7%	24%
Report to Management	10%	3%	19%	10%	10%	32%	6%	10%

Outline



Privacy definition

Motivation for privacy legislation

The GDPR

Practical advice

What is personal data?

TECHNOLOGY

A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr. AUC. 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga.," several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her.

AOL removed the search data from its site over the weekend and apologized for its release, saying it was an unauthorized move by a team that had hoped it would benefit academic researchers.

But the detailed records of searches conducted by Ms. Arnold and 657,000 other Americans, copies of which continue to circulate online, underscore how much people unintentionally reveal about themselves when they use search engines — and how risky it can be for companies like AOL, Google and Yahoo to compile such data.

Those risks have long pitted privacy advocates against online marketers and other Internet companies seeking to profit from the Internet's unique ability to track the comings and goings of users, allowing for more focused and therefore more lucrative advertising.

But the unintended consequences of all that data being compiled, stored and cross-linked are what Marc Rotenberg, the executive director of the Electronic Privacy Information Center, a privacy rights group in Washington, called "a ticking privacy time bomb."

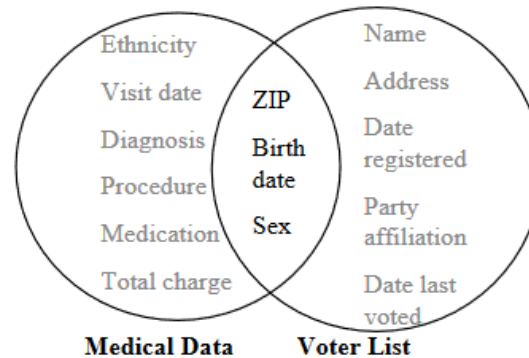


Figure 1 Linking to re-identify data

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

- Latest: Strava suggests military users 'opt out' of heatmap as row deepens



▲ A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava. Photograph: Strava Heatmap

Sensitive information about the location and staffing of military bases and spy outposts around the world has been revealed by a fitness tracking company.

The details were released by Strava in a data visualisation map that shows all the activity tracked by users of its app, which allows people to record their exercise and share it with others.

The map, released in November 2017, shows every single activity ever uploaded to Strava - more than 3 trillion individual GPS data points, according to the company. The app can be used on various devices including smartphones and fitness trackers like Fitbit to see popular running routes in major cities, or spot individuals in more remote areas who have unusual exercise patterns.

However, over the weekend military analysts noticed that the map is also detailed enough that it potentially gives away extremely sensitive information about a subset of Strava users: military personnel on active service.

<https://www.nytimes.com/2006/08/09/technology/09aol.html> accessed 29 Nov 2019

L. Sweeney - k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570.

<https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>, accessed 29 Nov 2019

What is personal data?

GDPR definition – Article 4 (1):

‘personal data’ means 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;

In general: Seemingly innocent data can become personal if it is linked to a person. The more information that is collected about an individual, the easier it is to identify the person.

What is *not* personal data?

Anonymity concepts for personal data



k-anonymity: A release provides k-anonymity protection if the information for each person contained in the release cannot be distinguished from at least k-1 individuals whose information also appears in the release. → *higher is better!*

l-diversity: A k-anonymous data set is said to satisfy it if, for each group of records sharing quasi-identifier values, there are at least l “well-represented” values for each confidential attribute. → *higher is better!*

	AOL search data	Voter registration	Fitness data
k	<ul style="list-style-type: none">Background on news of the day: manyCombinations of behavioral problems of dogs, addresses, names, ...: 1	<ul style="list-style-type: none">In the case of Massachusetts governor: exactly 1In other cases <i>maybe</i> a few	<ul style="list-style-type: none">Number of physically active people on the secret Army base: 1000?
l	<ul style="list-style-type: none">1 (no k-anonymity!)	<ul style="list-style-type: none">1	<ul style="list-style-type: none">Number of occupational groups: 1 (i.e. 0 which would make you believe it is not a secret Army base)

Why not anonymize everything? - „If you knew how to maintain the distribution after anonymization, you could just as well generate the data synthetically“ (Senior AI solution architect)

- How do you maintain demographic data?
- Utilities industry: addresses, houses, apartments in houses, owners, tenants (address histories, payment information, credit scores, contact history), businesses, ...

Making sure that it is impossible to tell whether a record is in a dataset or not (**differential privacy**) is an important research topic!

L. Sweeney - k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570.
Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R., and Schiffner, S. 2014. “Privacy and Data Protection by Design.” (<https://doi.org/10.2824/38623>).

Legal basis for data processing

Article 6 (1) defines the possible reasons for data processing

- a) **Consent** - „Yes, I agree“ (must be „Privacy by default“, i.e. active consent/Opt-In)
- b) **Performance of a contract** – e.g. online shop needs your address and payment details
- c) **To comply with legal obligation**
- d) **To protect the vital interests of the data subject or another person**
- e) **In the public interest**
- f) **„Legitimate interest“** – e.g. log access to web page to ensure security. Otherwise this is the “catch all” phrase in privacy policies

Data subject rights



- Art. 12 Right to transparent information: Especially to be informed of information collection (Art. 13 & 14) and about influencing data processing (Art. 15 – 22)
- Art. 13 Information rights for data collection
- Art. 14 Information rights for data processing (e.g. by other party)
- Art. 15 Right of access (ask for a copy with reasonable frequency) so you can exercise rights according to Art. 16 – 18
- Art. 16 Right to rectification (correct false credit records, wrong health information, ...)
- Art. 17 Right to be forgotten (ask for deletion IF this is not in conflict with other legislation (tax, criminal record))
- Art. 18 Right to restriction of processing
- Art. 19 The data controller must notify downstream processors of the data subjects claims according to Art. 16 – 18
- Art. 20 Right to data portability: Right to get a digital copy of all your data, so you can transfer it to another controller – e.g. social media or health data. This should foster competition for more privacy-aware services.
- Art. 21 Right to object to processing, e.g. for marketing purposes
- Art. 22 Right not to be subject to (entirely) automated decision making IF it is not necessary for entering into a contract or an obligation of the controller

What are your responsibilities?

Disclaimer: I am not a lawyer and this is not legal advice

Legal basis for processing	Most likely consent (Art. 6 (1) a). Make sure to have consent for the type of processing (e.g. audio recording) and the purpose
Transparent information about the data usage	Suggestion: „Conduct research for understanding the problem of X“ (Google: „we use your data for improving our services and developing new ones“). Be clear about what will be communicated in publications (pseudonyms, descriptive information about person/company)
Data minimization	Be sure about what you want to find out and which data you need for that purpose
Only use data for the reasons specified	„Repurposing“ data is not allowed! Exaggerated example: Do research interviews and use the insights to send affiliate links to interview partners
Comply with requests of data subjects	E.g. access, request for deletion, storage limitation
Secure storage	Apply common sense for the type of data you are collecting – password protection and access restriction go a long way
Limited time storage	Make a realistic guess when the data will no longer be needed

Q & A

- If someone asks me to delete personal data, do I have to delete it in my backups as well?
- Can I use the data that I have anyway for a different analysis?
- Is there a difference in the national implementations?
- Do I always have to ask for permission now?
- Who is my supervisory authority?
- What if I store other people's data on dropbox?
- Can I ask for deletion of any type of data now?
- Who tells me how to interpret the regulation?
- ...



Dipl. Math.oec.

Dominik Huth

Research Associate

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business
Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.17128

Fax +49.89.289.17136

dominik.huth@tum.de
www.matthes.in.tum.de



All images under pixabay license, free for commercial use and no attribution required

- Solove, D. J. 2006. “A Taxonomy of Privacy,” *University of Pennsylvania Law Review* (154:3), p. 477. (<https://doi.org/10.2307/40041279>).
- Colesky, M., Hoepman, J.-H., and Hillen, C. 2016. “A Critical Analysis of Privacy Design Strategies,” in *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*, pp. 33–40.
- Keighley, T. C. 2016. “Eurobarometer 431 Data Protection“ (<https://doi.org/10.2838/552336>).
- Jentzsch, N. 2016. “State-of-the-Art of the Economics of Cyber-Security and Privacy.” (<https://doi.org/10.1007/s10273-011-1262-2>).
- <https://www.privy.com/blog/whats-the-value-of-an-email-address> accessed 19/11/20
- <https://krebsonsecurity.com/2017/12/the-market-for-stolen-account-credentials/> accessed 19/11/20
- Jentzsch, N., Preibusch, S., and Harasser, A. 2012. “Study on Monetising Privacy An Economic Model for Pricing Personal Information,” *Agenda*, p. 76. (http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy/at_download/fullReport).
- Grossklags, J., Hall, S., and Acquisti, A. 2007. “When 25 Cents Is Too Much : An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information,” *Information Security*, pp. 7–8. (<https://doi.org/10.1.1.137.696>).
- Landesberg, M. K., Levin, T. M., Curtin, C. G., and Lev, O. 1998. “Privacy Online : A Report To Congress.” (<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>).
- European Union. 2016. “Regulation 2016/679 of the European Parliament and the Council of the European Union,” *Official Journal of the European Union*, pp. 1–88. (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504>).
- Bachelor’s thesis Michael Vilser, <https://www.matthes.in.tum.de/pages/12wb2907mhi4k/Bachelor-s-Thesis-Michael-Vilser>
- Huth, D., Faber, A., and Matthes, F. 2018. “Towards an Understanding of Stakeholders and Dependencies in the EU GDPR,” in *Multikonferenz Wirtschaftsinformatik*, P. Drews, B. Funk, P. Niemeyer, and L. Xie (eds.), Lüneburg, pp. 338–344.

Further reading

- Alan Westin: Privacy and Freedom
- Bruce Schneier: Data and Goliath
- Shoshana Zuboff: The age of surveillance capitalism
- Daniel Solove: „I’ve got nothing to hide“ and other misunderstandings of privacy
- Andreas Pfitzmann, Marit Hansen: A terminology for talking about privacy by data minimization
- www.enforcementtracker.com – Website collecting GDPR fines
- Das Standard-Datenschutzmodell – Process model for creating compliant processing activities, published by the German data protection authorities <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf>