
Data science & marketing: A legal view

Data Science & Marketing • Guest Lecture Series • 13 March 2018
David Vasella

walderwyss attorneys at law

The legal view

walderwyss attorneys at law

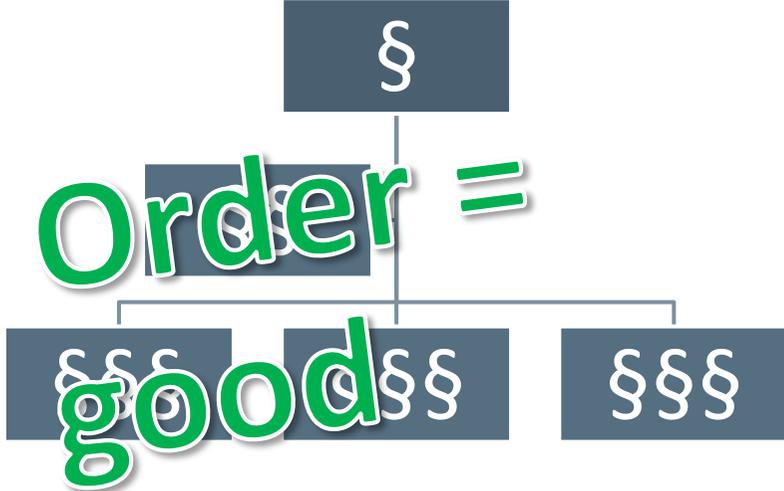
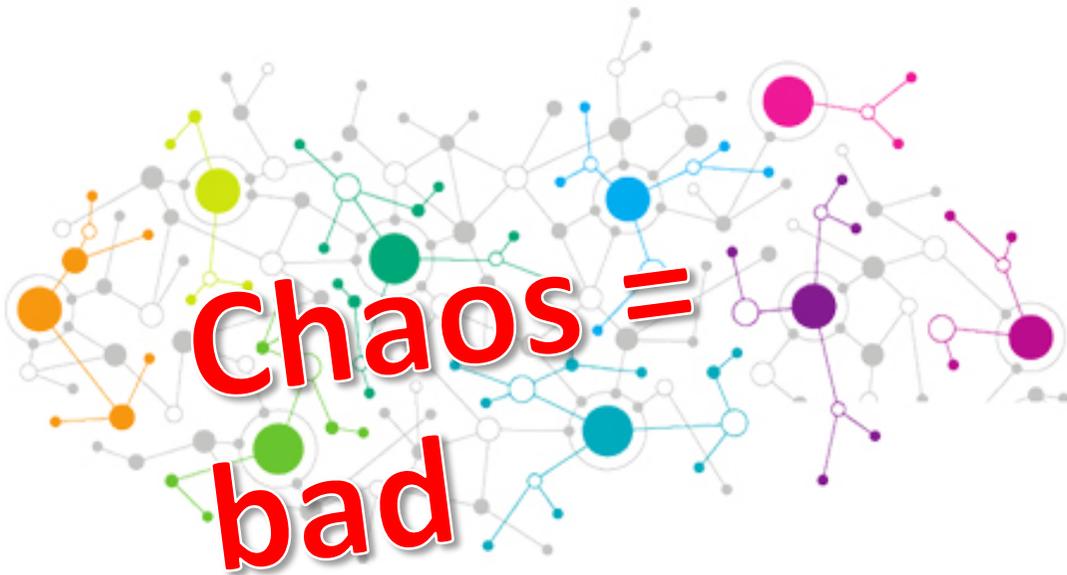
“Data Science”:

“Data science, also known as data-driven science, is an interdisciplinary field of scientific methods, processes, algorithms and systems to **extract knowledge or insights from data in various forms**, either structured or unstructured, similar to data mining.”

(Wikipedia)

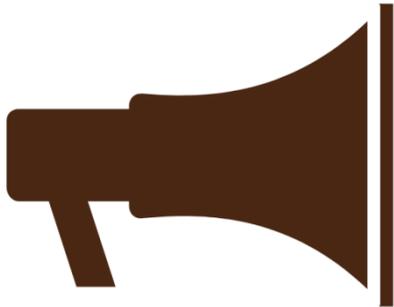
Data:

Law:



- What’s “data” in the first place? Information? But what is “information”?
- Do they speak about personal data? Or also about other data? Or anonymized data? Can they really anonymize data?
- What’s the difference between pseudonymization and anonymization?
- Does it fall under the GDPR?
- I have heard talk of “big data”. Is this the same?
- Is it artificial intelligence?
- Who owns the data?
- And the results achieved by the scientists?
- Who’s liable if something goes wrong?
- Is this regulated??
- Who gets access to data? Where is it located? Is this a safe country?
- What’s “science”, anyway?

“The World”:



“The Law”:



ru
be
ac
ov
produce the



the
h

Some background on data protection law

walderwyss attorneys at law

The main actors in the legal arena

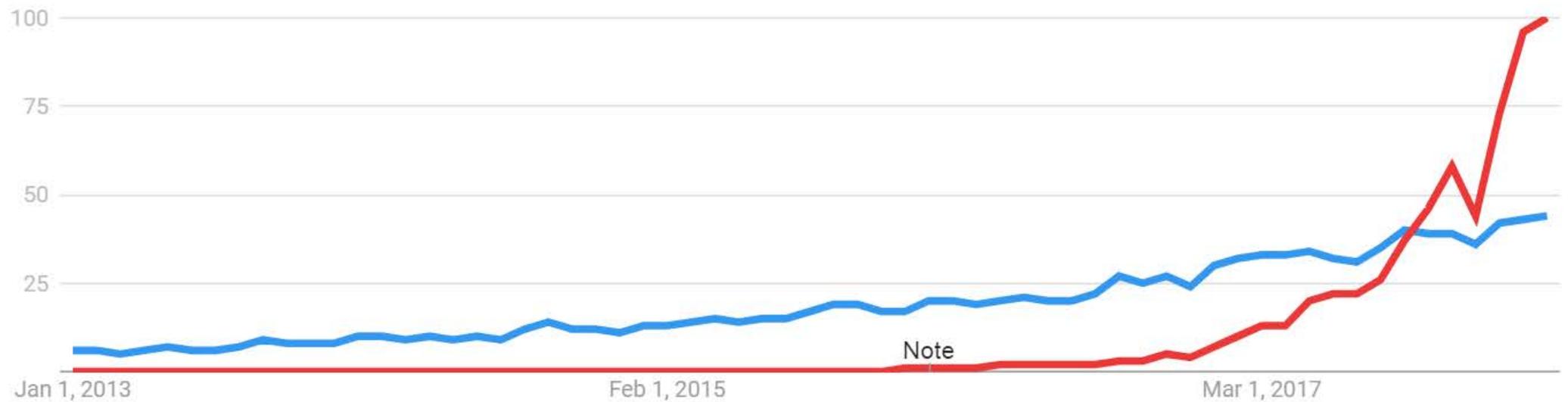
- **International organizations** with their treaties:
 - the EU (Directive, GDPR)
 - OECD (Guidelines)
 - the Council of Europe (Convention 108)
- **Countries** with their national laws:
 - Swiss “Datenschutzgesetz”, Canton of Zurich’s “Gesetz über die Information und den Datenschutz”, German “Bundesdatenschutzgesetz”, US HIPAA
- **Courts** with decisions:
 - Swiss Bundesgericht, “Logistep”
 - EU Court of Justice, “Schrems”
- **Official bodies** with guidance and recommendations:
 - the Swiss EDÖB, EU’s Article 29 Working Party, EU Commission
- **Private bodies** with recommendations and standards:
 - Industry standards
- **Companies** with their own requirements:
 - Internal policies, contracts with other companies

The main laws for private actors in Europe

- **Council of Europe**
 - Convention 108
- **EU**
 - the EU Data Protection Directive
 - the e-Privacy Directive
 - the upcoming GDPR
 - the new e-Privacy Regulation
- **Switzerland**
 - Swiss “Datenschutzgesetz”

Google Trends for the past 5 years:

- “Data Science”
- “GDPR”



The GDPR in a nutshell

- far-reaching reform of European data protection law
- effective as of 25 May 2018
- applicable directly without requiring implementation laws
- applies to many Swiss companies, too
- main principles are lawfulness, transparency, data minimisation, storage limitation, purpose limitation
- requires a review of data processing practices, including existing processes, workflow, and infrastructure
- massive sanctions possible



Swiss data protection law

- private actors: “Datenschutzgesetz” (DSG), in force since 1993. Very open wording and lack of sanctions
- the DSG is currently in revision, including to align with the GDPR
- no final text yet
- entry into force expected for 2019/2020 (?)

Key concepts

walderwyss attorneys at law

“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;

Article 4(1) GDPR

“Personal data”

1. information

2. relating to an identified or identifiable natural person: a person 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

← *who must be able to make the identification? The «owner» or someone else?*

← *any identifier?*

← *what is «specific to the identity»? What is the «identity»?*

Sensitive data

= data with generally increased risk

- Racial or ethnic origin
- Health
- Religion
- Sex life
- Genetic or biometric data
- Criminal convictions
- etc.

“Processing” of personal data

“Processing”:

“any operation or set of operations which is performed on **personal data** or on sets of personal data,

whether or not by automated means,

such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”

Article 4(2) GDPR

“Controller” and “processor”

“Controller”:

- the “owner” of the data who decides that data is processed, why, and how
- main responsible for complying with data protection law

“Processor”:

- someone who is not the controller but processes personal data on behalf of the controller (a service provider to the controller)
- has own responsibilities under data protection law

Controller

“owns” the data
and primary
responsible

Personal Data

information about
the data subject



Data Subject

the person to whom
the data pertains



Processor

processes data and
for the controller

Personal data in marketing

walderwyss attorneys at law

Reminder: the GDPR's view

- “The **scale of the collection and sharing** of personal data has increased significantly”
- “**Technology** allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities”
- “Natural persons should have **control** of their own personal data”
- “widespread public perception that there are **significant risks to the protection of natural persons**, in particular with regard to **online activity**”
- “Effective protection [...] requires the strengthening and **setting out in detail** of the rights of data subjects and the obligations of those who process [...]”

Some key principles

- Know what you do with data.
- Plan your processing ahead.
- Tell the subjects about your processing.
- Ask for permission, unless you have a legal right to process.
- Process data only as you have said you would.
- Document all your data processing.
- If you give data away, use a written agreement.
- Delete data if you don't need it anymore.
- Don't process data if you would not be comfortable with explaining on TV.

“Profiling”

“any form of automated processing of personal data consisting of the use of personal data

to **evaluate certain personal aspects** relating to a natural person,

in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;”

Article 4(4) GDPR

“Profiling”

“In order to ensure fair and transparent processing [...], the controller should use **appropriate mathematical or statistical procedures** for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in **inaccuracies** in personal data are corrected and the **risk of errors** is minimised, secure personal data [...] and that prevents, inter alia, **discriminatory effects** on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.”

Recital 71 GDPR

“Automated Individual Decision-Making”

“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 [...]

[...]

[...] 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.”

(Article 22 GDPR)

e-Privacy Regulation (draft)

No final text yet, but these are some expected revisions:

- **Cookies**: requires active, informed consent
 - except session cookies
 - statistical evaluation
 - cookie walls?
- **Tracking**:
 - tracking with cookies, device fingerprinting, beacons, WLAN tracking etc. requires consent
- **Browser settings**: privacy by default
- **Electronic direct marketing** (“spam”): requires consent
 - except for some existing customers

Key take-aways

walderwyss attorneys at law

- Data protection law is complex and a moving target, but the key principles are simple.
- When in doubt, consider data to be personal.
- Don't be careless. Know what you do, why you do it, how you do it, with whom and where.
- Plan your processing early on.
- Document your processing and be prepared to explain it.
- Involve the lawyers.
- Follow the developments and expect tougher rules for marketing.

Resources

- www.datenrecht.ch
- www.dataprotection.ch
- www.swissblawg.ch

Thank you.

Dr David Vasella, attorney at law, CIPP/E

david.vasella@walderwyss.com

+41 58 658 52 87

walderwyss attorneys at law