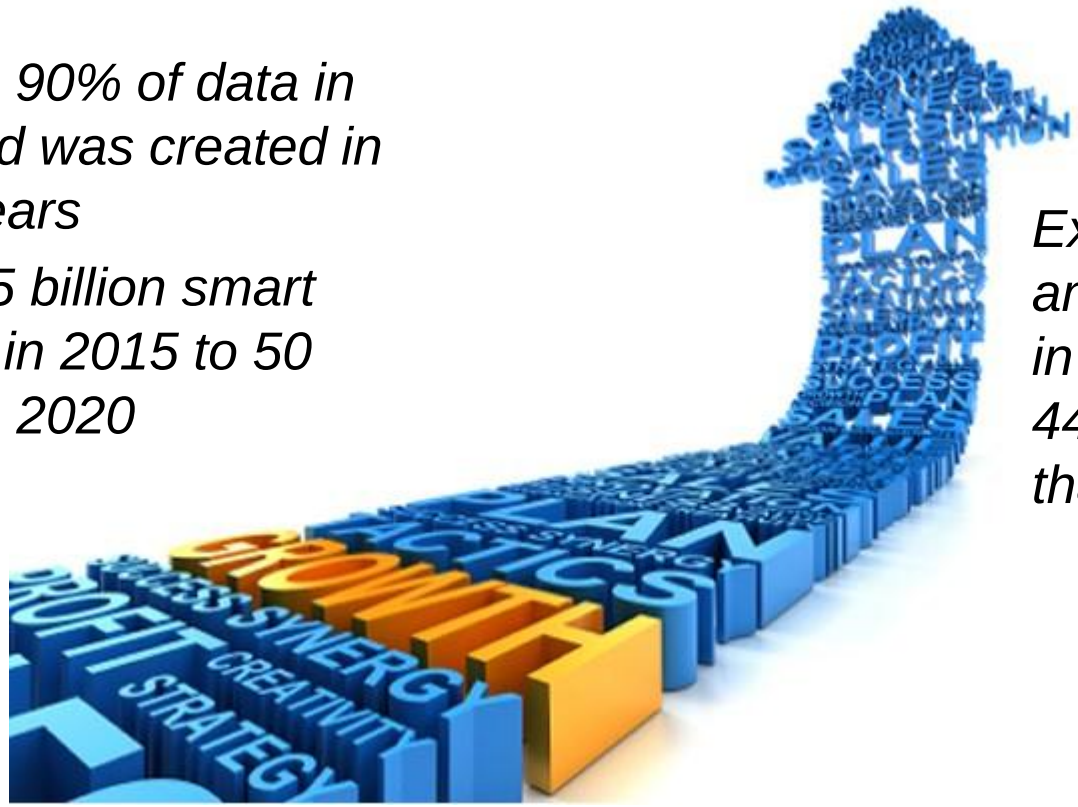
General EU Data Protection Regulation

How are we prepared?

mag. Predrag Krstić

Big data

- *In 2013, 90% of data in the world was created in last 2 years*
- *IOT – 15 billion smart devices in 2015 to 50 billion in 2020*



Expected amount of data in 2020 will be 44 times bigger than in 2009

Personal data collectors

A few examples:

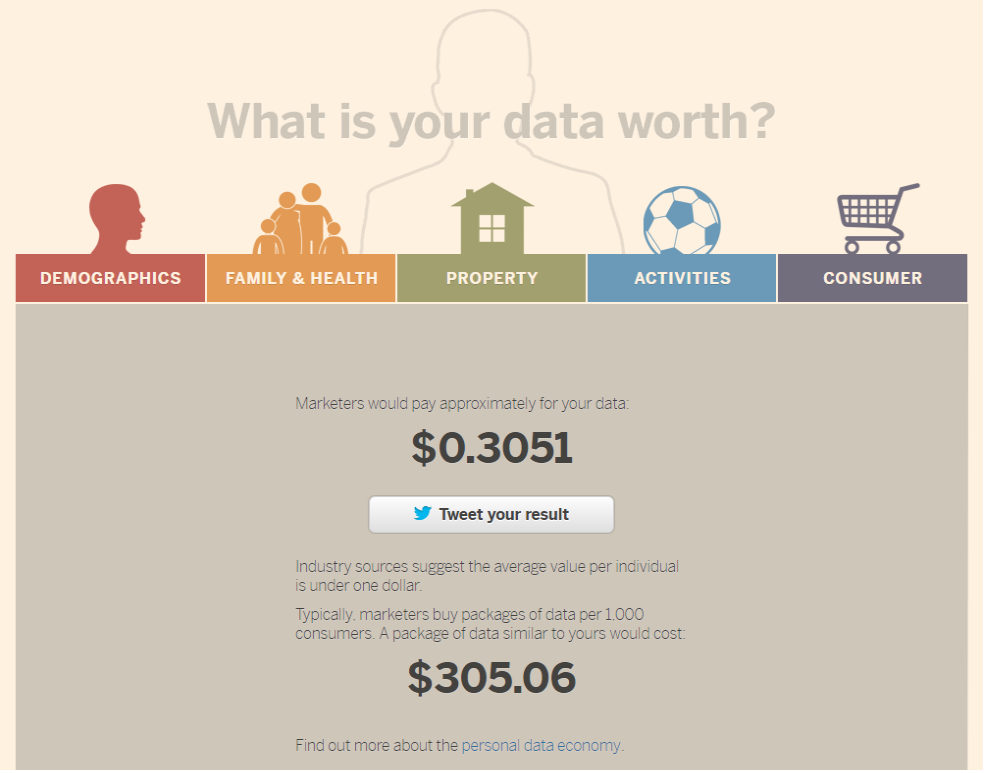
- Collecting information via forms (registractions on the internet, shopping cards)
- Visiting websites (cookies)
- Searching on the web (search engines)
- Smartphones (geolocation,...)
- Activity trackers, wearable devices (heartbeat monitoring, blood pressure,...)

What's your data worth?

The Financial Times published a calculator allowing to get your personal data worth by answering a simple poll.

My personal data is estimated at **0.3051 $**. That's the amount marketers would pay me.

Typically, marketers buy packages of data per **1,000 consumers**. A package of data similar to mine would cost: **$305.06**



Personal data

Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject");

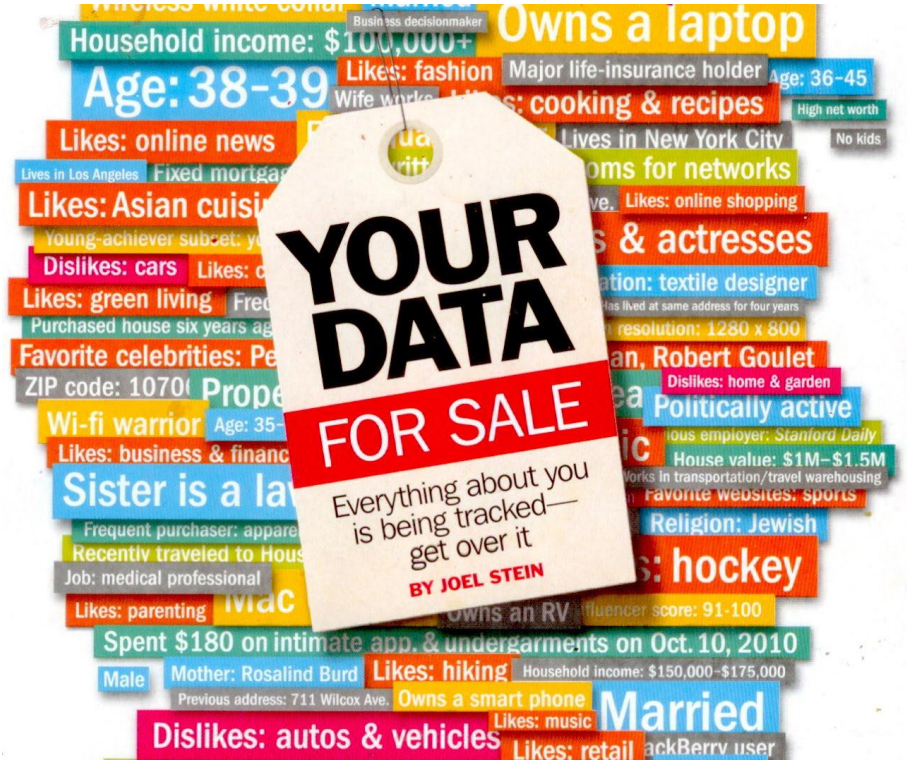
An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"

Who has the access

Virtually every organization acquires, uses and stores personally identifiable information (PII). Most have it for their employees and, depending on their area of business, may also have it for a wider group including customers, patients, residents and students.

Why does it matter?

"You might be refused health insurance based on a Google search you did about a medical condition. You might be shown a credit card with a lower credit limit, not because of your credit history, but because of your race, sex or ZIP code or the types of Web sites you visit."



Mistakes cost millions

- Hartland Payment Systems committed **$8 million to settle lawsuits** following a data breach which compromised 130 million credit and debit cards
- Health Net of the Northeast Inc. agreed to **pay for two years of credit-monitoring** for 1.5 million members whose details were on a lost hard drive
- Sony provided **free services to customers** affected by their 2011 data breaches to help them protect against identify theft

General Data Protection Regulative

- Will replace **DPD from 1995** which is obsolete due to the fast technological advancements and globalization.
- One of the **DPD's** biggest issues: **It comes in 28 flavors** ☺
- **GDPR** brings higher security for individuals, generalization and stricter legislation for organizations

GDPR for organizations

- Only one set of laws across all 28 states – this makes life a lot simpler for multi-nationals compared to today's mish-mash of national provisions
- Organisations ('controllers') will only have to work with one authority instead of 28, good when it comes to reporting breaches
- Organisations above 250 employees (or 5,000 records held) must appoint a Data Protection Officer (DPO). This post can be shared with other organisations
- Non-EU companies will also have to comply. Nobody's getting off this one, including third-party partners

GDPR for organizations

- Every organization will have to design in data protection during roll-out of new services and technology
- Personal data now has a defined lifecycle. Organizations will have to manage it very carefully or get into an expensive muddle
- Fines have been set at up to 4 percent of turnover or €20 million, whichever is higher. A two percent figure will apply for more minor breaches.
- Requirement to notify of data breaches within 72 hours. Where breaches are not notified records still need to be kept
- Encryption avoids breach notification but only if it has been competently implemented

GDPR for individuals

- Individuals will get more control over their data, including ‘portability’ when they move from one provider to another
- Consent must be given explicitly (not passively at present) and can be withdrawn at any time
- Individuals will have to be given more information about what data is held on them and how it is processed
- Qualified rights to be forgotten and more power to object to the ay data is processed

What it all means?

Data breaches in the future will no longer be simply embarrassing clean-up jobs but financial and legal minefields opening shareholders to major losses.

TalkTalk's embarrassing series of data breaches in 2015:
The company claimed its loss-of-business and clean-up costs for the incident were around €50 million. Under the GDPR they might have faced an additional €70 million fine and the possibility of legal action by customers. There would also be the possibility of further follow-on fines for repeat offences.

What's the solution?

- Implementation of policies for handling personal data - procedures and documentation need to be updated regularly
- Inspection group – regularly reviews activities on the personal data, reports findings
- Implementation of processes in the case of data breaches.
- Introducing security for personal data in all lifecycles of a system

Last but not least

Sources

- **European Commission** http://ec.europa.eu/justice/data-protection/
- **Computer Weekly,** http://www.computerweekly.com/guides/Essential-guide-What-the-EU-Data-Protection-Regulation-changes-mean-to-you
- **Sophos, What data is at risk and what can you do about it,** https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosprotectingPII.pdf
- **The economic value of personal data for online platform, firms and consumers,** http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/
- **Computerworld, The EU General Data Protection Regulation hands power to the people ,** http://www.computerworlduk.com/it-business/analysis-eu-general-data-protection-regulation-hands-power-people-3632424/
- **The Guardian, How much is your data worth?,** http://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth
- **The Financial Times, How much is your personal data worth?,** http://www.ft.com/intl/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz2z2agBB6R