Trust vs Security

Reinforcing Trust and Security in Digital Services and in the Handling of Personal Data

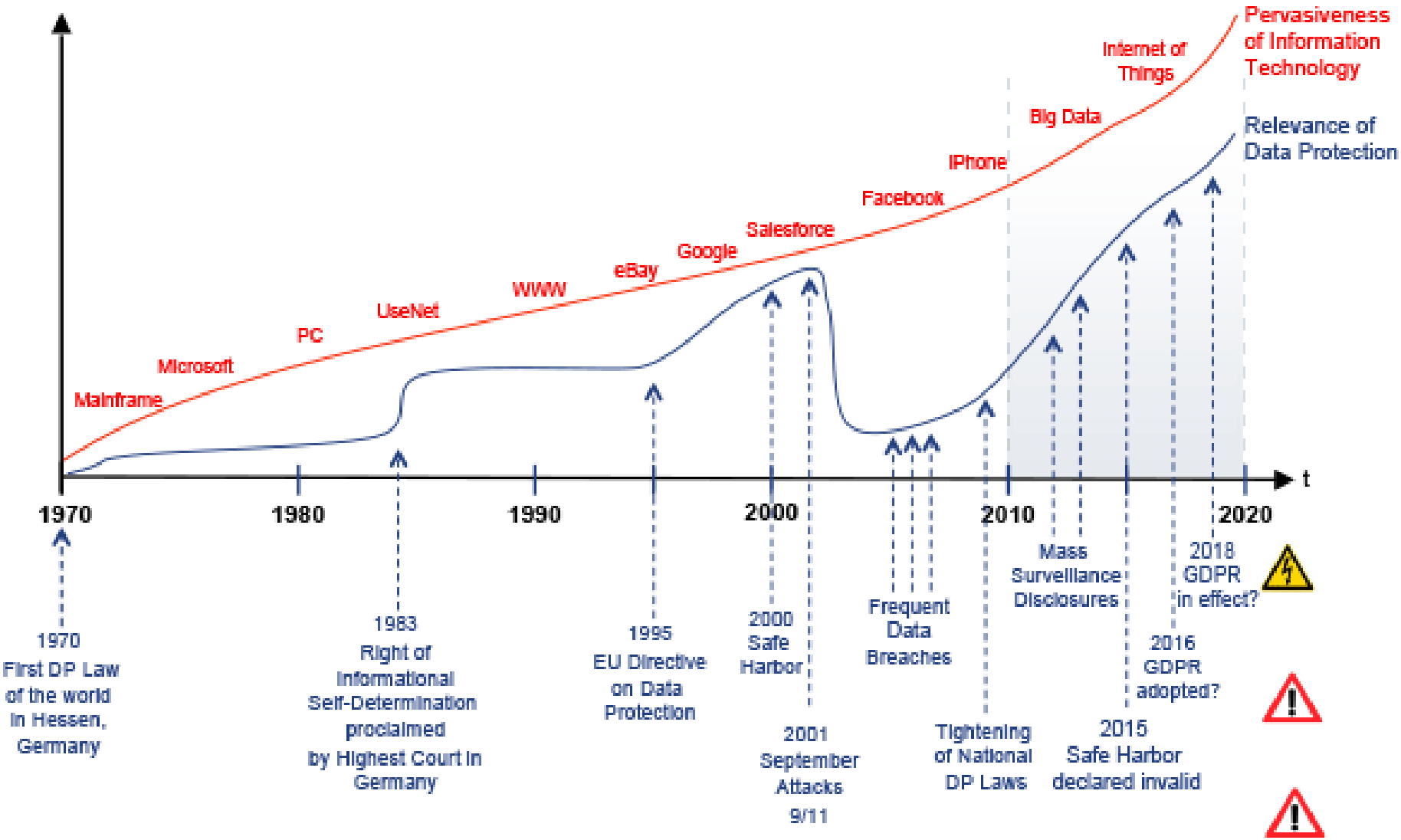
Anna Tikhomirova, Mark Lavrentev
Tyumen State University, Institute of State and Law

EU Data Protection Directive (95/46/EC) Article 2a

definition of personal data

- ***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.


Pervasiveness of Information Technology
Relevance of Data Protection
Internet of Things
Big Data
IPhone
Facebook
Salesforce
Google
eBay
WWW
UseNet
PC
Microsoft
Mainframe
t
1970
1980
1990
2000
2010
2020
1970 First DP Law of the world in Hessen, Germany
1983 Right of Informational Self-Determination proclaimed by Highest Court in Germany
1995 EU Directive on Data Protection
2000 Safe Harbor
2001 September Attacks 9/11
Frequent Data Breaches
Tightening of National DP Laws
Mass Surveillance Disclosures
2015 Safe Harbor declared invalid
2016 GDPR adopted?
2018 GDPR in effect?

Main Legal Acts, Regulating the Protection and Handling of Personal Data:

- Charter of Fundamental Rights of the EU (2000/C 364/01) (article 8);
- e-Privacy Directive (2002/58/EC);
- EU Data Protection Directive (95/46/EC);
- European Cybersecurity Strategy (Cybersecurity Strategy of the European Union An Open Safe and Secure Cyberspace 7.2.2013 JOIN(2013) 1 final);
- European Agenda on Security (COM/2015/0185 final); the General Data Protection Regulation (COM/2012/11 final).

The Main Aims and Objectives:

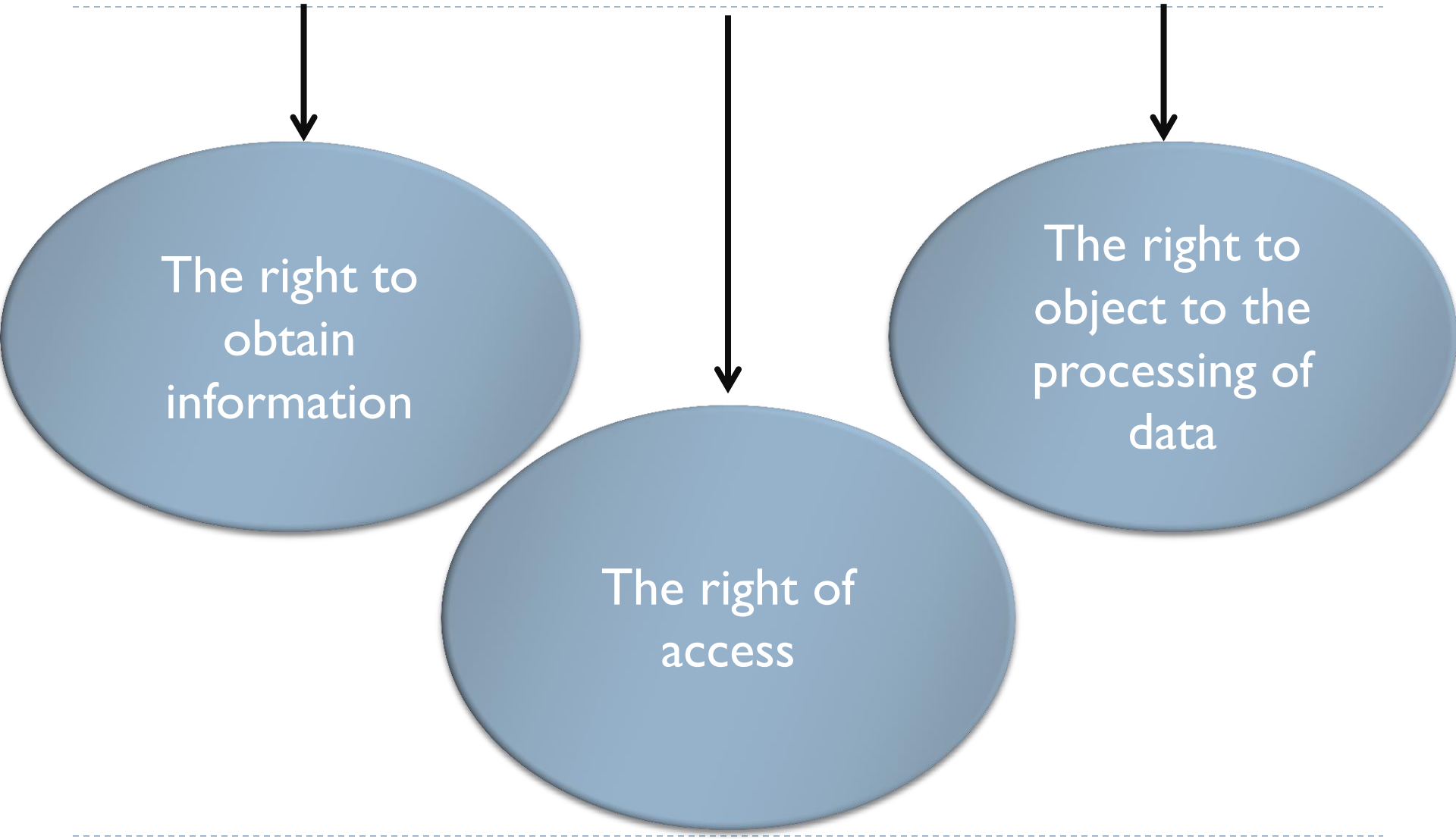
- To prevent ***cyber threats and negative impact*** on the EU economy and fundamental rights;
- To develop ***industrial and technological resources*** for cybersecurity;
- To fulfill ***gaps*** in the fast moving area technologies and offer solutions for online network security;
- To adopt ***special rules*** applying to electronic communications services (the Network and Information Security Directive).

The Main Principles of Data Quality

- personal data must be processed fairly and lawfully;

- special categories of processing: it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health etc.;

Rights of a person, whose data are processed



Major benefits of EU Data Protection Reform

- A right to be forgotten;
- Easier access to your own data;
- Allows to decide how your data is used;
- The right to know the period of time, when your data has been hacked;
- Strengthening Europe's high standards of data protection is a business opportunity;
- One continent - one law;
- The same rules for all companies;
- European regulators will be equipped with strong enforcement powers: data protection authorities will be able to fine companies, which do not comply with EU rules with up to 2% of their global annual turnover;
- Once-only principle for e-government.

Disadvantages from a privacy, data protection and IT-security perspective:

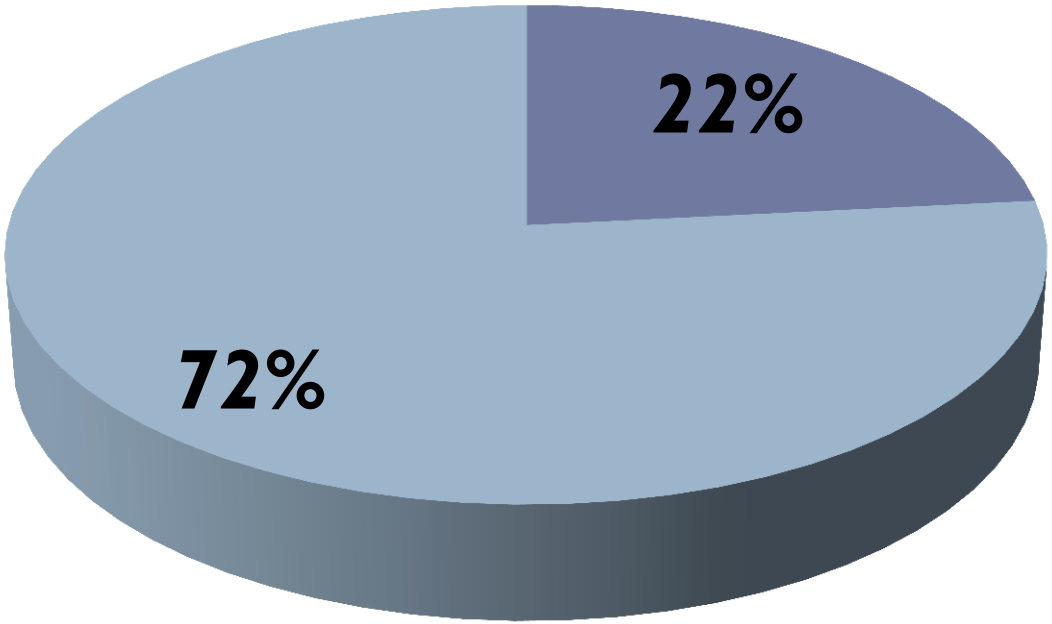
- Citizens are often not aware about what kind of data a specific public authority (data controller) processes;
- There is an inherent conflict between new privacy and security by design requirements in the proposed GDPR and the "once-only" principle;
- Member States will have 2 years to transpose the provisions into its national laws.

The Judgment of the CJEU (Case C-230/14) of 1 October 2015

- potentially far-reaching and may make data protection compliance more difficult and burdensome.

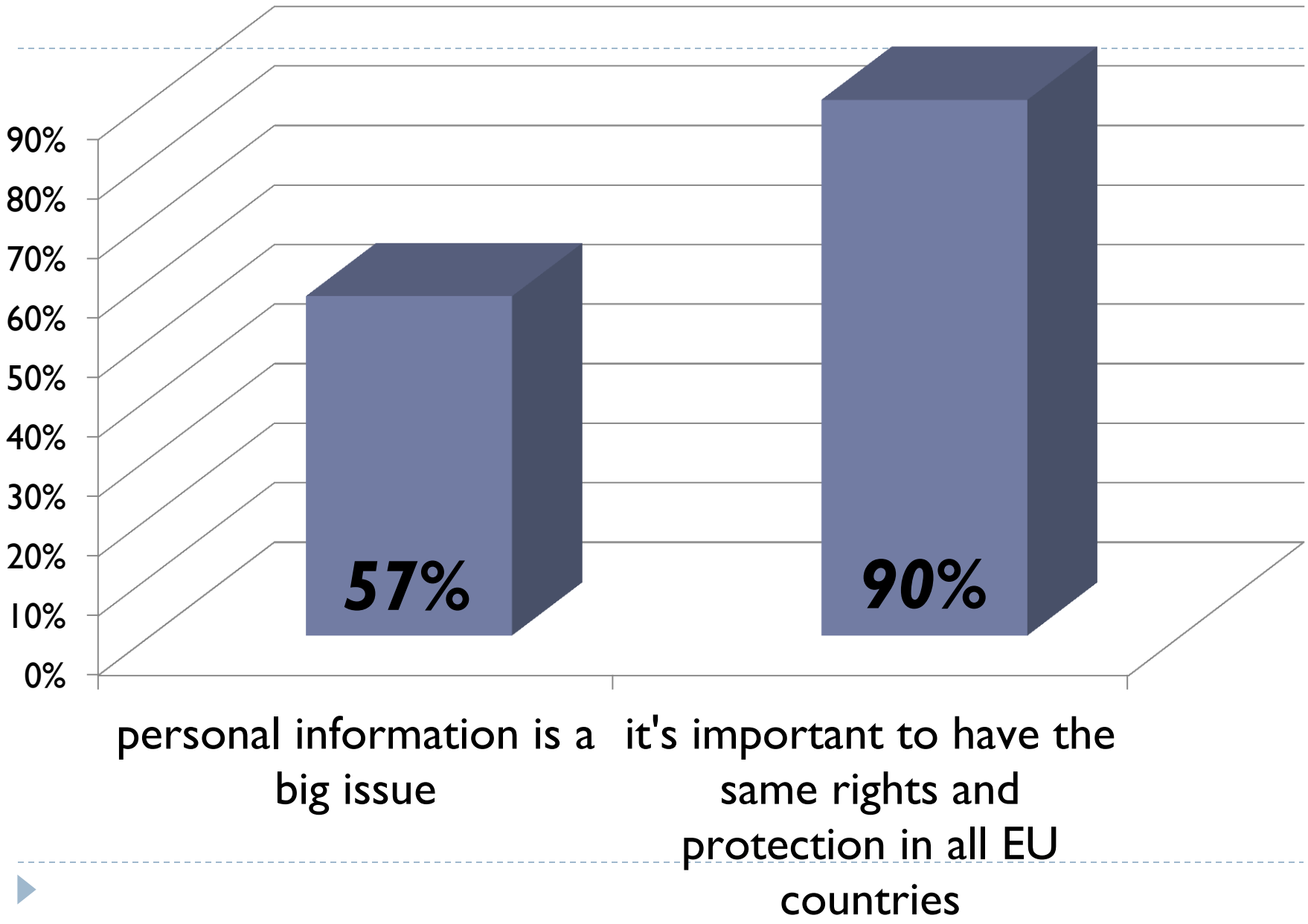
- arguably brings forward certain offered amendment to the applicable law rules set out in the draft of General Data Protection Regulation.

Europeans



- have full trust in companies
- think they are being asked for too much personal data

Europeans


90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
57%
90%
personal information is a big issue
it's important to have the same rights and protection in all EU countries

Putting a Price on Data

Surveys of consumers in the US, China, India, Great Britain, and Germany reveal that they value some types of information much more highly than others.

The approximate amount people said they would pay to protect each data type (per person, US$, 2014)

Conclusions

- Digital Single Market Strategy in the frame of personal data protection has substantial advantages for people and businesses and could get various economic benefits through the trust of users.
- However, it still has some disadvantages, such as:

- anawareness of citizens about what kind of data a specific public authority processes;
- an inherent conflict between new privacy and security by design requirements in the proposed GDPR and the "once-only" principle,

which can be solved by ***adopting the system of certain technical requirements*** for the processing of data.

Conclusions

- Adoption and implementation of DGPR
- is the main goal for achieving a new level of data protection;
- will simplify secure of data, because of the existence of one act for all member states;
- According to statistics people in EU worry about their personal data and free access to their information that's why right to be forgotten is one of the most important rights in new strategy;
- In addition, there is a need for improving literacy in IT field by carrying out special lectures in different institution. (schools, universities etc).

THANK YOU FOR YOUR ATTENTION!