Aspetos Socio Profissionais da Informática

Privacy and the GDPR (General Data Protection Regulation)

José Legatheaux Martins, Paulo Afonso Lopes

Departamento de Informática da

FCT/UNL

Lecture Outline

- What is privacy
- Privacy and the Law
- GDPR
- The Way Forward: is GDPR effective?

These slides are vey partially based on slides from the University of Glasgow and from Danny Palmer on ZDNet

Privacy Origins

- It is a very old, complex and fuzzy concept
- It was absent in old nomadic societies and also quite restrained in rural villages
- It was born with urban life, commerce and complex social relationships, at the same time as contracts, police and laws, to protect citizens from each other, specially from public "powers"
- Publilius Syrus (Roman writer of first century): "The one who reveals publicly your privacy, cannot be your friend"

Why Privacy?

- Our social life is a complex mix of cooperation and competition over resources
- If "society" knew everything on everyone, for example his intentions or her thoughts, society could protect itself from thiefs, burglars, terrorists, …
- Who could be the gatekeeper of that information, guaranteeing it would not be misused?
- What is law if evidence became superfluous?
- Some authors calls it the "the big brother society"

Privacy is Needed to Protect Persons and their Freedom

- Physical privacy: to protect your home from strangers
- To protect you from public powers abuses
- To protect you from discrimination (race, religion, opinions, ...)
- To refrain others of using their knowledge about you at their own advantage in contracts, negotiations, relationships, with rumours, …
- Lack of privacy can have serious consequences in the relationships with individuals that may want to take advantage of yourself
- **What is privacy? Is the right that a person has to control the disclosing of his or her personal information**

Your Privacy Rights are Protected by …

- Article 12 of United Nations Declaration of Human Rights
- Article 8 of the European Convention on Human Rights
- Artigo 35° da Constituição da República Portuguesa
- Lei de proteção de dados – Lei n.° 67/98 de 26 de Outubro
- Regulation EU 2016/67 – General Data Protection Regulation (GDPR)

Data is a Valuable Asset

- For Good
  - Data on commuters can be used to optimize urban transports
  - Data on people genomes, diseases, ancestors, is a key asset to public medicine studies and prevent future illnesses
- For Bad
  - Data on what you need and know is key to sell you products
  - Data on how you feel, or on the people you trust, is key to influence your opinions
  - Data on a person's genome, diseases, ancestors, may be used by insurance companies to deny contract/indemnities

GDPR is an European Union Regulation

Image: iStock

GDPR / RGPD

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, and repealing Directive 95/46/EC (General Data Protection Regulation)

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO
de 27 de abril de 2016

relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)

Went Live on May 2018

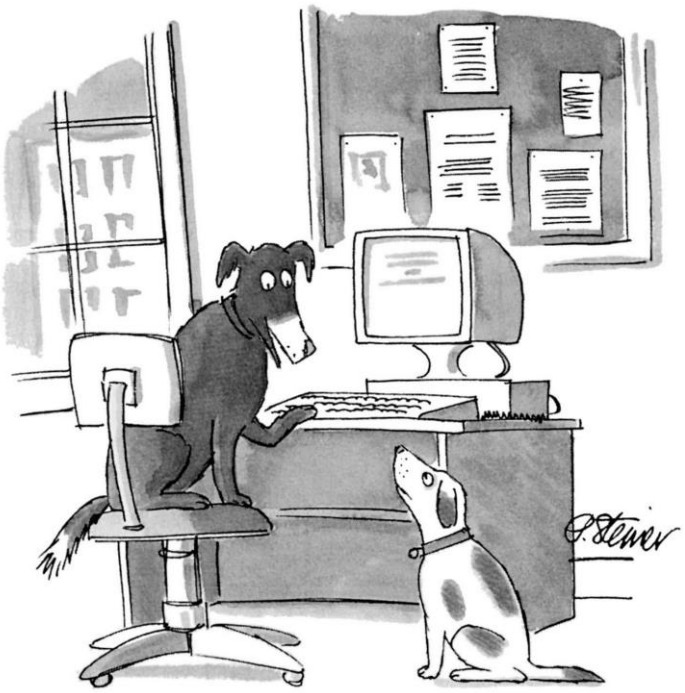
88 páginas, 173 considerandos (pág. 1-32), seguidas de 99 artigos

General Data Protection Regulation

- At its core, GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy

- The reforms are designed to reflect the world we're living in now, and brings laws and obligations - including those around personal data, privacy and consent - across Europe up to speed for the internet-connected age

Privacy in the Information Age



"On the Internet, nobody knows you're a dog."

- *On the Internet they know you're a dog*
- If you do a lot of posts in social networks, probably they know you better than your psychiatrist
- They also know:
  - The name of your owner
  - Your preferred can food
  - Where you go for a walk
  - In which trees you prefer to pee

What is Personal Information

- The types of data considered personal under the previous legislation included name, address, images and photos

- GDPR extends the definition of personal data. New additions:
  - Online identifiers, Device identifiers,
  - Cookie IDs, IP addresses,
  - Pseudonymised data,
  - Sensitive data includes genetic and biometric data

Proportionality

- *C* 4: … 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…

Nota: *C* indica considerando

Does not apply to…

- C 18: … to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. … could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

Does not apply to…

- C 19: This Regulation should not apply… competent authorities…prevention investigation … criminal offences … penalties, safeguarding against and the prevention of threats to public security…

So, to whom does it apply to? (1)

- Does the GDPR Apply to Me?

  Unless you never, ever, ever deal with the personal information of an EU subject, the GDPR applies to you.

  It does not matter whether your business is physically located in the EU. The GDPR is not based on the location of your company, but whether your company manages, transfers, or stores any personal information of an EU subject.

So, to whom does it apply to? (2)

- Am I Collecting EU Citizens' Personal Data?

  Art. 4 defines personal data as "any information related to a natural person" used to "directly or indirectly" identify the person … this information can include "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." This definition is broad and can easily apply to any app developer who maintains, stores, collects, or distributes this data. For example, companies that collect analytics concerning an EU subject's personally identifiable information (PII) are beholden to the GDPR rules as data collectors.

Data Controllers and Data Processors

- A controller is "a person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data"

- A processor is "a person, public authority, agency or other body which processes personal data on behalf of the controller"

- A controller can also be the processor, or may outsource processing to an external processor

Data Controller @ UNL

- Nas páginas da UNL e na FCT: … Tendo em conta a relação de transparência que as regras de proteção de dados pessoais visam assegurar, informa-se que todas as questões relativas ao processo de implementação do RGPD, bem como o exercício dos direitos do titular dos dados, podem ser enviadas para o seguinte endereço: nova.rgpd@unl.pt

New and Expanded Rights

- Right to be informed and need to informed consent (explicit opt-in)
- Right to erasure
- Right to data portability
- Right to rectification
- Right of access, including additional processing details
- Right to prevent automated processing, including profiling

Changes to Privacy Notices and Consent

Privacy Notices:

- More robust, concise, transparent, understandable and accessible
- Must explain personal data processed, purpose of processing, intended retention, subject rights, source of data, conditions of processing

Consent:

- Freely given, specific, informed, unambiguous,
- Demonstrable by a statement or clear affirmative action

Data Protection by Design

- Requirement for increased accountability and documentation of processing activities
- Data protection concerns reflected into design of all procedures, projects, systems
  - Good data protection compliance should be default
- Privacy Impact Assessments required for new activities and undertakings
  - Particularly for profiling, surveillance, and processing of special categories of personal data

Pseudonymisation

- Art 26: The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person….

GDPR Compliance

Under the terms of GDPR, not only will organisations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it will be obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners - or face penalties for not doing so

Data Controllers and Data Processors

- GDPR ultimately places legal obligations on a processor to maintain records of personal data and how it is processed, providing a much higher level of legal liability should the organisation be breached.

- Controllers will also be forced to ensure that all contracts with processors are in compliance with GDPR

- Even if the breach is caused by a processor, the controller is also liable

Breach Reporting and Sanctions

- Data breaches inevitably happen. Information gets lost, stolen or otherwise released into the hands of people who were never intended to see it - and those people often have malicious intent
- Mandatory breach notification
- Notify Information Commissioner (Comissão Nacional de Proteção de Dados - CNPD) within 72 hours
- Sanctions of up to €20,000,000 or 4% of annual worldwide turnover

"Fresquinhas"

- Zoom privacy: Vendor faces lawsuits over Facebook data-sharing
  - Two Zoom users are accusing the video conferencing company of sharing data with Facebook without permission. Zoom's privacy practices have come under increased scrutiny in recent weeks… The suits accuse Zoom of violating the California Consumer Privacy Act (CCPA) and other state laws. Cullen and Taylor both filed in the federal district court for Northern California under a national law governing class actions.
  - References: just Google it ☺

GDPR Advantages for Business

- Instead of having to deal with 28 different laws

- GDPR establishes one law across the continent and a single set of rules which apply to companies doing business within EU member states

- The Commission claims GDPR will save €2.3 billion per year across Europe

- This means the reach of the legislation extends further than the borders of Europe itself, as international organisations based outside the region but with activity on 'European soil' will still need to comply

Image: iStock

GDPR took effect on 25 May 2018

GDPR Two Years Later

- The Click to Accept Syndrome
- Are consumers more protected?
- Do they have alternatives to "one size fits all"?
- Three different scenarios
  - small traditional business
  - small and medium business or agencies dependent on the digital to deal with the public (e.g. banks, supermarkets, press, public services, …)
  - the giant GAFA companies (Google, Amazon, Facebook, Apple)

Barriers to Progress

- The business model: "free" service in exchange of your data
- How to price individual data?
  - Probably, all services providers should be obliged to also provide a paid version of their services at a reasonable price
  - Music and movies distribution, some news services, newspapers and Apple News are signs of new business models
- Major things missing
  - Real fight against monopolies
  - Sets of easily recognizable privacy signs (e.g. devices power consumption classification)
  - More public awareness on privacy concerns

Some Good Signs

- Technology
  - Solid (web decentralization project) Tim Berners-Lee project
  - Homomorphic cryptography
  - A cheaper way of making micro payments in an anonymous way
- Public awareness is rising
- In response, a new wave of companies is monetizing the new opportunity of offering paid-for services with heightened privacy
- Does privacy will become something only the rich can pay?

Conclusion

- Personal data became a commodity and a valuable asset for governments, public institutions and businesses
- Personal data mining is a promising tool for human progress in medicine, administration, urban management, …
- But is also a powerful weapon against individual rights
- Will privacy concepts change in the near future?