MATES ED2MIT

Education and Training for Data Driven Maritime Industry

Tutorial DMG01.02

Personal Data Protection and GDPR

Yuri Demchenko MATES Project
University of Amsterdam

Outline

Part 2. Privacy protection and regulations

- Privacy related standards
- EU General Data Protection Regulation (GDPR)

Data Privacy Protection Regulation

Security and compliance standards are also covering data protection and privacy. Specifically focused documents:

- The White House report ‘Big Data: Seizing Opportunities, preserving values’ (May 2014)
- Consumer Data Privacy In A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy (February 2012)
- HIPAA/HITECH - The U.S. Health Insurance Portability and Accountability Act (**HIPAA**) and HITECH (Health Information Technology for Economic and Clinical Health)
  - Act created by the US federal government include provisions to protect patients' private information.

- Protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.05.2018, COM(2018)
  - Based on Regulation (EU) 2016/679 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
- EU – U.S. Privacy Shield, 12 July 2016: Protection of Transatlantic data flows
  - Repeals former U.S.-EU Safe Harbor existed until 2016

White House report “Big Data: Seizing Opportunities, preserving values” (2014)

- The White House report ‘Big Data: Seizing Opportunities, preserving values’ published in May 2014.
  - The report is the result of the 90-day study commissioned by the President of the United States to examine how big data will transform the way people live and work and how big data will alter the relationships between government, citizens, businesses and consumers.

- Data security and privacy challenges in Cloud Computing and big data have been a focus of numerous study groups initiated by different governmental bodies that produced several valuable reports.
  - Wide implementation of Cloud Computing provided a basis for developing big data technologies and data-centric and data-driven applications that in their own turn facilitate cloud technologies development.
- ***The main approach in developing recommendations was to protect privacy while not hindering/restricting development of new technology for the benefit of the whole society.***
  - ***The report expresses the opinion that despite widely discussed needs for personal control of the collected e-commerce and social data, the practical use of such control is impractical due to the unmanageable volume of information and its variety. Instead, the advertisement companies and other organisational users of the personally***

Privacy Protection in Cloud and Big Data

Modern cloud based applications (in particular those that are empowered with the Big Data technologies) collect a lot of different information about users - their behaviour and preferences - and can correlate it with other information, e.g., that obtained from social networks or behavioural mobile device based applications.

- A Web browser is a common way of accessing Web information and e-commerce services.
- A ***cookie*** is a Web browser mechanism that allows for storing and retrieving user preferences, SSO and user sessions management in a distributed Web applications environment.
  - Information exchanged in the session between application site and Web browser is sufficient to identify the user/client machine.
  - If connected to other information, e.g., from the mobile application in a smartphone, the address and even name of the user can be identified.

EU Data Protection Directives and Regulations

- GDPR and former EU regulations
- Former Framework: EU data protection law is based on Directive 95/46/EC (the “Directive”), which was introduced in 1995.
  - Significant technology advances, and fundamental changes to the ways in which individuals and organisations communicate and share information.
  - Many EU Member States have taken divergent approaches to implementing the Directive, creating compliance difficulties for many businesses

- Regulation (EU) 2016/679 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), Published 4 May 2016 (78 pages)
  http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434
  - In force in all Member States since 25 May 2018, “without delay, any subsequent amendment affecting them.”

Attitude to Data Protection (EU study)

Special Eurobarometer 431 - Data protection, June 2015

http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf

- A large majority of people (71%) still say that providing personal information is an increasing part of modern life and accept that there is no alternative other than to provide it if they want to obtain products or services
- Over half of Europeans who use the Internet use an online social network at least once a week. This proportion is similar for using messaging or chat sites.
- A large majority of Europeans (69%) would like to give their explicit approval before the collection and processing of their personal data
- More than six out of ten respondents say that they do not trust landline or mobile phone companies and internet service providers (62%) or online businesses (63%).
- 67% find it important to be able to transfer personal data to a new online service provider (‘data portability’).

Trust in internet services:

- 81% of Europeans feel that they do not have complete control over their personal data online
- Only 24% of Europeans have trust in online businesses such as search engines, social networking sites and e-mail services.

GDPR main principles and key changes

- One simple technologically neutral and future-proof set of rules across the EU
  - Help building trust in the online environment (that is global, distributed, opaque)

- Everyone has the right to the protection of personal data
  - Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose.
    - **Explicit consent to be obtained**
  - Furthermore, persons or organisations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.
- Privacy impact and requirements
  - Right to be forgotten (RTBF) – complex issue for global cloud infrastructures and all information collected on the web and mobile applications
- Data portability: right to obtain data and relocate to new provider/location
- Recommendation to establish a position responsible for compliance
- Privacy by-design (PbD) principle for services and infrastructure

Principles Related to processing of personal data

Chapter II, Article 5.

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (...) (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; … inaccurate data, or not relevant, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

GDPR – Key changes

- Guaranteeing **easy access to one's own personal data** and the **freedom to transfer personal data** from one service provider to another.
- Establishing the **right to be forgotten** to help people better manage data protection risks online. When individuals no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.
- Ensuring that whenever the consent of the individual is required for the processing of their personal data, it is always **given by means of a clear affirmative action**.
- Ensuring a **single set of rules** applicable across the EU.
- **Clear rules** on when EU law applies to data controllers **outside the EU**.

EU – U.S. Privacy Shield – **Invalidated 15 August 2020 the European Court of Justice (ECJ)**

- EU-U.S. Privacy Shield: stronger protection for transatlantic data flows
  - Adopted *12 July 2016.* Repeals **former Safe Harbor Framework**
  - http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm
- *The new framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers.*
- The new arrangement includes:
  - strong data protection obligations on companies receiving personal data from the EU
  - **safeguards on U.S. government access to data;**
  - effective protection and redress for individuals;
  - annual joint review to monitor the implementation.
- What will it mean in practice for American companies
  - Self-certify annually that they meet the requirements.
  - Display privacy policy on their website.
  - Reply promptly to any complaints.
  - If handling human resources data: Cooperate and comply with European Data Protection Authorities.

EU – U.S. Privacy Shield: Obligations and Mechanisms (historical, obsolete)

- **Strong obligations on companies handling data**
  - **Regular reviews** of participating companies and **effective supervision mechanisms**
    - If companies do not comply in practice they face sanctions and removal from the Privacy Shield list.
  - **Tightened conditions for onward transfers** to third parties by the companies participating in the scheme.
  - **Data retention** limitation: Companies may keep personal data only as long as this serves the purpose the data was collected for.
- **Clear limitations and safeguards with respect to U.S. government access**
  - **Strong commitments** in written form by the Office of the Director of National Intelligence (White House), ruling out indiscriminate mass surveillance on data transferred under the Privacy Shield arrangement.
  - Additional document how **bulk collection of data** could only be used under specific preconditions. The new document once more **rules out the use of indiscriminate mass surveillance by the U.S.**
  - To regularly **monitor the functioning of the arrangement** there will be an annual joint review, which will also include the issue of national security access.
  - The Privacy Shield is a **living mechanism**, which will be reviewed continuously
- **Effective protection of European's rights**

  Any citizen who considers that their data has been misused under the Privacy Shield scheme will benefit from several accessible and affordable dispute resolution mechanisms:
  - Complaints to be preferably resolved **by the company** itself.
  - Privacy Shield companies can opt between **free of charge Alternative Dispute resolution** (ADR) or voluntary submission to the oversight of the **EU Data Protection Authorities**.
  - In any event, individuals can go to the EU Data Protection Authorities who will channel their complaints to the **Department of Commerce** and/or the **Federal Trade Commission (FTC)** to ensure that complaints by individuals are investigated and resolved.
  - Further resolution mechanisms: **arbitration mechanism, handled by** an **Ombudsperson** independent from the US intelligence services.

New EU-US Data Sharing Framework

- **The European Commission is to issue updated standard contractual clauses (SCCs) that will allow organisations in the EU to exchange data with the US**
- companies gearing up to replace Privacy Shield with legal agreements known as standard contractual clauses (SCCs)
- European Court's judgment had for the first time "put a spotlight" on the need for businesses to carry out legal assessments before they start sharing data with countries outside the EU.
  - The ECJ has raised questions over the US Executive Order 12333 https://www.cia.gov/about-cia/eo12333.html), which has been used by the US National Security Agency as a legal basis for collecting data passing through the datacentres of big tech companies, including Google
  - Questions remain whether data transfers from Europe to the US "under any mechanism" would comply with European human rights law,
  - Companies transferring data to US firms would be on firmer ground under EU law if they could show that, in reality, their US business partners rarely received orders under FISA to hand over private data. (US law is Section 702 of the US Foreign Intelligence Surveillance Amendments Act (FISA))
    - US companies cannot refuse to respond to orders to hand over data to US law enforcement and intelligence agencies under FISA.
    - But they can publish how many requests they receive, allowing European companies to benchmark the risks of transferring personal data overseas.

- **Germany Presidency message : Time for digital autonomy**
- The European Data Protection Board (EDPB), an independent group of 30 data protection regulators from Europe and the European Economic Area, has criticised the lack of safeguards for EU citizens under US surveillance laws, which allow the collection and analysis of the private data of non-US citizens for national security.

European Data Protection Board (EDPB) and **Standard Contractual Clauses (SCC)**

- Standard contractual clauses for data transfers between EU and non-EU countries https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
- The European Data Protection Board (EDPB) is an independent European body
  - https://edpb.europa.eu/edpb_en
  - Contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.
  - Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1 Adopted on 4 May 2020 - https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Standard Contractual Clauses (SCC) – On the way to future e-Law

- Commission Decision 2001/497/EC of 15 June 2001
  on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC
- Commission Decision 2004/915/EC of 27 December 2004
  Amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries
- Commission Decision 2010/87/EU of 5 February 2010
  Standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

EDPB Guidelines 05/2020 on consent under Regulation 2016/679

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

2 Consent in Article 4(11) of the GDPR
3 Elements of valid consent
3.1 Free / freely given
3.1.1 Imbalance of power
3.1.2 Conditionality
3.1.3 Granularity
3.1.4 Detriment
3.2 Specific
3.3 Informed
3.3.1 Minimum content requirements for consent to be 'informed'
3.3.2 How to provide information
3.4 Unambiguous indication of wishes
4 Obtaining explicit consent
5 Additional conditions for obtaining valid consent
5.1 Demonstrate consent
5.2 Withdrawal of consent
6 Interaction between consent and other lawful grounds in Article 6 GDPR
7 Specific areas of concern in the GDPR
7.1 Children (Article 8)
7.2 Scientific research
7.3 Data subject's rights
8 Consent obtained under Directive 95/46/EC

Still to be analysed to match current practice

Cloud Security Alliance: Cloud and Big Data Security and Compliance - https://cloudsecurityalliance.org/

- Cloud Security requirements and best practices
- Cloud Computing Compliance
  - Covering (Big) Data on clouds
- Target audience: Auditors, Cloud Service Providers, Security Specialists, Developers, Users

CSA Code of Conduct for GDPR Compliance

https://cloudsecurityalliance.org/privacy/gdpr/code-of-conduct/

For Cloud Service Providers

- **Flexibility:** Can be applied to any cloud delivery model - IaaS/PaaS/SaaS
- **Transparency:** Provides cloud customers with clear understanding and transparent view of what Cloud Service Provider is doing
- **Rigor:** The CSA CoC provides a rigorous and proven template to adhere to GDPR privacy requirements
- **Utility:** Cloud customers of any size can use this tool to evaluate the level of personal data protection offered by different CSPs (and thus to support informed decisions)
- **Completeness:** Enables CSPs of any size and geographic location with guidance to comply with European Union (EU) personal data protection legislation and to disclose the level of personal data protection they offer to customers.

CSA CoC Self-assessment and Compliance

- The Code of Conduct Self Assessment consists of the voluntary publication on a public registry, the CSA Security, Assurance and Transparency Registry (CSA STAR) of two documents:
  - Self Assessment Statement of Adherence and
  - Self Assessment results based on the PLA Code of Practice (CoP) Template - Annex 1
- The Self Assessment covers compliance to GDPR of the service(s) offered by a CSP.
  - A submission fee of €1495 euros is required to facilitate the publication.
  - After publication, the company will receive authorized use of a Compliance Mark, valid for 1 year.

Summary and take away

- Data Protection and Privacy in cloud is regulated by numerous group of standards and regulatory documents
  - European General Data Protection Regulation (GDPR) provides common framework for all EU Member States
  - EU-U.S. Privacy Shield is a new framework for cross-Atlantic cooperation

Additional materials

- Security and compliance standards

European Union Cloud Computing and Data Protection Directives and Regulations

- GDPR (General Data Protection Regulation). Legal Act, Official Journal of the European Union, 27 April 2016 (78 pages)
  http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434

USA Privacy related document

The following documents are the main documents cited in the White House Big Data Privacy report that are related to privacy protection in our networked and IT driven world that experiences Big Data technologies emergence.

- Big Data: Seizing Opportunities, preserving values, Executive Office of the President, May 2014, Washington. [online] http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf
- Randy Reitman, “Deep Dive: Updating the Electronic Communications Privacy Act,” *Electronic Frontier Foundation*, December 2012, https://www.eff.org/deeplinks/2012/12/deep-dive-updating-electronic-communications-privacy-act
- European Commission, “Commission Proposes a Comprehensive Reform of the Data Protection Rules,” January 25, 2012, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
- OECD Work on Privacy, Organization for Economic Cooperation and Development, 2012 http://www.oecd.org/sti/ieconomy/privacy.htm
- Samuel Warren and Louis Brandeis, “The Right to Privacy,” 4 *Harvard Law Review* 193, 195 (1890).
- President Barack Obama, *International Strategy for Cyberspace*, The White House, May 2011, http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework
- President Barack Obama, Consumer Data Privacy In A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy, The White House, February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
- President Barack Obama, Making Open and Machine Readable the New Default for Government Information, Executive Order 13642, May 2013, http://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government
- President Barack Obama, Making Open and Machine Readable the New Default for Government Information, Executive Order 13642, May 2013, http://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government