

EU POLICIES IN DATA GOVERNANCE

THE NEW CHALLENGE ON THE FIELD OF PUBLIC ADMINISTRATION



By Georgios Roussaris

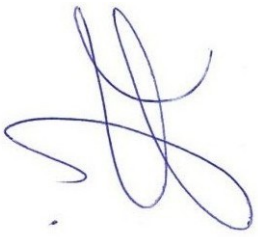
Master Degree in International Public Administration

University of Macedonia

Department of International and European Studies

I hereby declare, that all the data used in this work, have been obtained and processed according to the rules of the academic ethics as well as the laws that govern research and intellectual property. I also declare that, according to the above mentioned rules, I quote and refer to the sources of all the data used and not constituting the product of my own original work.

Georgios Roussaris



Acknowledgements

I would like to express my gratitude to Professor Dimitrios Skiadas, President of the Department of International and European Studies in the University of Macedonia, for his support during the master's courses, for encouraging me to conduct my thesis work and for his valuable instructions and suggestions throughout the period of my thesis' production. Furthermore, I would like to add a special thanks to Professor IliasKouskouvelis, Dean of the School of Social Sciences, Humanities and Arts of the University of Macedonia, for sharing his knowledge during his courses and for his valuable guidance during the period of my thesis' conduction.

Dedication

I would like to dedicate my work to all the people that supported my pursuit of obtaining this degree. My parents, Aris and Maria, my grandmother Paraskevi and my brother Konstantinos. They give me unbelievable confidence and support in order to accomplish my goals.

I would also like to dedicate this to my two grandparents, Dimitris and Konstantinos, who have both passed away. They taught me how to chase my dreams with confidence, affection and hard work. I miss them every day, but I am sure that they're still somehow watching out for me.

Table of Contents

Introduction.....	(1)
1.1 Data and Information Significance.....	(1-3)
1.2 Data Governance Background.....	(3-4)
1.3 Data Governance Landscape.....	(4-6)
1.4 Principles of Data Governance.....	(5-6)
1.5 Data Governance Goals.....	(6-7)
1.6 Relation of Data Governance to other sectors related to data.....	(7)
1.6. a. Master Data Management.....	(7-8)
1.6. b. Data Management.....	(8-9)
1.6. c. Data Warehouses.....	(9-10)
1.6. d. Data Lakes.....	(10)
1.6. e. Information & IT Governance in relation to Data Governance.....	(10-11)
2. Developments of Data Governance policies in EU.....	(11)
2.1 Digital Agenda & Digital Single Market Strategy.....	(11-14)
2.2 European Agenda for collaborative economy.....	(14)
2.3 eIDAS Regulation.....	(15)
2.4 e-Government Action Plan 2016-2020.....	(15-16)
2.5 Horizon 2020.....	(16)
2.6 Open Science Cloud.....	(16-17)

2.7 Urban Agenda & European smart cities’ initiative (Initiatives related to digital society)	(17-18)
2.8 Health Data Policies in EU.....	(18)
2.8. a. Digital Health Policies in EU.....	(18-19)
2.8. b. Legislation around health data.....	(19-20)
2.8. c. Cross border interoperability for the exchange of health data.....	(20-21)
2.8. d. Cross border exchange of data.....	(21)
2.8. e. Big Data - Real World Data & Cloud Computing.....	(22-23)
3. GDPR	(23)
3.1 Relation between concepts of privacy and data protection.....	(23-24)
3.2 Background of data protection in EU.....	(24-25)
3.3 GDPR concept.....	(26)
3.4 Relation to the concept of Data Governance.....	(26-27)
3.5 Key changes on the GDPR.....	(27)
3.5. a. General provisions & principles.....	(27-28)
3.5. b. Transfers of personal data.....	(28-29)
3.5. c. Security of personal data – general obligations – national derogations – DPO – sanctions & liability.....	(29-30)
3.5. d. Individual rights under GDPR.....	(30)
3.5. e. Relation between e-Privacy Directive & GDPR.....	(30-31)
4. Policies related to Data Governance in other countries.....	(31)
4.1 USA.....	(31-38)
4.2 CHINA.....	(38-44)
4.3 JAPAN.....	(44-45)
4.4 SOUTH KOREA.....	(45-47)
4.5 DENMARK.....	(47-49)
5. Case studies on Data governance, data protection & privacy.....	(50)
5.1 Maximillian Schrems case study.....	(50-53)
5.2 “This is your digital life” case study.....	(53- 65)
6. Conclusion.....	(65-67)

ACRONYMS

ERP: Enterprise Resource Planning

CRM: Customer Relationship Management

AI: Artificial Intelligence

EU: European Union

EC: European Commission

USA: United States of America

DG: Data Governance

MDM: Master Data Management

DM: Data Management

SCM: Supply Chain Management

IT: Information Technology

DA: Digital Agenda

DSMS: Digital Single Market Strategy

ENISA: European Network and Information Security Agency

GDP: Gross Domestic Product

TOOP: The Once Only Principle Project

ICT: Information and Communication Technologies

EGE: The European Group in Science and New Technologies

GDPR: General Data Protection Regulation

EHR: Electronic Health Records

ECHR: European Convention on Human Rights

DPD: Data Protection Directive

EEA: European Economic Area

FTC: Federal Trade Commission

HIPAA: Health Insurance Portability and Accountability Act

HITECH: Health Information Technology for Economics and Clinical Health

FCC: Federal Communications Commission

PMA: President's Management Agenda

IOT: Internet of Things

NSA: National Security Agency

CJEU: Court of Justice of the European Union

CEO: Chief Executive Officer

CTO: Chief Technology Officer

1. Introduction

The new millennium found nations faced with new major challenges. Emerging wars in the east, terrorist attacks in the west, internet explosion everywhere and in the middle of everything, the innovation of the need for more qualitative and quantitative data and information from anyone, for anyone and anything. The importance of data and information technologies emerged by the technological innovations of the 20th and 21th century but also by the necessity of states, international organizations and private corporations to integrate and leverage these technologies to their models of operation in order to evolve and adjust in a world that is being digitized enormously and rapidly. In the following years, the necessity of data had become a prerequisite for every serious operational sector which involves and defines human life. From health to economics and national defense to space operations, everything has to do with data and information. Data became not only an asset for major corporations and governments but also a good that terms public and private policies and opens a new era for both legal science and every sciences' sector of human involvement. One of the aftermaths of digital evolution of societies is the creation and establishment of new ways of governance. Data governance or governance of data is an emerging new area of governance, whose significance will be determined by the willingness of governments, international institutions and private corporations to cooperate and establish a crucial, for the following generations, form of governance with respect to human integrity, growth and stability. In the following chapters, the formation of this new section of governance, the relation with other sectors that are connected with data harvesting, control and use, and its relation with other forms of digital governance, will all be examined. Furthermore, the policies, strategies and legislation established from EU that interconnect and integrate this form of governance with traditional ones, will be addressed. In addition to that, a comparative approach through other major developed countries will show the progressive steps that EU is following in order to establish and implement a coherent, transparent and accountable approach in the way that data should be governed. Finally, the case studies of Maximilian Schrems and the Facebook-Cambridge Analytica scandal will demonstrate a different point of view, more individualistic in the first case and more corporate-centric in the second one, around this type of governance.

1.1 DATA & INFORMATION SIGNIFICANCE

In order to estimate the essence and the value of a good data governance plan or policy, either the latter takes place in the public or private sector, data should be understood in the first place. On the one hand, as a word, data means “information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a

computer”¹. On the other hand, information as a concept is defined as “any entity or form that provides the answer to a question of some kind or resolves uncertainty”². As concepts, data and information are nearly related and interchangeable to each other but the main difference between them is that information is basically data formatted in a proper way that allows it to be used by human beings for specific utilities and tasks³.

Throughout the 20th and of course the 21th century, data have been collected and used by almost every big organization and institution across the globe. Governments, businesses and non-governmental organizations collect, process and use data in various ways to make decisions, to create policies or even to design and structure new fields of scientific research. With the explosion of information technologies and computer engineering in the 20th century, data became a tool of understanding and decision-making for every sector which is included in the everyday life of a modern human society.

Nowadays, data can affect economies, health policies, geopolitical relations between states, education, national security, justice, etc. However, data as a fact is not something new. From the ancient wedge-shaped writing (cuneiform) to the filing systems of Victorian bureaucracy and the “information explosion” in the European continent between 1550-1750, data had always played a crucial role in governments, organizations and institutions⁽⁴⁾⁽⁵⁾. Until the 1990s, data had been seen as a by-product of running governments, institutions and businesses. Since then (early 1990s), and until nowadays the value of data as an asset, has changed drastically. The creation of sophisticated electronic systems, such as modern computers, smartphones and the invention of the internet, has changed the dynamic of data in a world which is more globalized than ever before⁶. Processes and decisions have been modernized through data and data analysis. The creation of complex data repositories, data warehouses, Enterprise Resource Planning (ERP) and Customer Relationship Management (CRMs) have led to growing investment in the sector of data management and furthermore in master data management⁽⁷⁾⁽⁸⁾.

Nowadays, the complexity and volume of data continue to grow rapidly and enormously across the private and public sector. Moreover, the creation of new sectors of technology, such as the Artificial Intelligence (AI), have established new demands to the combination, collection, storage and presentation of information. Innovative approaches across companies have also established the realization that data management alone cannot solve the problem of utilization of data. That occurs

¹<https://dictionary.cambridge.org/dictionary/english/data>.

²<https://www.merriam-webster.com/dictionary/information>

³<https://www.computerhope.com/issues/ch001629.htm>

⁴Hobart ME and Schiffman ZS. 1998 Information Ages: Literacy, Numeracy, and the Computer Revolution. Baltimore: Johns Hopkins University Press; Agar J.2003 The Government Machine: a Revolutionary History of the Computer. Cambridge, MA: MIT Press.

⁵Rosenberg D.2003, Early modern information overload, Journal of the History of Ideas.64,1-9.

⁶Majid Al-Ruithi, ElhadjBenkhelifa, Khawar Hameed. Data Governance Taxonomy: Cloud versus Non Cloud.

⁷Begg,C ; Caira T. Exploring the SME Quandary: Data Governance in Practice, in the Small to Medium Enterprise Sector. Electron. J. Inf. Syst. Eval. 2012, 15, 3-13.

⁸Buffenoir, E; Bourdon, I. Managing extended organizations and data governance. Adv. Intell. Syst. Comput. 2013, 205, 135-145.

because, as a field of activation, data management solutions are too expensive and cannot keep up with business realities, regulations and decision-making policies⁹.

As, Andreas Weigend, former chief scientist at Amazon, puts it: “Data is the new oil”¹⁰. This is a statement which could be translated and analyzed in various ways. One important conclusion drawn from the statement above is that governments and businesses now behave and face data as a strategic and organizational asset for good decision-making policies and economic growth. As an asset, data have to be shared, taking in consideration the value of data ownership and responsibility. The paradigm of the 911 Commission, which blamed the top governmental agencies in the USA (FBI, CIA, NSA and the executive branch) for an unwillingness or inability to share vital security data, can depict the reason why data should be utilized as a shared asset agreed upon boundaries of ownership and responsibility¹¹. For many governments and businesses data are spread across multiple and complex silos that are not connected to each other. In order to maximize their performance and at the same time their profit, governments and businesses have to handle data in a more shared-properly way¹². Also, high quality of data leads to more effective decision-making policies and improves operational, tactical and strategic performance¹³.

The reasons described previously establish the fact that data governance, as a concept of practices, policies and standards, provides a foundation for valuing and perceiving profoundly all data that organizations and governmental agencies collect and maintain to their repositories¹⁴.

1.2 DATA GOVERNANCE BACKGROUND

Back in the early days of IT, data were managed by organizations in a series of files which were difficult to control and also time consuming to create¹⁵. In the 1970s Codd presented the concept of relational database as a set of rules which described the needs of a database management system in order to be relational¹⁶. Furthermore, the concept of storing data in a regular and organized way seemed to have a good prospect for the future, but in that time organizations still needed to

⁹Niemi, E. Designing a Data Governance Framework. In Proceedings of the IRIS Conference, At Oslo, Norway 18 August 2011; Volume 14.

¹⁰Executive Report: Demystifying Health Data Governance by Dale Sanders, Senior Vice President, Strategy, Health Catalyst.

¹¹<https://www.forbes.com/sites/ciocentral/2016/06/22/the-case-for-data-governance/#6e1631f354be>

¹²The IBM Data Governance Council Maturity Model: Building a roadmap for effective data governance.

¹³Australian Institute of Health and Welfare, Data Governance Framework, 2014.

¹⁴<https://www.forbes.com/sites/ciocentral/2016/06/22/the-case-for-data-governance/#6e1631f354be>

¹⁵Codd, E. F (1982), Relational database: A practical foundation for productivity. Communications of the ACM, 25(2), 109-117. <https://dl.acm.org/citation.cfm?doi=358396.358400>

¹⁶Codd, E. F (1970). A relational model of data for large shared data banks. Communications of the ACM, 13(6), 377-387. <https://dl.acm.org/citation.cfm?doi=362384.362685>

program at a low level in order to interact with these systems¹⁷. Relational databases continued to be explored in the 1970s, and finally in 1979 Software Development Laboratories released Oracle Version 2, which is considered to be the first commercial relational database system based on Structured Query Language¹⁸. That helped organizations increase their productivity in data. Relational database systems helped organizations to solve the problem of data access and since then, the latter had started seeking for new ways in order to increase the control and understanding of their data. In the 1980s, focus gravitated towards data security and other management functions of data¹⁹. Also, understanding of collected data became more important for organizations and metadata management systems (e.g. data dictionary) helped in that. This knowledge, concerning the understanding of data which were collected by organizations, demonstrated the importance of data to them²⁰.

In the 1990s organizations started treating data as an asset similar to people or money and realized that data had to be governed in a more sophisticated and structural manner²¹. During that period, the concept of quality of data warehouses also came as a tool for combining varied data sources into a unified and solid data system²². With the new millennium, questions were raised about where decision-making rights and responsibilities for assets of IT technology should be laid upon²³. Also, the concept of data stewardship between different organizational sectors and employees led to the creation of the first data governance frameworks⁽²⁴⁾⁽²⁵⁾⁽²⁶⁾.

¹⁷Codd, E. F (1982), Relational database: A practical foundation for productivity. Communications of the ACM, 25(2), 109-117.<https://dl.acm.org/citation.cfm?doi=358396.358400>

¹⁸Oracle Corporation (2007). Oracle timeline. Profit Magazine, 12(2), 26-33.
<https://www.oracle.com/index.html>

¹⁹Egelstaff, R., Wells, M. (2013). Data governance frameworks and change management. Studies in Health Technology and Informatics, 193, 108-119.<https://www.ncbi.nlm.nih.gov/>

²⁰Levitin, A.V., Redman, T. C (1998). Data as a resource: Properties, implications, and prescriptions. Sloan Management Review, 40(1), 89-101.<https://sloanreview.mit.edu/>

²¹Levitin, A.V., Redman, T. C (1998). Data as a resource: Properties, implications, and prescriptions. Sloan Management Review, 40(1), 89-101.<https://sloanreview.mit.edu/>

²²Ramakrishnan, R., Gehrke, J. (2000). Database management systems (2nded). New York, NY: Mc Graw-Hill.

²³Weill, P. (2004). Don't just lead, govern: How top-performing firms govern IT. MIS Quarterly Executive, 3(1), 1-21.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=317319

²⁴Data Management Association (DAMA). (2010). Guide to the data management body of knowledge. Bradley Beach, NJ: Technics Publications.

²⁵Seiner, R.S. (2014). Non- invasive data governance: The path of least resistance and greatest success. Basking Ridge, NJ: Technics Publications.

²⁶Plotkin, D. (2014). Data stewardship: An actionable guide to effective data management and data governance. Waltham, MA: Morgan Kaufmann.

1.3 DATA GOVERNANCE LANDSCAPE

According to Egelstaff and Wells, there hasn't been a single universal data governance framework developed²⁷. There are many organizations in the private sector, such as IBM and Oracle, which develop their own strategy and framework around data governance but there are also examples in the public sector as well, such as the US Department of Defense. The latter has developed and worked with such frameworks, in association with prestigious universities, such as the MIT and Harvard, but also with organizations from the private sector²⁸. The truth is that there cannot be a unified and single DG framework because organizations in both sectors (private and public) vary in their operations, strategies, structures and needs. In many ways they have to coexist and cooperate in different levels of decision-making but on the other hand the diversity and disparity of their operations and strategies cannot allow them to handle data in a single way. Furthermore, a data governance framework has to do with the approach of an organization, company or a government agency upon the collection, management and storage of data. So, not only does it define the strategies and operations of an organization but most importantly it shapes the entire philosophy of businesses, processes and people in and out of an organization²⁹.

As it happens with the no-existence of a single data governance framework, the same situation exists with data governance definitions. There are numerous definitions of data governance. MDM Institute defines data governance as “the formal orchestration of people, processes and technology to enable an organization to leverage data as an enterprise asset”. The Data Governance Institute states that “data governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed- upon models, which describe who can take what actions with what information, and when, under what circumstances, using what methods”.

Oracle Corporation defines data governance as “the specification of decision rights and an accountability framework to encourage behavior in the valuation, creation, storage, use, archival and deletion of data and information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of data and information in enabling an organization to achieve its goals”³⁰. The IT Encyclopedia defines data governance as “the overall management of the availability, usability, integrity, and security of the data employed in an enterprise. A sound data governance program includes a governing body or council, a defined set off procedures, and a plan to execute those procedures”³¹. Last but not least, Data Management Association defines data governance as “the exercise of authority,

²⁷Egelstaff, R., Wells, M. (2013). Data governance frameworks and change management. *Studies in Health Technology and Informatics*, 193, 108-119.

²⁸Egelstaff, R., Wells, M. (2013). Data governance frameworks and change management. *Studies in Health Technology and Informatics*, 193, 108-119.

²⁹https://www.sas.com/en_us/insights/articles/data-management/what-is-a-data-governance-framework.html

³⁰An Oracle White Paper on Enterprise Architecture: Enterprise Information Management: Best Practices in Data Governance, May 2011.

³¹Rouse, M. Data governance definition.<https://whatis.techtarget.com/search/query?q=data+governance>

control and shared decision-making (planning, monitoring and enforcement) over the management of data assets”³².

1.4 PRICIPLES OF DATA GOVERNANCE

Every sector of human evolving, either it is technological or economical, politics, defense, etc., has its own principles in order to protect not only the values and integrity of the organization or government but most importantly to establish a clear, solid and safe environment for the people whose data are used for different reasons and with disparate patterns. According to the Royal Society: “the overarching principle is that systems of data governance should promote human flourishing”. This opinion is a human-centric approach around use, collection, processing and valuation of data. In other words, data should be used for the wellbeing and prosperity of human race and not the other way around. This approach is built upon four guiding principles, whose main goal is to promote the overall principle of human flourishing. These principles promote that the systems of data governance should³³:

- 1) Protect individual and collective rights and interests.
- 2) Ensure that trade-offs affected by data management and data use are made transparently, accountably and inclusively.
- 3) Seek out good practices and learn from success and failure.
- 4) Enhance existing democratic governance.

On the other way around, principles of DG are structured in a more enterprise-centric path. According to the Data Governance Institute, the founding principles of DG are³⁴: Integrity, Transparency, Auditability, Accountability, Stewardship, Standardization and Change Management. This approach is established around the framework of businesses, processes and people, mainly within an organization’s operational framework and in accordance with the relevant legislation, but also with fragments of respect to the people outside the decision-making field of DG.

1.5 DATA GOVERNANCE GOALS

According to the dictionary.com, the definition of the term governance is: “to rule over; to influence and guide; to control”³⁵. From this sentence it is understandable the fact that data governance, in general, strive for ruling, influencing, guidance and controlling. These goals come from the etymological foundations of the word

³²Cheong, L.K.; Chang, V. The Need for Data Governance: A Case Study. In Proceedings of the 18th Australasian Conference on Information System, Toowoomba, Australia, 5-7 December 2007; Volume 100, pp.999-1008.

³³British Academy for the humanities and social sciences, The Royal Society, Data Management and use: Governance in the 21th century. A joint report by the British Academy and the Royal Society, June 2017, p 9.

³⁴<http://www.datagovernance.com/goals-and-principles-for-data-governance/>

³⁵<http://www.dataversity.net/data-governance-not-governing-data/>

governance. The same situation exists on the concept of governance of data. The Data Governance Institute provides the following seven universal goals for DG programs. As a result, DG programs should³⁶:

- 1) Enable better decision-making.
- 2) Protect the needs of data stakeholders.
- 3) Reduce operational friction.
- 4) Build standard, repeatable processes.
- 5) Train management and staff to adopt common approaches to data issues.
- 6) Ensure transparency of processes.
- 7) Reduce costs and increase effectiveness through coordination of efforts.

Also, there are views from the corporate world about DG goals. According to Oracle Corporation the main goals of DG are the following³⁷ :

- 1) To define, approve, and communicate data strategies, policies, standards, architecture, procedures and metrics.
- 2) To track and enforce conformance to data policies, standards, architecture and procedures.
- 3) To sponsor, track and oversee the delivery of data management projects and services.
- 4) To manage and resolve data related issues.
- 5) To understand and promote the value of data assets.

It is intelligible, from the information mentioned above, that the goals of DG are closely related to the principles of DG and in most occasions emerge from the etymological origin of these principles.

1.6 RELATION OF DG TO OTHER SECTORS RELATED TO DATA

1.6.a. MASTER DATA MANAGEMENT

Master data management can be defined as an extensive and broad method, which is used by organizations and governmental agencies in order to provide references of data required to operate across several applications and organizations³⁸. Paradigms of such applications could be the Customer Relationship Management (CRM), Enterprise Resource Planning (ERP) and Supply Chain Management(SCM)³⁹. In other words, MDM is “comprised of processes, governance,

³⁶<http://www.datagovernance.com/goals-and-principles-for-data-governance/>

³⁷ An Oracle White Paper on Enterprise Architecture, Enterprise Information Management: Best Practices in Data Governance, May 2011, p 4.

³⁸ Study on Standard-Based Archival Data Management, Exchange and Publication, Final Report, ISA² Action 2017.01, p 20.

³⁹https://en.wikipedia.org/wiki/Customer-relationship_management

policies, standards and tools that consistently define and manage the critical data of an organization to provide a single of reference”⁴⁰. The main task of MDM is to provide the right processes for the collection, aggregation, matching, consolidation, quality-assurance and distribution of such reference data, in order to secure that both the consistency and control of these information are handled in a transparent, legislative-complied and accountable way by an organization⁴¹.

According to Aaron Zornes, Founder and Chief Research officer of the MDM Institute: “Across both private and public sectors, many organizations of all sizes continue to struggle to provide a single view of the truth - either for “party” (customer, citizen,supplier,etc.) or “thing”(product, location, measurements, etc.) across the enterprise. Data Governance is critical when it comes to achieving sustainable and effective MDM. Failure to execute Data Governance concurrently with an MDM program, greatly decreases the probability of success and economic sustainability of the MDM programs”⁴².

DG and MDM are not the same thing. Good governance of data provides a transparent and clear environment for MDM programs. This happens because MDM programs embrace DG initiatives offering trust between users of data, who cannot count on their master data, becauseof the way itis collected, processed and generally used by an institution, a corporate organization or a governmental agency.

1.6. b. DATA MANAGEMENT

Among various definitions of DG, there is one that defines DG as “....a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions, with what information, and when, under what circumstances, using what methods”⁴³. In the definition mentioned above, Data Management is described using the phrase “agreed-upon models”. In other words, DM is “the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets”⁴⁴. As concepts of the strategic improvement and growth of a private organization or a public agency, they interlink and complement one another. A solid DM initiative needs a well-planned DG sector which will plan, monitor and control how data will be collected, stored and processed and a DG initiative also needs a solid DM sector which will provide the processes,

https://en.wikipedia.org/wiki/Enterprise_resource_planning
https://en.wikipedia.org/wiki/Supply-chain_management

⁴⁰ Health Catalyst, Executive Report: Demystifying Healthcare Data Governance by Dale Sanders, senior vice president, strategy, health catalyst, 2016, p 20.

⁴¹Study on Standard-Based Archival Data Management, Exchange and Publication, Final Report, ISA² Action 2017.01, p 20.

⁴²<http://tdan.com/master-data-mgmt-data-governance/16845>

⁴³<http://www.datagovernance.com/defining-data-governance/>

⁴⁴https://dama.org/files/public%20DI_DAMA_DMBOK_Guide_Presentation_2007.pdf

tools and methods that are necessary for a high level planning, monitoring and control over data.

According to Wende, DG complements DM, but does not replace it⁴⁵. Mahanti stated that DG contains data management⁴⁶. Dahlberg and Nokkala figured that DG is closely related to daily DM functions⁴⁷. According to others, DG is considered as a central data management function whose influence is felt through all of IT and DM disciplines⁴⁸.

All statements mentioned above, show that DM and DG are highly related and their interlink within an organization can affect the entire structure, strategy and effectiveness of the organization. They point out the fact that a solid DM policy is always better using a transparent, accountable and well-established DG plan or the other way around.

1.6.c. DATA WAREHOUSES

William H. (Bill) Inmon, who is a computer scientist, is recognized as the father of data warehouses⁴⁹. He characterized data warehouses as a collection of subject-oriented, integrated, nonvolatile and time-varying data to support management decisions⁵⁰. Data Warehouses, came into force as a consequence of the high demands of organizations for well-performed data analysis to support their system of decision-making processes⁵¹.

Back in the 1990's, operational or transactional databases, which were used for data analysis from the 1970's, didn't satisfy the needs for data analysis mainly because they were designed to support the day to day business operations. Also, they did not include historical data and their performance around complex requests or large volumes of data was poor⁵². Moreover, organizational behavior must be analyzed as a whole, with data from different operational systems that should be integrated⁵³.

⁴⁵Wende, K. A Model for Data Governance-Organizing Accountabilities for Data Quality Management. In Proceedings of the 18th Australasian Conference on Information Systems; University of Southern Queensland: Toowoomba, 2007; pp.417-425.

⁴⁶Mahanti, R. (2014) Critical success factors for implementing data profiling: The first steps towards data quality. *Software Quality Professional*, 16(2), 13-26.

⁴⁷Dahlberg, T., Nokkala, T. (2015). A framework for the corporate governance of data: Theoretical background and empirical evidence. *Business, Management and education* 13(1):25-45.

⁴⁸Thompson, N., Ravindran, R., Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government Information Quarterly*, 32(3), 316-322.

⁴⁹Jill Dyche (2000). *e-Data: turning data into information with data warehousing*. Addison-Wesley. p 323.

⁵⁰Alejandro Vaisman, Esteban Zimanyi, *Data Warehouses Systems: Design and Implementation* (2014), p 5.

⁵¹Alejandro Vaisman, Esteban Zimanyi, *Data Warehouses Systems: Design and Implementation* (2014), p 5.

⁵²Alejandro Vaisman, Esteban Zimanyi, *Data Warehouses Systems: Design and Implementation* (2014), p 5.

⁵³Alejandro Vaisman, Esteban Zimanyi, *Data Warehouses Systems: Design and Implementation* (2014), p 5.

All these reasons led organizations to the establishment of data warehouse systems as a tool of business intelligence and a decision-support system that provides more sophisticated data analysis and therefore better management and decision-making policies and strategies.

1.6.d. DATA LAKES

The term of “Data Lake” is credited to the Pentaho Chief Technology officer, James Dixon. He contrasted the term with data mart, which is a subset of a data warehouse, arguing that data marts have enough problems, such as information siloing. According to him: “if you think of a data mart as a store of bottled water, cleansed and packaged and structured for easy consumption, the data lake is a large body of water in a more natural state. The contents of the data lake stream in from a source to fill the lake and the various users of the lake can come to examine, dive in, or take samples”⁵⁴.

Data Lakes are repositories which retain all data. In contrast with data warehouses, data lakes support a variety of all data types including non-traditional data sources such as social network activities, text, images, web server logs and sensor data. All data are stored regardless of source and structure and all users have equal access to data. Because of the raw form of data which are stored in “the lake”, adaptability in changes is easier than in data warehouses because, in the second case, the complexity of data processing and analysis is far more time and resource consuming. Finally, because of the above mentioned, data lakes offer faster knowledge of data to their users⁵⁵.

Data Lakes emerged through the explosion of Big Data Initiatives and are highly equivalent to technologies such as Apache Hadoop. They are considered to be a tool for better Big Data Governance and Management but their future lays upon their ability to strengthen governance and address security issues⁵⁶.

1.6.e. INFORMATION & IT GOVERNANCE IN RELATION TO DG

IT has been characterized as the core and absolutely important department for every business⁵⁷. It is defined as “procedures and policies established in order to assure that the IT system of an organization sustain its goals and strategies”⁵⁸. As for the relation between IT Governance and DG, Microsoft Corporation gives an excellent example of it. It characterizes IT as a form of governance which focuses on

⁵⁴ <https://jamesdixon.wordpress.com/2010/10/14/pentaho-hadoop-and-data-lakes/>

⁵⁵ <https://www.blue-granite.com/blog/bid/402596/top-five-differences-between-data-lakes-and-data-warehouses>

⁵⁶ <http://www.dataversity.net/data-lakes-complicating-big-data-governance/>

⁵⁷ Preittigun, A.; Chantatub, W.A. Comparison between IT Governance Research and Concepts in Cobit5. *Int. J. Res. Manag. Techno.* 2012, 2, p 581-590.

⁵⁸ Herbst, N. R; Kounev, S.; Reussner, R. Elasticity in Cloud Computing: What It is and What It is not. In *Proceedings of the 10th International Conference on Autonomic Computing*, San Jose, CA, USA, 26-28 June 2013; pp 23-27.

the “pipelines” or the organization’s IT infrastructure. In contrast, DG is characterized as a form of governance whose main focus is on the “water” or the flows of data through these pipelines⁵⁹.

Concerning Information governance, it was introduced by Donaldson and Walker in 2004, and established as a framework of support to the work of the National Health Society in the USA⁶⁰. It is defined as “the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, usage, archiving and deletion of information”⁶¹. According to the DG Institute, data and information governance are so closely related that the two terms mean the same thing⁶². This view is supported by a paper published in 2016. This paper enhanced the argument that DG should become an inherent part of Information and IT governance, based on a systematic analysis whose main task is to prove that DG is necessary for information governance⁶³.

2. DEVELOPMENTS OF DG POLICIES IN EU

2.1. DA & DSMS

On March 3, 2010 EC proposed a 10-year strategy -Europe 2020- in order to face the financial crisis of 2008 which caused severe damage to the economic and social structure of many member states (Greece, Italy, Spain, Portugal, etc.)⁶⁴. The main goal of Europe 2020 was to offer “a smart, sustainable and inclusive growth” across EU. It was consisted of seven initiative pillars, one of which is the Digital Agenda for Europe. It was launched in May 2010 with the goal to generate economic and social growth in EU⁶⁵.

Moreover, DSMS was created as an overall result of the Europe 2020 strategy and DA. It was adopted by the EC in May 2015 and its main objective was to maximize the potential growth of digital economy⁶⁶. It is a market where goods, services, capital and people can move in a free and ensured way and at the same time,

⁵⁹Microsoft Corp. A Guide to Data Governance for Privacy, Confidentiality and Compliance, Part 1: The case for Data Governance, January, 2010, p 10.

⁶⁰Majid Al-Ruithe, ElhadjBenkhelifa, Khawar Hameed. Data Governance Taxonomy: Cloud versus Non Cloud, p 7.

⁶¹Gartner, Information Governance: a model for security in medical practice. J. Digit. Forensics. Secur. Law. 2007, 2, p 57-74.

⁶²Majid Al-Ruithe, ElhadjBenkhelifa, Khawar Hameed. Data Governance Taxonomy: Cloud versus Non Cloud, p 7.

⁶³Olaitan, O.; Herselman, M; Wayi, N .Taxonomy of literature to justify data governance as a prerequisite for information governance. In Proceedings of the 28th Annual Conference of the Southern African Institute of Management Scientists(SAIMS), Pretoria, South Africa, 4-7 September 2016.

⁶⁴European Commission, Communication from the Commission, Europe 2020: A strategy for smart, sustainable and inclusive growth.

⁶⁵https://eige.europa.eu/resources/digital_agenda_en.pdf

⁶⁶Urban Agenda for the EU. Partnership for Digital Transition Orientation Paper, 27-02-2017.

people and businesses can exercise their online activities with protection towards consumers and personal data⁶⁷. It is built upon the pillars of⁶⁸:

- 1) Better access for consumers and businesses to online goods and services across Europe.
- 2) Creating the right conditions for digital networks and services to flourish.
- 3) Maximizing the growth potential for European digital economy.

The main objectives of DSMS in Europe are⁶⁹:

- 1) Enhancing of e-commerce in the EU⁷⁰ (Regulation (EU) 2018/302, provisional agreement of the co-legislators, on December 14, 2017, to the prices for cross-border parcel delivery services and revised Consumer Protection Cooperation Regulation).
- 2) Innovation and modernization of the EU copyright rules^{(71) (72) (73) (74)} {COM (2016)594, COM (2016)593, implementation of the Marrakesh Treaty in the EU law with the Regulation (EU) 2017/1563 and Directive (EU) 2017/1564}.
- 3) Update of the EU audiovisual rules and cooperation with platforms to build an environment of promoting European films, protecting children and tackling hate policies and talks⁷⁵ (revision of the Directive on Audiovisual Media Services).
- 4) Strengthening of the EU cyber security agency, ENISA, for better reply to cyber-attacks and establishing an efficient EU cyber dissuasion and criminal law response for more solid protection of EU's citizens, businesses and institutions⁷⁶ (EC's cyber security package on September 13, 2017⁷⁷, the implementation of the Directive on the

⁶⁷European Commission: Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions, A Digital Single Market Strategy for Europe, 6-5-2015.

⁶⁸European Commission: Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions, A Digital Single Market Strategy for Europe, 6-5-2015, p 7.

⁶⁹https://ec.europa.eu/commission/priorities/digital-single-market_en

⁷⁰<https://ec.europa.eu/digital-single-market/en/boosting-e-commerce-eu>

⁷¹<https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-laying-down-rules-exercise-copyright-and-related-rights-applicable-certain>

⁷²<https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and%20-council-copyright-digital-single-market>

⁷³<https://ec.europa.eu/digital-single-market/en/news/implementation-marakesh-treaty-eu-law>

⁷⁴<https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules>

⁷⁵<https://ec.europa.eu/digital-single-market/en/news/european-parliament-approves-revised-rules-audiovisual-media-across-europe>

⁷⁶<https://ec.europa.eu/digital-single-market/en/cyber-security>

⁷⁷<https://ec.europa.eu/digital-single-market/en/cyber-security>

security of network and information systems, NIS, and the EU promotion of the application of International law in cyberspace, the adopted framework for shared EU diplomatic act to cyber threats and attacks, the so called “cyber diplomacy toolbox” and the expected, in 2018, proposals of the Commission on cybercrime will establish a solid fortress for EU’s cyberspace⁷⁸).

5) Construction of a European data economy⁷⁹. It is estimated that the value of the European data economy will reach EUR 739 billion by 2020, representing 4% of the overall EU GDP⁸⁰. The EC promotes the creation of a common European data space with legislative proposals such as the proposal for a review of the Directive on the re-use of public sector’s information (PSI Directive), the refresh of the 2012 Recommendation on access and preservation of scientific information and the policy of guidance on private sector’s data sharing, between private companies and public agencies for public interests⁸¹. These initiatives are related to the proposal of the Commission for a regulation on the free flow of non-personal data⁽⁸²⁾⁽⁸³⁾. This regulation will provide a sustainable ecosystem for data economy growth by providing a secure environment of free flow of data and by giving the opportunity to private and public sector to store and process non-personal data anywhere they prefer in the EU⁸⁴.

6) Engaging with the digital economy by providing high-speed internet connection (the so-called “connectivity for a European gigabit society”, which includes the European Electronic Communications Code. This is a set of general rules and objectives for the existing and upcoming regulations of the telecom industry, the common EU broadband targets for 2025, the 5G Action Plan and the WiFi4EU initiative⁸⁵).

7) Adaptation of e-privacy rules to the new era of digital transition. The EC, taking into consideration the enhancing DSMS, proposed a regulation on privacy and electronic communications⁸⁶. The new regulation will safeguard that new electronic

⁷⁸ <https://ec.europa.eu/digital-single-market/en/cyber-security>

⁷⁹ <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>

⁸⁰ <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>

⁸¹ <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>

⁸² <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>

⁸³ <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>

⁸⁴ <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>

⁸⁵ <https://ec.europa.eu/digital-single-market/en/policies/improving-connectivity-and-access>

⁸⁶ <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>

communication services (Facebook Messenger, Viber, Skype, etc.) will guarantee the level of confidentiality of communications just as major telecom operators do. Metadata, a crucial component of privacy, will be anonymized or deleted if there is no user-consent, unless “the data is needed for billing”⁸⁷. Also, the cookie provision will be “streamlined” providing a friendly environment for the users in order to accept or deny tracking cookies. Furthermore, ban upon not requested electronic communications, through emails, SMS, and automated calling machines, will be enforced through the new Regulation⁸⁸.

8) Promotion of digital skills across Europe. The emergence of new technologies changed the necessary skills needed for businesses, research and public administration. This is why the EC promotes various initiatives such as the Skills Agenda for Europe⁸⁹ and Digital Skills and Jobs Coalition⁹⁰, in order to build a strong environment for consumers and employees⁹¹. In that direction, the EC published on April 18, 2016 the Communication on Digitizing European Industry, which is a set of measures mainly focused on digital skills⁹².

2.2. EUROPEAN AGENDA FOR COLLABORATIVE ECONOMY

Another project of the EC around the economic growth of the EU, is the so-called “collaborative economy”. Basically, it is a supplementary project of the DSMS plan. It was adopted by the EC in June 2016 with the goal to promote the establishment and development of innovative services around economy and to guarantee consumers’ and social protection⁽⁹³⁾⁽⁹⁴⁾.

It can be characterized as an environment where providers of goods and services can trade online with individuals. It is also an environment where individuals, but also small and medium businesses, can trade their assets with others

⁸⁷ <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>

⁸⁸ <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>

⁸⁹ <http://ec.europa.eu/social/home.jsp?langId=en>

⁹⁰ <https://ec.europa.eu/digital-single-market/digital-skills-jobs-coalition>

⁹¹ <https://ec.europa.eu/digital-single-market/digital-skills-jobs-coalition>

⁹² <https://ec.europa.eu/digital-single-market/digital-skills-jobs-coalition>

⁹³ Urban Agenda for the EU, Partnership for Digital Transition, Orientation Paper, 27/02/2017, p 4.

⁹⁴ https://ec.europa.eu/growth/single-market/services/collaborative-economy_en

through intermediaries, which connect providers with consumers through collaborative platforms. The latter connect and relate supply and demand in a trusted way, using information technologies as a tool⁹⁵.

2.3. eIDAs REGULATION

The most valuable regulation around EU's DSMS is the electronic Identification Authentication and trust services (eIDAs) Regulation⁹⁶. Regulation (EU) 910/2014 replaces the Directive 1999/93/EC. It was applied from July 1, 2016 and its main objective is to create a solid regulatory environment across EU, which will secure electronic interactions between the public sector, private companies and citizens⁹⁷. Furthermore, all organizations which deliver public digital services in an EU member state have to approve electronic identification for all member states from September 29, 2018⁹⁸.

The regulation controls and inspects electronic identification and trust services for electronic transactions across EU's market providing the "one click" initiative as a new-entered method for across-borders transactions⁹⁹. Through the eIDAs Regulation, the principles of interoperability and transparency are performed, as it establishes a common framework for eIDs and also creates a catalogue of trusted services which can be used around the common framework of signing⁽¹⁰⁰⁾⁽¹⁰¹⁾.

2.4. e-GOVERNMENT ACTION PLAN 2016-2020

Following the positive effect of the previous eGovernment Action Plan 2011-2015, the EU launched a new one under the umbrella of the overall strategy of DSMS, in 2016¹⁰². Its main goal is to offer "open, efficient and inclusive, providing borderless, personalized, user-friendly, end-to-end digital public services to all citizens and businesses in the EU"¹⁰³. In addition, it is supported by a set of initiatives

⁹⁵ <http://bruegel.org/2018/04/collaborative-economy-market-design-and-basic-regulatory-principles/>

⁹⁶ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

⁹⁷ <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>

⁹⁸ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

⁹⁹ <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>

¹⁰⁰ <https://www.cryptomathic.com/news-events/blog/the-eidas-agenda-innovation-interoperability-and-transparency>

¹⁰¹ https://en.wikipedia.org/wiki/EIDAS#cite_note-SecureIdentity%20Alliance-6

¹⁰² <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN>

¹⁰³ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN>

and principles, such as openness and transparency, cross-border by default, interoperability by default, etc.¹⁰⁴.

Additionally, it introduced the “once-only” principle, which means that public authorities have to safeguard and secure that citizens and companies will supply the same information to a public authority only once¹⁰⁵. As a result of the “once-only” principle, the TOOP initiative was launched in January 2017¹⁰⁶. The eGovernment Action Plan 2016-2020 also focuses on minimizing expenditure and bureaucratic waste of public services, using e-services and e-solutions to do so and that is a potential factor of debilitation of barriers between officials and citizens¹⁰⁷.

2.5. HORIZON 2020

It is the most funded EU’s research and innovation program with nearly EUR 80 billion of funding¹⁰⁸. It is a Europe 2020 flagship initiative with a main objective to boost European’s economy and to create jobs¹⁰⁹. Horizon 2020, is stretched around every sector that could offer solutions, through new technologies, to the problems (economic, social, science, health, job vacancies, etc.) of the European citizens.

It is used as a tool which will integrate e-infrastructures, will unite current research programs and scientific clouds and will help to the establishment of cloud-based services for Open Science giving the opportunity for easier, affordable and efficient scientific data¹¹⁰. In addition, it will make new market opportunities and answers to problems in sectors such as health, environment and transport¹¹¹.

2.6. OPEN SCIENCE CLOUD

Open Science Cloud initiative is a vision of the EC to create and support open science and open innovation not only for Europe but also for the globe¹¹². This

¹⁰⁴ <https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2016-2020>

¹⁰⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN>

¹⁰⁶ <https://ec.europa.eu/digital-single-market/en/news/once-only-principle-toop-project-launched-january-2017>

¹⁰⁷ Urban Agenda for the EU, Partnership for Digital Transition, Orientation Paper, 27/02/2017, p 10.

¹⁰⁸ <https://ec.europa.eu/programmes/horizon2020/what-horizon-2020>

¹⁰⁹ <https://ec.europa.eu/programmes/horizon2020/what-horizon-2020>

¹¹⁰ Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 28.

¹¹¹ Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 27-28.

¹¹² <https://www.egi.eu/about/newsletters/what-is-the-european-open-science-cloud/>

initiative is part of the European Cloud Initiative, which builds upon the DSMS and the accomplishments of the European Cloud Strategy¹¹³.

Its main goal is to take EU to the top of scientific data infrastructures technologies and data-driven science¹¹⁴. Moreover, the creation of a trusted and open environment for science not only will benefit the economy and science sector but it will also enhance the position and structure of EU governance through digitalization. In addition, it will create an environment where privacy and data protection are certified by design, based on admitted standards and a standard where users' data are secured without responsibility risks¹¹⁵.

2.7. URBAN AGENDA & EUROPEAN SMART CITIES' INITIATIVE (INITIATIVES RELATED TO DIGITAL SOCIETY)

It was adopted by the pact of Amsterdam in May 2016, setting priorities around many sectors such as climate adaptation, inclusion of migrants and refugees, housing, urban poverty, etc.¹¹⁶. On the top of its priorities also lays the digital transition of EU urban authorities¹¹⁷. This initiative needs more integrated action and cooperation between the Commission, EU organizations, national governments, local authorities and stakeholders¹¹⁸. With this agenda, urban-policy knowledge and exchange of good practices, studies and data will be enhanced, contributing to an environment of better funding and laws¹¹⁹.

As for the European Smart Cities Initiative, the EC website defines a smart city as “a place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and business. A smart city goes beyond the use of information and communication technologies (ICT) for better resource use and less emissions. It means smarter urban transport networks, upgraded water supply and waste disposal facilities, and more efficient ways to light and heat buildings. It also means a more interactive and responsive city administration, safer public spaces, meeting the needs of an ageing

¹¹³European Cloud Initiative-Building a competitive data and knowledge economy in Europe, COM (2016), p 3.

¹¹⁴Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 28.

¹¹⁵Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 28.

¹¹⁶<https://ec.europa.eu/futurium/en/urban-agenda>

¹¹⁷Urban Agenda for the EU, Partnership for Digital Transition, Orientation Paper, 27/02/2017, p 4.

¹¹⁸https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/urban-agenda-eu_en

¹¹⁹https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/urban-agenda-eu_en

population”¹²⁰. It creates an ecosystem of connecting and exchanging information, with practices and utilities between public authorities, industry, banks, small business(SMEs) and others, while taking advantage of the digital transition that EU society enters¹²¹.

2.8 HEALTH DATA POLICIES IN EU

Another area of high demanding policies and strategies across EU is the sector of health. The European Group on Ethics in Science and New Technologies (EGE) defined health data as “a wide range of information about an individual, which all touch upon an individual’s private life”¹²². This means that health data are not only medical data. They include a biography of all medical diseases, interventions, diagnoses, test results, medications prescriptions etc.¹²³. Furthermore, this health history of a person includes more sensitive data such as data relevant to family history, sexual life, mental health, social and economic factors¹²⁴. In addition, health care administrative data (admissions, data routine, operational data, insurance and financial transactional data, etc.) are included in the category of sensitive health data¹²⁵.

2.8.a DIGITAL HEALTH POLICIES IN EU

The first action plan for e-health in EU was adopted by the EC in 2004¹²⁶. This action helped to create many initiatives to boost the implementation of e-health solutions over EU member states. Such an initiative was the epSOS pilot project, which was introduced in 2008 with the goal to provide smart cross-border health services. It ended in June 2014¹²⁷.

The second big strategy around health was launched in 2011 with the Cross-Border Healthcare Directive (2011/24/EU). It established the eHealth Network, which

¹²⁰<https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities>

¹²¹<https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities>

¹²²Opinion No13 Ethical Issues of Health Care in Information Society.

¹²³OECD Health Policy Studies, Health Data Governance: Privacy, Monitoring and Research, 2015, p 15.

¹²⁴OECD Health Policy Studies, Health Data Governance: Privacy, Monitoring and Research, 2015, p 15.

¹²⁵OECD Health Policy Studies, Health Data Governance: Privacy, Monitoring and Research, 2015, p 15.

¹²⁶Simona Guagliardo, European Policy Centre, Policy Brief, Digital Health: How can the EU help make the most out of it?, 25 January 2018.

¹²⁷<https://ec.europa.eu/digital-single-market/en/news/cross-border-health-project-epsos-what-has-it-achieved>

supports formal cooperation between national authorities of the member states and helps the development of common measures to support the cross-border exchange of health care data¹²⁸. In 2014, the second e-Health Action Plan (2012-2020) was initiated with the goal to handle and minimize the barriers of health between member states and also to clarify the policies and the vision of e-health in EU, in relation with the overall strategy of Europe 2020¹²⁹. Since 2015 it has been constituting an integral part of the DSMS.

Furthermore, the EC designates and promotes innovation in health sector through programs such as the Horizon 2020 Work Program 2018-2020, the European Open Science Cloud and the European Cloud Initiative¹³⁰. Also, promotion and empowerment of digital literacy and digital solutions in health are included in the EU cohesion policy for the period 2014-2020¹³¹.

2.8.b. LEGISLATION AROUND HEALTH DATA

The first major legislation around e-health in EU was the Directive 2011/24/EU on the application of patients' rights in cross border healthcare¹³². It was the first attempt of creating a cross border, solid and secure system in the field of healthcare. It includes not only the provision of healthcare but also the concept of prescription, healthcare costs, delivery of medications and medical devices¹³³. The Directive created a network of national contact points for cross border healthcare, a set of measures on a list of elements to be included in cross border prescription and the development of European Reference Networks of medical expertise for cooperation between EU countries¹³⁴.

The second legislation related to health data is the GDPR. It is directly related to the digitalization of health with Article 9, which refers to the process of special categories of personal data and defines provisions that are applicable to health data⁽¹³⁵⁾⁽¹³⁶⁾. The GDPR extends the scope of accessing rights for patients¹³⁷ and

¹²⁸Simona Guagliardo, European Policy Centre, Policy Brief, Digital Health: How can the EU help make the most out of it? , p 3, 25 January 2018.

¹²⁹Simona Guagliardo, European Policy Centre, Policy Brief, Digital Health: How can the EU help make the most out of it? , p 3, 25 January 2018.

¹³⁰Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 27-28.

¹³¹Simona Guagliardo, European Policy Centre, Policy Brief, Digital Health: How can the EU help make the most out of it?, 25 January 2018.

¹³²<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024>

¹³³<https://ec.europa.eu/digital-single-market/en/news/cross-border-digital-prescription-and-patient-data-exchange-are-taking>

¹³⁴<https://ec.europa.eu/digital-single-market/en/news/cross-border-digital-prescription-and-patient-data-exchange-are-taking>

¹³⁵Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 5.

permits re-use of personal data, including health data, for scientific purposes¹³⁸. According to Article 9 of the GDPR, processing of special categories of data, such as health data, is prohibited without consent given by the data subject unless second paragraph of Article 9 is applied¹³⁹ or there is an authorized permission for secondary use¹⁴⁰. The GDPR offers European citizens the right to access and share their data¹⁴¹. A recent study showed that 52% of respondents wish to have online access to their health data, including prescriptions and medical records¹⁴². This right is for the time being limited, and only 9% of hospitals in EU allow their citizens to access or partial access their medical records¹⁴³.

2.8. c. CROSS BORDER INTEROPERABILITY FOR THE EXCHANGE OF HEALTH DATA

A crucial section on the digital innovation of health in EU, is the ability of member states to establish a coherent and solid network for cross border interoperability to exchange data around health.

The first eHealth Action Plan prioritized interoperability of electronic health records among member states¹⁴⁴. Later, the 2008 Communication Recommendation on cross-border interoperability of electronic health record systems developed the first European Interoperability Framework for eHealth(ReEIF), which proved to be inadequate when it came to providing cross border access to electronic health records by healthcare professionals and securing the technological means for citizens to access and operate their health data¹⁴⁵. This is why, a new European Interoperability Framework (EIF) was adopted on March 13, 2017 as a part of the Interoperability Solutions for European Public Administrations (ISA) program (2016-2020)¹⁴⁶. Interoperability frameworks in EU health are enhanced through HORIZON 2020, the

¹³⁶ Article 9, Regulation (EU) 2016/679

¹³⁷ Recital 63, Regulation (EU) 2016/679.

¹³⁸ Towards a European Ecosystem for Healthcare Data, Workshop Report, Brussels, BE, 25 October 2017, p 6.

¹³⁹ Article 9, Regulation (EU) 2016/679

¹⁴⁰ Towards a European Ecosystem for Healthcare Data, Workshop Report, Brussels, BE, 25 October 2017, p 6.

¹⁴¹ Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 27-28.

¹⁴² Special Eurobarometer 460 (results from March 2017) Attitudes towards the impact of digitization and automation on daily life.

¹⁴³ <https://ec.europa.eu/digital-single-market/en/news/european-hospital-survey-benchmarking-deployment-ehealth-services-2012-2013>

¹⁴⁴ Commission Communication on “eHealth – making healthcare better for European citizens: An action plan for a European eHealth Area”, COM (2004), 356 final.

¹⁴⁵ Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 6.

¹⁴⁶ Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 5.

Directive 2011/24/EU, DSMS, eHealth Network, the European Innovation Partnership on Active and Healthy Ageing (EIP on AHA), Open Science Cloud and e-Government Action Plan (2016-2020)¹⁴⁷.

Currently, there is a lack of electronic health records' interoperability in EU. The absence of a unified framework to support interoperability of electronic health record systems creates obstacles to the innovation of health, affects the development of opportunities for SMEs and impacts negatively to the process and expenditure of digitizing health data and information¹⁴⁸.

Cross-border interoperability of electronic health record systems will affect positively not only the European citizens but also the development and growth of the European Market. A market analysis of the European electronic health record systems initiated by Frost & Sullivan came to the conclusion that "the absence of a pan-European electronic health records' strategy has worsened market fragmentation and continues to act as a barrier to electronic health adoption"¹⁴⁹. Cross border interoperability will affect positively citizens who live or travel abroad of their EU member state, SMEs and companies with innovative policies around health market and it will provide better opportunities for EU research health community¹⁵⁰.

2.8.d. CROSS BORDER EXCHANGE OF DATA

Currently, the same situation which exists in cross border interoperability of electronic health records, also applies to cross border exchange of health data. Hospitals' percentage on the electronically exchanging clinical care information about patients with other healthcare providers, in the same country, is up to 39%, whereas 4% exists on the exchanging between hospitals and other health providers in other EU countries¹⁵¹. As for the percentage of exchanging medical patient data between general practitioners and other healthcare providers and professionals, this varies between EU member states¹⁵².

Voluntary coordination and cooperation between member states, eHealth Digital Service Infrastructure and ePrescriptions services are initiatives that enable better and more valued cross border exchange of health data while in 2018, member

¹⁴⁷Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 6, 10, 18

¹⁴⁸Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 13.

¹⁴⁹Frost & Sullivan Market Analysis "European Electronic Health Records Market", 2015 <https://ww2.frost.com/news/press-releases/interoperable-electronic-health-records-can-revolutionize-healthcare-delivery-europe/>

¹⁵⁰Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 22-23.

¹⁵¹Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 18.

¹⁵²Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 19.

states have the opportunity to exchange Patient Summaries and ePrescriptions across borders for first time in EU history¹⁵³.

2.8.e.BIGDATA-REALWORLD DATA AND CLOUD COMPUTING

Big Data policies around health include high-volume and diversity clinical, biological, environmental and lifestyle information and data, which is collected from individuals to big groups and is related to their health and well-being status, at one or more times. Data generation occurring every year is estimated to a 4300% annual growth between 2012-2020¹⁵⁴. The sources of big data could include social media, physical activity trackers, electronic health records, insurance claim databases, health surveys, patient registries and observational studies¹⁵⁵.

On the other hand, real world data is substantial but it refers to “any type of data not collected in a randomized clinical trial. This data can complement randomized clinical trial data to fill the knowledge gap between clinical trials and clinical practice, can provide new insights into disease patterns and can help improve the safety and effectiveness of health interventions”¹⁵⁶.

It is employed for regulatory reasons and health technology evaluations. It can provide faster access to novel health interventions with safety and effectiveness and it can give better solutions for new treatments and payment models¹⁵⁷. Major initiatives around Real World Data include the European Medical Information Framework project¹⁵⁸, the Electronic Health Record for Clinical Research¹⁵⁹, the GET REAL project¹⁶⁰ and the GAPP Joint Action¹⁶¹. Furthermore, there are several EU big data

¹⁵³Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 21, 25.

¹⁵⁴<https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX%3A52018SC0126>

¹⁵⁵Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 36.

¹⁵⁶Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 36.

¹⁵⁷Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 37.

¹⁵⁸<http://www.emif.eu/>

¹⁵⁹<http://www.ehr4cr.eu/>

¹⁶⁰<http://www.imi-getreal.eu/>

¹⁶¹<https://www.gapp-ja.eu/>

initiatives around health such as: MIDAS¹⁶², BigO¹⁶³, IASIS¹⁶⁴, PULSE¹⁶⁵, CrowdHEALTH¹⁶⁶ and EVOTION¹⁶⁷.

Cloud computing is defined by the National Institute for Standards and Technology (NIST) in USA as “a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”¹⁶⁸.

Cloud technology could be used in the health sector as a tool for connecting mobile devices, storing patient-related data during treatment and using data for public health and clinical research¹⁶⁹. Since 2012, the EC is fully engaged to the establishment of a cloud computing strategy and with the European Cloud Initiative, which was launched in April 2016, and Open Science Cloud, it leads EU to a well-funded and solid environment not only for health data but for any kind of data.¹⁷⁰

3.GDPR

3.1. RELATION BETWEEN CONCEPTS OF PRIVACY & DATA PROTECTION

In order for the value of developing privacy and data protection laws to be understood, the relation between the concepts of privacy and data protection have to be comprehensible. The right to privacy is protected by Article 8 of the European Convention on Human Rights¹⁷¹. In addition to that, the right to privacy is a fundamental right in the Charter of Fundamental Rights of EU and EU is indirectly bound by the ECHR through Article 6 of the Treaty on the Functioning of EU⁽¹⁷²⁾⁽¹⁷³⁾. On the other hand, the right to data protection is also a fundamental right under

¹⁶²<http://www.midasproject.eu/>

¹⁶³<https://bigoprogram.eu/>

¹⁶⁴<http://project-iasis.eu/>

¹⁶⁵<http://www.pulse-fp7.com/>

¹⁶⁶<https://www.crowdhealth.eu/>

¹⁶⁷<http://h2020evotion.eu/>

¹⁶⁸Joint Action to Support the eHealth Network, Report on the use of cloud computing in health, 2015, p 5.

¹⁶⁹Joint Action to Support the eHealth Network, Report on the use of cloud computing in health, 2015, p 4.

¹⁷⁰Commission staff working document, COM (2018) 233, final, on the enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, p 26-28.

¹⁷¹Council of Europe, Article 8, European Convention on Human Rights, 1950.

¹⁷²Beyond Data Protection: Strategic Case Studies and Practical Guidance, Springer, 2013, p 219.

¹⁷³Article 7, The Charter of Fundamental Rights of the EU, 26/10/2012.

the Charter of Fundamental Rights of EU¹⁷⁴. The Charter of Fundamental Rights of EU gave these two separate and independent articles because the rights which are included are not expressing the same concept¹⁷⁵.

The concept of data protection enhances and protects the individuals' (subjects) right to privacy, while the right of privacy can be defined as a wider concept of individuals' protection¹⁷⁶. Furthermore, the concept of data protection in EU is a strategic tool for a well-established and preserved balance between an individual's right in privacy and protection of the right to freedom of expression⁽¹⁷⁷⁾⁽¹⁷⁸⁾. It can be concluded that the concept of privacy contains personal data as a dimension of it, but it is more than this, while the concept of data protection has a privacy depth and it is also a regulator and protector of other fundamental rights as well.

The expansion or limitation of each concept to the other, depends on the legal grounds and the interoperability layers that have to be used in order to enhance and protect the individual's fundamental rights and freedoms.

3.2. BACKGROUND OF DATA PROTECTION IN EU

The first legal document that established the right of individual's privacy was the Universal Declaration of Human Rights in 1948 with Article 12¹⁷⁹. After that, the Guidelines on the Protection of Personal Privacy and Trans-border Flows of Personal Data, in 1980, by the Organization for Economic Cooperation and Development¹⁸⁰ and then the Guidelines for the Regulation of Computerized Personal Data Files, as adopted by the General Assembly resolution 45/95 of December 14, 1990¹⁸¹, helped to the development of EU policies and laws around privacy and personal data as binding or non-binding documents.

In European level, the first legally binding text for the protection of personal data of individuals came in 1981 with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No:108), by the Council of Europe¹⁸². An additional protocol to the Convention 108 was adopted in 2001 and with it were introduced provisions on cross-border personal data flows to and from

¹⁷⁴Article 8, The Charter of Fundamental Rights of the EU, 26/10/2012.

¹⁷⁵Beyond Data Protection: Strategic Case Studies and Practical Guidance, Springer, 2013, p 218.

¹⁷⁶Beyond Data Protection: Strategic Case Studies and Practical Guidance, Springer, 2013, p 218.

¹⁷⁷Data Security Breaches and Privacy in Europe, Rebecca Wong, Springer, 2013.

¹⁷⁸Beyond Data Protection: Strategic Case Studies and Practical Guidance, Springer, 2013, p 218.

¹⁷⁹http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf

¹⁸⁰Chao Li, Student Member, IEEE, BalajiPalanisamy, Member, IEEE, Privacy in Internet of Things: from Principles to Technologies, p 2.

¹⁸¹<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/un-guidelines>

¹⁸²<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>

non-member states, and the adaptation and compliance of laws and regulations around the sectors of personal data protection and trans-border data flows¹⁸³. Moreover, the Schengen Agreement, which was taken in force in 1995, includes articles for the protection of personal data and security of data in the Schengen Information System¹⁸⁴ (Articles 102-118).

The most significant step to the development of modernized, solid and influential policies and laws around data protection and privacy field, was the establishment of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹⁸⁵. The Data Protection Directive (DPD) was adjusted to Greek legislation with the law No.2472/1997¹⁸⁶ and it was the first legal effective international data protection document¹⁸⁷. It created a regulatory framework where protection of individual's privacy and free movement of personal data in the EU were in the same agenda and not confronted with each other¹⁸⁸. The Directive created limits on the collection and use of personal data and made it obligatory for each member state to create an independent national body which would be responsible for the supervision of activities related to the processing of personal data¹⁸⁹. The Directive was imposed to data which were processed by automated means and data included in or planned to be a piece of a non-automated filing system¹⁹⁰. This was the reason that led to the establishment and enforcement of the Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the European Community institutions and bodies and to the free movement of such data¹⁹¹.

The Data Protection Directive came into force in an environment where technological developments, internet and digitization demands were not a top priority for EU. Factors, such as the lack of harmonization of data protection legislation between member states, demands for integration and cooperation between member states for economic growth and the development of digital industry in almost every strategic sector of human evolution, led the EU Commission, back in 2012, to the proposal of the General Data Protection Regulation, which was taken into force on May, 25, 2018 and superseded the Data Protection Directive⁽¹⁹²⁾⁽¹⁹³⁾.

¹⁸³<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181>

¹⁸⁴[https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:42000A0922\(02\)](https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:42000A0922(02))

¹⁸⁵<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5>

¹⁸⁶http://www.nurs.uoa.gr/fileadmin/nurs.uoa.gr/uploads/Nomothesia_Nosilefton/Nomoi/Nomos_2472_FEK_501997.pdf

¹⁸⁷ Lee.A.Bygrave, Data Privacy Law: An International Perspective, Oxford University Press, 2014.

¹⁸⁸ The Royal Society, Data Governance: Landscape Review, June 2017, p 4.

¹⁸⁹ The Royal Society, Data Governance: Landscape Review, June 2017, p 4.

¹⁹⁰ The Royal Society, Data Governance: Landscape Review, June 2017, p 4.

¹⁹¹<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:EN:PDF>

¹⁹² The Royal Society, Data Governance: Landscape Review, June 2017, p 6.

¹⁹³ Amanda Cole, Louis Garrison, Jorge Mestre-Ferrandiz, Adrian Towse, Data Governance Arrangements for Real-World Evidence, Consulting Report, 2015, p 5.

3.3. GDPR CONCEPT

The GDPR repeals the former legislation on data protection in EU, the Directive 95/46/EC. In contrast to the Directive, it is a binding legal document for all member states. The unification of data protection law across EU started back on January 25, 2012, when the EC proposed the establishment of the GDPR (Regulation 2016/679). The GDPR is applicable in all member states from May 25, 2018 and its main objective is not only to enhance and safeguard the rights that individuals have over their data but moreover to create a simple and efficient regulatory environment, where compliance with the regulation, is a key element not only for public sector but also for private businesses¹⁹⁴. In addition to these, the GDPR provides the requirements under which exporting of personal data, outside the EU, takes place¹⁹⁵.

3.4. RELATION TO THE CONCEPT OF DG

The GDPR text does not include a single reference to the term of “Data Governance”¹⁹⁶. However, DG is implied through the text of GDPR, as well-established procedures, policies and processes are needed for the implementation of the regulation by organizations and DG best practices offer and protect the development of policies, procedures and processes for the protection of the privacy of personal data¹⁹⁷. Furthermore, the close relation between the GDPR and DG can be enhanced through the relation between the guiding principles of data protection as they are addressed under the GDPR and the principles of DG¹⁹⁸.

Article 5 of the Regulation (EU) 2016/679 includes the principles of processing personal data. Lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and the new entrance of accountability principle of controllers, compose the founding principles of data protection¹⁹⁹. On the other hand, integrity, transparency, stewardship, auditability, accountability, change management and standardization, constitute the guiding principles of DG²⁰⁰. These principles are far more general than the principles of data protection as addressed in Article 5 of the GDPR but they are

¹⁹⁴The Royal Society, Data Governance: Landscape Review, June 2017, p 9.

¹⁹⁵ISA² Action 2017.01, Standard-Based Archival Data Management, Exchange and Publication Study, Final Report, p 20.

¹⁹⁶Microsoft, Data Governance for GDPR Compliance: Principles, Processes and Practices, November 2017, p 17.

¹⁹⁷Microsoft, Data Governance for GDPR Compliance: Principles, Processes and Practices, November 2017, p 17.

¹⁹⁸Microsoft, Data Governance for GDPR Compliance: Principles, Processes and Practices, November 2017, p 20.

¹⁹⁹European Data Protection Supervisor, Guidelines on the protection of personal data in IT governance and IT management of EU institutions, 23 March, p 13-15.

²⁰⁰Microsoft, Data Governance for GDPR Compliance: Principles, Processes and Practices, November 2017, p 15.

closely aligned²⁰¹. Furthermore, the GDPR requirements for collection, processing, usage and storage of data are also aligned with the structure of a well-established data governance plan²⁰². The requirements of data discovery (identification and classification of personal data) and data management (covering response to the requests of data subjects) are addressed under Chapter 3 (Articles 12-23) of the GDPR²⁰³. Also, the requirement of data protection is described in Article 32 of the GDPR, which addresses the security of processing personal data²⁰⁴.

Last but not least, the requirement of report and documentation is addressed through the GDPR in various ways (lawful collection of data, freely given consent, management of data subject's rights requests, security measures for the protection of data, notifications, etc.)²⁰⁵. These requirements are the basic tools for a good DG plan and they are also described and used for the implementation of the GDPR.

3.5. KEY CHANGES ON THE GDPR

3.5. a. GENERAL PROVISIONS & PRINCIPLES

In Article 3, an extended territorial scope of the regulation is established²⁰⁶. Consequently, Article 4 includes new definitions of pseudonymisation, genetic data, data concerning health, biometric data, binding corporate rules and personal data breach. Also, the definition of personal data is expanded as it includes any data of a data subject that could be used to directly or indirectly identify a person²⁰⁷.

Under Chapter 1 and 2, the GDPR introduces new provisions and principles. Data processing has to happen with a transparent manner in relation to the data subject²⁰⁸. In Article 5(2), the principle of accountability is introduced, referring to the controller's responsibility to demonstrate compliance with the provisions of Article 5(1)²⁰⁹. In comparison with the Directive 95/46/EC, where unambiguous consent of the data subject was needed, the GDPR requires a freely given consent with a

²⁰¹Microsoft, Data Governance for GDPR Compliance: Principles, Processes and Practices, November 2017, p 20.

²⁰²Microsoft, Data Governance for GDPR Compliance: Principles, Processes and Practices, November 2017, p 21.

²⁰³Microsoft, Data Governance for GDPR Compliance: Principles, Processes and Practices, November 2017, p 21-22.

²⁰⁴Microsoft, Data Governance for GDPR Compliance: Principles, Processes and Practices, November 2017, p 23.

²⁰⁵Microsoft, Data Governance for GDPR Compliance: Principles, Processes and Practices, November 2017, p 24.

²⁰⁶Christina Tikkinen-Piri, Anna Rohunen, JouniMarkkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, p 5.

²⁰⁷Microsoft, Data Governance for GDPR Compliance: Principles, Processes and Practices, November 2017, p 18-19.

²⁰⁸Article 5(1), Regulation (EU) 2016/679.

²⁰⁹Christina Tikkinen-Piri, Anna Rohunen, JouniMarkkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, p 6.

specific, informed and explicit indication of the data subject's wishes²¹⁰. The controller is responsible to prove the consent of a data subject²¹¹ and the data subject has the right to withdraw his or her consent at any time²¹². But this withdrawal cannot affect the lawfulness of processing based on the consent before its withdrawal²¹³. Furthermore, the regulation enhances and adds the requirements of lawful processing in Article 6 and 9(for special categories of data) and also illuminates further processing of personal data even without consent of the data subject in Article 6(4) and Recital 50²¹⁴. As for the protection of children personal data, the GDPR includes new provisions in Article 8 and 12(1).

3.5. b. TRANSFERS OF PERSONAL DATA

The GDPR ensures the level of data protection within EU. Because of this and in accordance with Article 1(3), transfers of personal data are approved without restrictions or prohibitions within EU. This principle is imposed to transfers from EU member states to the three states²¹⁵ which all together form the European Economic Area(EEA)²¹⁶.

As for transfers outside the EEA, the GDPR describes, in Chapter V, the conditions under which data transfers can be accomplished to the so called "third countries". The regulation presents the conditions that the controller and the processor have to establish on personal data transfers outside the EEA²¹⁷. The conditions for transfers of personal data outside the EEA include transfers on the basis of an adequacy decision²¹⁸, transfers subject to appropriate safeguards²¹⁹ and if needed, the use of derogations from the first two conditions in certain situations²²⁰. The criteria under which the EC ends up to an adequacy decision are described in Article 45(2) and according to Article 45(3) the EC has to evaluate an adequacy decision every four years. The appropriate safeguards are divided in two categories: these that do not require any specific authorization from a supervisory authority and these that require one. The first are described in Article 45(2) and include three new conditions (binding corporate rules²²¹, approved code of conduct²²² and approved certification mechanism²²³). The second ones are described in Article 46(3) of the Regulation.

²¹⁰Christina Tikkinen-Piri, Anna Rohunen, JouniMarkkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, p 6.

²¹¹Article 7(1), Regulation (EU) 2016/679.

²¹²Article 7(3), Regulation (EU) 2016/679.

²¹³Article 7(3), Regulation (EU) 2016/679.

²¹⁴The Royal Society, Data Governance: Landscape Review, June 2017, p 12.

²¹⁵Norway, Liechtenstein, Iceland.

²¹⁶Paul Van den Bulck, Article, Transfers of personal data to third countries, 15 September 2017, p 231.

²¹⁷Christina Tikkinen-Piri, Anna Rohunen, JouniMarkkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, p 12.

²¹⁸Article 45, Regulation (EU) 2016/679.

²¹⁹Article 46, Regulation (EU) 2016/679.

²²⁰Article 49, Regulation (EU) 2016/679.

²²¹Article 47, Regulation (EU) 2016/679.

In absence of an adequacy decision or appropriate safeguards, the GDPR elucidates the derogations of a data transfer outside the EU²²⁴. The approved derogations are enlisted in Article 49(1) of the GDPR, while classifications about these derogations are also provided in paragraphs 2 to 6 of Article 49²²⁵.

3.5.c. SECURITY OF PERSONAL DATA - GENERAL OBLIGATIONS - NATIONAL DEROGATIONS - DPO - SANCTIONS & LIABILITY

Article 32 of the GDPR, extends the obligation of controllers to implement appropriate technical and organizational measures to ensure a level of security. This obligation also covers the processors' aspect from now on. In addition to that, Articles 33-34, introduce the obligation of the controller to notify the supervisory authority within 72 hours after having become aware of a data breach and to notify the data subject in some cases²²⁶. Also Article 33(2), introduces the obligation of the processor to notify the controller for a data breach.

Moreover, Article 25 introduces the principles of data protection by default and by design, while Article 27 introduces the new obligation of the controllers and processors to designate a representative in the EU if they are established in third countries²²⁷. What is more, the new obligation of controllers and processors to maintain records of data processing under their responsibility and to cooperate with the supervisory authority is introduced in Article 30 of the GDPR²²⁸. The GDPR, empowers member states to bring in derogations to the regulation in specific situations²²⁹.

In Article 37 of the GDPR a new obligation of the controller and the processor is introduced: the designation of a Data Protection Officer (DPO), in certain occasions which are described in paragraph one of the Article²³⁰. The GDPR extended the liability for the damage caused to the data subject by processing of data that infringes the GDPR. Under the regulation, liability covers not only the controllers but also the processors²³¹. As for sanctions for infringements of the GDPR, the member states' supervisory authorities are obliged to develop rules for administrative fines imposed

²²²Article 40, Regulation (EU) 2016/679.

²²³Article 42, Regulation (EU) 2016/679.

²²⁴Christina Tikkinen-Piri, Anna Rohunen, JouniMarkkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, p 12.

²²⁵Paul Van den Bulck, Article, Transfers of personal data to third countries, 15 September 2017, p 245.

²²⁶Articles 33-34, Regulation (EU) 2016/679.

²²⁷Article 27, Regulation (EU) 2016/679.

²²⁸Christina Tikkinen-Piri, Anna Rohunen, JouniMarkkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, p 9.

²²⁹The Royal Society, Data Governance: Landscape Review, June 2017, p 16.

²³⁰Article 37, Regulation (EU) 2016/679.

²³¹Article 82, Regulation (EU) 2016/679.

on the controller, its representative or the processor²³². The imposition of these fines depends on the circumstances of each individual case and the maximum amount is up to 4% of the annual worldwide turnover or EUR 20 million, depending on whichever is higher²³³.

3.5. d. INDIVIDUAL RIGHTS UNDER GDPR

Articles 13 and 14 of the GDPR include new additions concerning the information provision to the data subject²³⁴. Moreover, Article 15 stipulates the right of a data subject to have access to the processed information. Also, the GDPR ensures the rights to rectification, erasure and restriction of data processing and introduces the right to data portability²³⁵.

In addition to the above mentioned, the GDPR guarantees the right of the data subject to object to the processing of his or her data for certain purposes and for direct marketing purposes, at any time²³⁶.

3.5. e. RELATION BETWEEN e-PRIVACY DIRECTIVE & GDPR

The Directive 2002/58/EC regarding the processing of personal data and the protection of privacy in the electronic communications' sector is known as the ePrivacy Directive or "cookie law"²³⁷. It was amended with the Directive 2009/136/EC²³⁸ and now a proposal of the EC for an ePrivacy Regulation is on the move. The proposed ePrivacy Regulation aims to enhance trust and security in the DSMS²³⁹. Furthermore, the proposed regulation ensures that privacy rules will be applicable not only to traditional telecom providers but also to new ones such as Facebook Messenger, Viber, Skype, Gmail, etc.²⁴⁰. It will also: provide stronger rules for people and businesses, guarantee communications' content and metadata (e.g.time of a call or location), create new opportunities for business, create a more user-friendly environment on cookies and other identifiers and enhance protection against spam (by default or do not call list)²⁴¹.

²³²Christina Tikkinen-Piri, Anna Rohunen, JouniMarkkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, p 13.

²³³Article 83, Regulation (EU) 2016/679.

²³⁴Christina Tikkinen-Piri, Anna Rohunen, JouniMarkkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, p 7.

²³⁵Articles 16,17,18,20, Regulation (EU) 2016/679.

²³⁶Articles 21, 22, Regulation (EU) 2016/679.

²³⁷The Royal Society, Data Governance: Landscape Review, June 2017, p 8.

²³⁸<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0136>

²³⁹<https://ec.europa.eu/digital-single-market/en/proposal-privacy-regulation>

²⁴⁰The Royal Society, Data Governance: Landscape Review, June 2017, p 8.

²⁴¹<https://ec.europa.eu/digital-single-market/en/proposal-privacy-regulation>

As for the existing legislation and its relation to the GDPR, the Directive 2002/58/EC is a “lexspecialis” with regard to the GDPR, which means that it complements the GDPR in the processing of personal data in the field of electronic communications and it prevails over it in case of conflict²⁴². Finally, the GDPR and the proposed ePrivacy Regulation are part of the overall reformation of the EU’s data protection framework, which includes a proposal of the European Parliament and of the Council for a regulation on the subject of free flow of non-personal data in the EU, as well²⁴³.

4. POLICIES RELATED TO DATA GOVERNANCE IN OTHER COUNTRIES

The following states were chosen as paradigms of good and innovative policies around the sector of governance of data and digital governance in general, based on criteria such as: economic growth, geopolitical and historical importance as nations, innovation in research, technology and law and their importance as nations that define policies globally in every sector, private or public. Four of them (USA, China, South Korea and Japan) are out of the European Region and one of them, Denmark, is a member of the EU. Denmark, with its innovative policies on data and digital governance, is considered as one of the most prominent nations not only in the EU but also globally, and can be considered as an excellent sample of how EU should develop and implement policies, legislation and guidelines around the sectors of digital governance generally and of governance of data specifically, in order to be globally competitive and innovator in every field of human flourishing.

4.1. USA

The United States of America are following a different approach, in contrast to EU, concerning the field of DG. The integrity of data as an industrial, commercial and financial asset comes forward as a main policy view and practice. This is outlined through a variety of federal and state laws, corporate policies and standards and through the handling of corporate America in situations such as the Facebook-Cambridge Analytica scandal²⁴⁴. However, EU’s policies around DG are focused firstly on the protection of individual rights and secondly on the protection and economic growth of business interests²⁴⁵.

The right to privacy is not explicitly expressed by the Constitution of the USA. Even though it had been applicable in US common law since 1890, it was the Federal Privacy Act (1974) that recognized the right to privacy as a fundamental right

²⁴² Article 95, Regulation (EU) 2016/679.

²⁴³ <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM%3A2017%3A495%3AFIN>

²⁴⁴ <https://www.theguardian.com/technology/2018/jan/31/data-laws-corporate-america-capitalism>

²⁴⁵ <https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/>

protected by the US Constitution²⁴⁶. The same Act could be recognized as the first global official document that embodied fair information principles and practices that were included in other regimes such as the EU's Data Protection Directive²⁴⁷. Still, the absence of an omnibus and modernized Act around privacy and the deficiency of central data protection authority both show that privacy and data protection sectors are being balanced between the obligations, statutes and involvement of various factorssuch as the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the Consumer Financial Protection Bureau, the Securities and Exchange Commission (SEC), state attorneys general, the Department of Health and Human Services, the judicial system, the Department of Education and US private plaintiffs' bar²⁴⁸.

As with the lack of an omnibus privacy law, the same situation exists with the data protection sector. The absence of a, similar to the GDPR, federal law is covered through a sectoral-based package of federal and state laws and guidelines developed by governmental agencies and industries. The Federal Trade Commission Act, is a federal law which provides consumer protection around unfair and misleading practices, with applicability to online-offline privacy and data security policies²⁴⁹. It applies to companies and individuals outside the scope of transportation, financial companies and telecommunications industry²⁵⁰. The Financial Services Modernization Act (Gramm-Leach-Bliley Act) establishes standards for the protection of customers' nonpublic, personal-financial information, which are stored by financial institutions (banks, security firms and insurance companies)²⁵¹. Also, the GLBA is applicable to non-affiliated third parties by prohibiting the exposure of such data to them, unless exceptions are applied, and its main task is to enforce consumer's privacy by obligating financial institutions to supply notifications of information-sharing practices that they develop and apply²⁵². As for entities that sustain consumer credit reporting information or information provided from consumer credit report, the Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions Act, is applicable²⁵³. This Act is applicable to every consumer reporting agency which

²⁴⁶The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 364.

²⁴⁷The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 364.

²⁴⁸The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 365.

²⁴⁹[https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1)

²⁵⁰[https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1)

²⁵¹The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 373.

²⁵²The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 373.

²⁵³The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 373.

is related with consumer's creditworthiness, credit history, capacity and reputation, criteria that are used to define consumers' entitlement to insurance or credit²⁵⁴.

In the sector of healthcare, the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), is the basic strategic and legislative tool for the protection of personal information of patients. It regulates medical information, providing federal-based standards for electronic healthcare transactions and gives patients the right to choose if their personal-health information is able to be shared with other organizations²⁵⁵. The HIPAA contains a privacy rule (the Standards for privacy of Individually Identifiable Health Information) which applies to the collection and use of personal-health information, and a security rule (the Security Standards for the Protection of Electronic Protected Health Information) which stipulates standards for the protection of medical data²⁵⁶. Furthermore, HIPAA applies to covered entities such as health plans, healthcare clearing houses and providers who participate to electronically provided financial and administrative transactions. It also applies to service providers of covered entities and provides requirements in relation to employee medical insurance²⁵⁷. Of such importance are also the HIPAA Omnibus Rule (2013), revised privacy, security, breach notification and enforcement rules²⁵⁸.

In the field of communications and technological innovation, there are four-main federal laws related to privacy and data protection. The Controlling of the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) regulates commercial email messages, providing the conditions under which companies use marketing advertisements through email addresses and the Telephone Consumer Protection Act regulates the use and collection of telephone number correspondingly²⁵⁹. In addition, the Electronic Communications Privacy Act regulates the interception of electronic communications, protecting privacy and security of the content of certain electronic communications and related records, while the Computer Fraud and Abuse Act regulates computer interference by prohibiting hacking and

²⁵⁴[https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1)

²⁵⁵The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 374.

²⁵⁶[https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1)

²⁵⁷The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 374.

²⁵⁸[https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1)

²⁵⁹The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 373.

other ways of unauthorized access or trespass to computer systems²⁶⁰. Moreover, it applies to intruders and cybercriminals of trade secrets and other precious corporate information²⁶¹. The use of cookies and other online tracking tools are not regulated specifically under US federal legislation but there are subjects regulated under the Digital Advertising Alliance code of conduct, FCC regulations on the collection and revealing of location tracking by telecommunications providers and FTC's and California's best-practices suggestions for mobile apps and platforms²⁶².

In the area of children's data protection there is the Children's Online Privacy Protection Act (COPPA), which is applicable to operators of commercial websites and online services that are addressed to children under the age of 13, but also to general websites and online services which collect personal information for persons under the age of 13²⁶³.

In the field of cybersecurity, the Cybersecurity Act, which includes the Cybersecurity Information Sharing Act (CISA), is the most advanced and modernized federal law around cybersecurity area. Especially, the CISA is created to promote cyber threat information sharing and liability protection for sharing cyber threat information between government and private parties²⁶⁴. The Cybersecurity Act is not an omnibus federal law, but it collaborates with other federal laws (GLBA, HIPAA), the National Institute for Standards and Technology (NIST) cybersecurity framework, state laws (Massachusetts's state law) and presidential executive orders (PPD-41) to establish a coherent and solid policy around the crucial, for USA's interests, area of cybersecurity²⁶⁵.

Moreover, another significant federal law was passed in 2016. The Judicial Redress Act provides the opportunity to citizens of ally countries (mainly EU citizens) to seek redress in US courts for violations of privacy, when their personal information is shared with law enforcement agencies²⁶⁶. Finally, the Federal Information Security Management Act (FISMA), which is part of the larger e-Government Act of 2002 and which requires federal agencies to create, store and implement an information security and protection program²⁶⁷, finishes the puzzle of significant data protection, security and privacy federal laws.

²⁶⁰The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 375.

²⁶¹The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 375.

²⁶²The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 373.

²⁶³The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 375.

²⁶⁴The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 389.

²⁶⁵The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 386-390.

²⁶⁶[https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1)

²⁶⁷<https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/>

In state level, the most prestigious and modernized law around data protection and privacy, is California's Consumer Privacy Act, which was introduced in 2018 (it will take force on January 1, 2020) and is characterized as GDPR-like privacy law²⁶⁸. Also, from March 2018 all 50 US states, as well as the District of Columbia, Guam, Puerto Rico and the US Virgin Islands have established breach notification laws which oblige companies to notify consumers in the occasion of personal information²⁶⁹. In addition to that the USA enacted, in 2018, the Clarifying Lawful Overseas Use of Data Act, which is a federal law that amends the Stored Communications Act and allows federal law enforcement to force U.S.-based technology companies through warrant or allows subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil²⁷⁰.

Regardless of the regulations that are established around data governance, the last two presidential administrations provide an environment where data policies are dealt as a strategic asset to further development, economic growth and security of American interests. Previous to them, Acts such as the e-Government Act (2002) and the Data Quality or Information Quality Act (2001), were the first steps to digital transformation of USA's federal government model.

President Obama, showed his willpower to the area of open data government on his first day in office with an executive order (Memorandum on Transparency and Open Government), that required agencies to classify and release data sets of high quality²⁷¹. After that, in May 2009, the Data.gov website was launched in order to provide access to high value and machine readable datasets for the public²⁷². This is a repository which includes data sources from federal, state, local and tribal governments²⁷³. On December 8, 2009, the Open Government Directive or OMB Memorandum M-10-06 was enacted to orchestrate executive departments and agencies to provide specific actions on the implementation of principles (transparency, participation, collaboration), which were addressed in the President's Memorandum on Transparency and Open Government²⁷⁴. The four principles that are provided through this Directive are²⁷⁵: publication of government information online,

²⁶⁸<https://www.dataprotectionreport.com/2018/06/california-passes-major-privacy-legislation-expanding-consumer-privacy-rights/>

²⁶⁹<https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/>

²⁷⁰https://en.wikipedia.org/wiki/CLOUD_Act

²⁷¹<https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government>

²⁷²<https://www.data.gov/about>

²⁷³<https://digital.gov/resources/how-to-get-your-open-data-on-data-gov/#non-federal-data>

²⁷⁴<https://digital.gov/open-government-directive/>

²⁷⁵<https://www.state.gov/digital%20strategy/>

improvement of the quality of government information, creation and institutionalization of a culture of open government and creation of a policy framework for Open Government. The next step to digital transformation was launched on May 23, 2012 with the Digital Government Strategy. The Digital Government Strategy is built upon several initiatives such as²⁷⁶: Executive Order 13571 (Streamlining Service Delivery and Improving Customer Service), Executive Order 15576 (Delivering an Efficient, Effective and Accountable Government), the President's Memorandum on Transparency and Open Government, OMB Memorandum M-10-06 (Open Government Directive), the National Strategy for Trusted Identities in Cyberspace (NSTIC) and the 25-point Implementation Plan to Reform Federal Information Technology Management (IT Reform). One of the basic constituent of Digital Government Strategy, the open data policies, was further promoted with the Memorandum M-13-13, Open Data Policy-Managing Information as an Asset²⁷⁷. Its main task is to enhance public access to valuable government information, to improve operational efficiencies at reduced costs, to upgrade services and support mission needs and to protect personal information²⁷⁸. On May 9, 2014, President Obama signed the Digital Accountability and Transparency Act (DATA Act), which demands federal agencies to publish their spending data in accordance to transparent standards, that will promote and enhance the quality of government information, the decision-making process and the efficiency of government tasks to the American people²⁷⁹.

The Obama Administration also introduced the third Open Government National Action Plan (The Open Government Partnership) in 2015, with its main goals to improve accessibility issues and to provide codifying web standards²⁸⁰.

The Trump Administration continues previous policies around governance of data and recognizes data as a strategic asset, which will provide economic growth and government effectiveness, through the President's Management Agenda (PMA)²⁸¹. The implementation of this strategy is developed through a Federal Data Strategy which includes four key components²⁸²:

1) Enterprise Data Governance.

²⁷⁶<https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html>

²⁷⁷<https://www.state.gov/digitalstrategy/>

²⁷⁸<https://www.state.gov/digitalstrategy/>

²⁷⁹https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/final_us_open_government_national_action_plan_3_0.pdf

²⁸⁰https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/final_us_open_government_national_action_plan_3_0.pdf

²⁸¹The President's Management Agenda, 2018, p15.

²⁸²The President's Management Agenda, 2018, p15-16.

- 2) Data access, use and augmentation.
- 3) Decision-making and accountability.
- 4) Data commercialization, innovation and public use.

Building on the 2014 DATA Act, the PMA provides the government will to establish policies and procedures that empower stakeholders to access and use data assets in an efficient and effective way²⁸³. Furthermore, through the enterprise data governance plan, the government “will set priorities for managing data as a strategic asset, including establishing data policies, specifying roles and responsibilities for data privacy, security and confidentiality protection, and monitoring compliance with standards and policies throughout the information lifecycle”²⁸⁴. In addition, improvement of the use of data assets for decision-making and accountability for the Federal’s Government internal and external uses and the facilitation of the use of Federal Government data assets by external stakeholders through commercial ventures, innovation and other public uses, will provide the four pillars that Federal Data Strategy builds on²⁸⁵. The Federal Data Strategy is a cross-agency initiative which includes the Department of Commerce, the Small Business Administration, the White House Office of Management and Budget and the White House Office of Science and Technology Policy²⁸⁶.

According to Federal Data Strategy website, federal data are approached not only as a strategic asset but also as an important national resource²⁸⁷. It is a tool which will help the government to be more efficient, transparent and accountable, providing also knowledge of the government’s social, economic and environmental data to the public²⁸⁸. This strategy is based upon four categories of principles which are the foundation for the development of its initiatives, programs and statistics around governance of data. The principles are divided in four general categories which are the following²⁸⁹: Mission Statement, Ethical Governance, Conscious Design and Learning Culture.

President’s Trump PMA does not include a specific timeline for the full accomplishment of this strategy but notices that it will take time because it is a collaborative effort that includes the efforts of the Federal Government, private industry and research institutions²⁹⁰. In addition, this administration, following the paradigm of the previous one, provides federal legislation around data governance.

²⁸³<https://fedtechmagazine.com/article/2018/05/why-state-department-sees-data-strategic-asset>

²⁸⁴The President’s Management Agenda, 2018, p15.

²⁸⁵The President’s Management Agenda, 2018, p17.

²⁸⁶<https://strategy.data.gov/>

²⁸⁷<https://strategy.data.gov/principles/>

²⁸⁸<https://strategy.data.gov/principles/>

²⁸⁹<https://strategy.data.gov/principles/>

²⁹⁰The President’s Management Agenda, 2018, p17.

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) is an example of the continuation of data legislation. Being part of the omnibus Consolidated Appropriations Act, the CLOUD Act is a federal law that will change the way the US government can access user's data stored overseas²⁹¹. It is a federal law based on a collaborative effort of the US government and online service providers that will try to solve cross-border data stored problems, providing a statutory change, based on legal rules, which should apply when one government's seek criminal evidence are in contrast to privacy and sovereignty issues of another country²⁹².

Furthermore, the USA are moving forward to the digitization of their government, providing new federal legislative documents, which will contribute to the general plan for more transparent, efficient and accountable governance of data, if they are finally enacted. The Open, Public, Electronic and Necessary Government Data Act (OPEN Government Data Act), which is a codification of President's Obama executive order on Making - the New Default for Government Information and the,2018, proposed by two Democrat senators, Customer Online Notification for Stopping Edge-provider Network Transgressions Act (CONSENT Act) - Open and Machine Readable, are two different federal legislative proposals, which will help to the overall effort for a transparent, fair, accountable, clear, effective and efficient future of governance of data in USA, if they are finally passed and enacted⁽²⁹³⁾⁽²⁹⁴⁾.

4.2. CHINA

The People's Republic of China is the most populated country in the world with more than 1.4 billion residents. It is governed by the Communist Party since 1949. The last 18 years China's leadership attempts to change the old authoritarian regime in various ways. The former leadership under China's General Secretary of the Communist party, Hi Jintao(2002-2012), tried to govern the most populous country in a more "democratic manner" by providing ways for complaints to reach the corruption of the ruling class²⁹⁵. The current administration, under General Secretary Xi Jinping, is developing a different strategy to approach, control and understand a nation of 1.4 billion people²⁹⁶.

²⁹¹<https://iapp.org/news/a/the-cloud-act-explained/>

²⁹²<https://iapp.org/news/a/the-cloud-act-explained/>

²⁹³<https://www.insideprivacy.com/united-states/congress/senate-democrats-propose-consent-act/>

²⁹⁴<https://www.congress.gov/bill/115th-congress/house-bill/1770?q=%7B%22search%22%3A%5B%22actionDateChamber%3A%5C%22114%7C%2015-09-18%5C%22+AND+%28billIsReserved%3A%5C%22N%5C%22+or+type%3A%5C%22AMENDMENT%5C%22%29%22%5D%7D>

²⁹⁵<https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/>

²⁹⁶<https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/>

Since his appointment, Xi Jinping has provided a series of plans that will try to modify China in a world leader country, using technology (AI and Big Data) and harvesting of data at the center of this overall initiative²⁹⁷. From a legislative perspective around the sector of governance of data, China does not possess a unified law in data protection area²⁹⁸. Instead, there is a complex system of legal rules in relation to the protection of personal information. In 2012, the Standing Committee of the National People's Congress (NPC) came to the conclusion of empowering internet information protection by requiring internet service providers to safeguard Chinese's people personal electronic information with a set of principles²⁹⁹. After that, a sector-specific legal regime for personal information was formed under several departments of the State Council such as³⁰⁰: the Ministry of Industry and Information Technology (MIIT), the State Administration for Industry and Commerce (SAIC), the National Health and Family Planning Commission (NHFPC) and People's Bank of China (PBOC). Furthermore, the above mentioned NPC's decision provides many of its requirements under the Consumer Rights Protection Law, which was enacted in 2014³⁰¹. In addition, the Tort Liability Law, enacted in 2010, provides many provisions related to the protection of personal data and it is the first law that treated the right of privacy as an independent type of civil right³⁰². Another tool for the protection of personal information is the Article 253 of the Chinese Criminal Law (as provided in Amendment VII and Amendment IX to the Criminal Law)³⁰³. It provides the penalization of selling or illegally offering personal information, gained from an individual (including governmental authorities and companies) in his or her employment³⁰⁴. Moreover, when it comes to the area of cookies, other tracking identifiers and behavioral advertising, China does not prohibit their use because of the overall policy around innovation on Big Data, AI and Cloud Computing³⁰⁵. As for cross-border transfer of personal information, general privacy prerequisites under

²⁹⁷<https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/>

²⁹⁸The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 105.

²⁹⁹The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 105.

³⁰⁰The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 105.

³⁰¹The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 108.

³⁰²The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 108.

³⁰³The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 108.

³⁰⁴The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 108.

³⁰⁵The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 109.

civil law and requirements under industry-specific regulations and rules are required³⁰⁶. In addition to that, the State Secrets Protection Law (2010) and the Measures for Implementing the State Secrets Protection Law (2014) prohibit carrying, transmitting, posting and transporting of documents, which are including state secrets, without the approval of adequate governmental authorities³⁰⁷.

Another three pieces of legislation relating to information and technology security have been provided since 2014. The National Security Law (NSL), the Counter-Terrorism Law (CTL) and the Cyber Security Law (CSL) are the most modernized legal documents of China in this area. The first two are bringing changes and innovation of policies around national cyberspace sovereignty and counter-terrorism activities³⁰⁸. The Cybersecurity Law was enacted in 2017 and it is considered to be an omnibus law on cybersecurity issues and it is also fundamental for the protection of personal information³⁰⁹. The CSL includes a set of obligations for network operators but it also provides new rules on the protection of personal information such as data breach notification requirements and data anonymization³¹⁰. It is made upon six systems³¹¹:

- 1) The Internet Information Content Management System.
- 2) The Cybersecurity Multi-Level Protection System.
- 3) The Critical Information Infrastructure Security Protection System.
- 4) The Personal Information and Important Data Protection System.
- 5) Network Products and Services Management System.
- 6) The Cybersecurity Incident Management System.

This law, along with additional measures which accompany it and many draft standards, all together consist China's data protection regime, which focus on personal information, data transfers and data management and governance³¹². This law is also combined with other national strategies which focus on the technological innovation and economic growth of China. The main strategies around this area are³¹³: National Cyberspace Strategy (2016), International Strategy for Cooperation in Cyberspace (2017), 13th Five-Year Plan for Information (2016), 13th Five-Year Plan for Major Science and Technology Projects (2016), National People's Congress Standing Committee Regulations on Strengthening Network and Information

³⁰⁶The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 112.

³⁰⁷The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 112.

³⁰⁸The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 115.

³⁰⁹The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 115.

³¹⁰The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 107.

³¹¹<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/>

³¹²<https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr>

³¹³<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/>

Protection and Technology-specific plans around big data, semiconductors, cloud services and artificial intelligence (AI).

Another major strategy around technological innovation and governance of data for the economic and social growth of China is the Next Generation Artificial Intelligence Development Plan which was launched in 2017, by the State Council of China³¹⁴. The strategic objectives of this enormous plan are divided in three timeline periods³¹⁵: The first goal of this plan is to provide global standards for AI by the year 2020. The second one is to establish AI laws and regulations by the year 2025 and the third one is to drive China to the top world's AI developer by the year of 2030.

This agenda is one precious key to the economic development and industrial upgrading of China. It will be involved in every strategic area of Chinese policy, from military advancement and minimizing the exploding cost of healthcare to effective transportation and accountability of the civil servants³¹⁶. In addition, it will be used as a tool that will provide a future, where public security and social stability are also at the center of its policies³¹⁷. This initial plan is enhanced with initiatives such as the Three-Year Action Plan to promote the Development of New-Generation AI Industry (2018-2020), which was released by the MIIT, and the decision of the Ministry of Science and Technology to add "AI 2.0" technologies (big data intelligence, cross-media intelligence, hybrid-augmented intelligence, autonomous intelligent systems etc.) to the "15-Science and Technology Innovation 2030 Megaprojects"³¹⁸. This strategy, like almost every major strategy of China, is assisted by the private sector with the three biggest commercial and technological companies of China (Baidu, Alibaba and Tencent), to play a critical role to its development³¹⁹.

The combination between technological innovation and governance of data for the economic and social growth of China is also triggered by another big project. The Internet Plus strategy aims to combine and integrate mobile internet, IOT, cloud computing and big data with manufacturing, e-commerce, industrial networks, internet banking and it also aims to increase the international appearance and influence of internet companies³²⁰. This action plan was initially raised in 2013 by entrepreneurs in IT industry, with the main goal to transform China into a world class

³¹⁴<https://www.insideprivacy.com/artificial-intelligence/chinas-vision-for-the-next-generation-of-ai/>

³¹⁵<https://www.insideprivacy.com/artificial-intelligence/chinas-vision-for-the-next-generation-of-ai/>

³¹⁶<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/>

³¹⁷<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/>

³¹⁸<https://thediplomat.com/2018/02/chinas-ai-agenda-advances/>

³¹⁹<https://thediplomat.com/2018/02/chinas-ai-agenda-advances/>

³²⁰<https://forbes.com/sites/gordonchang/2015/04/19/chinas-internet-plus-strategy-a-net-minus/#4a378916315d>

industrial power by year 2025³²¹. Moreover, another big project that is relied upon the usage of big data technologies is Healthy China 2030. This plan was initiated in 2016, with the goal to provide better online health services that can improve diagnoses and treatment advice based on big data solutions³²². It is the first long-term healthcare program since the nation's founding in 1949, with a task to create an efficient, more accessible, more professional and personalized system of healthcare for the common population of the country³²³.

Apart from the above mentioned, China has another enormous, in thought and reality, plan to reshape its economic and social governance structure using data at the center of this initiative³²⁴. The so called "Social Credit System" is one of the most important programs of the Chinese government on its road to become the world's economic and technological leader. Using big data solutions and AI, this program will try to re-establish the economic and social structure of individuals and enterprises. According to the Planning Outline for the Construction of a Social Credit System(2014-2020), issued by the Chinese State Council, its main goal is the "construction of sincerity in government affairs, commercial sincerity and judicial credibility"³²⁵. The plan introduces three projects to establish a social credit system³²⁶: the Government Affairs Information Openness Project, Rural Credit System Construction Project and Small and Micro-Enterprise Credit System Construction Project. Furthermore, it is a coordinated effort between the Chinese government and major enterprise players such as³²⁷: China Rapid Finance, which is a partner of social-network giant Tencent, Alibaba, Baihe and DidiChuxing. A paradigm of how this system works is the Sesame Credit, built by a subsidiary of the Chinese e-commerce giant Alibaba, Ant Financial. Sesame Credit is one of the earliest parts of this system and it assigns citizens with a score of 350 to 950 points based on factors such as credit history, fulfilment capacity, personal characteristics, behavior and preference and interpersonal relationships³²⁸. If a user, has a score of 600 or more points, he or she can enjoy "privileges" such as renting cars without putting down a deposit, reduction in paperwork for visas or checking out from hotels faster³²⁹. Even if Alibaba is

³²¹ <https://www.telegraph.co.uk/sponsored/china-watch/technology/11563092/china-internet-plus.html>

³²² <https://www.ft.com/content/43170fd2-a46d-11e7-b797-b61809486fe2>

³²³ <https://www.nytimes.com/2018/09/30/business/china-health-care-doctors.html>

³²⁴ <http://www.medialaws.eu/chinas-social-credit-system-a-governance-model-in-the-era-of-big-data/>

³²⁵ <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>

³²⁶ <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>

³²⁷ <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

³²⁸ <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

³²⁹ <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

refusing to connect negative posts on social media with affected scores, it offers tips to assist individuals on how to enhance their scores, including warning about the downsides of friending someone who has a low score³³⁰.

From the government side, a few local governments have already implemented social credit scores. For example, in the city of Rongcheng everyone begins with 1.000 points and they can gain points from a donation to a charity or lose points by violating traffic laws³³¹. Those who have good scores gain discounts on winter heating supplies or good terms on mortgages while those with bad ones might lose access to bank loans or get promoted in government jobs³³². In general, high scores can gain better access to discounts, loans, visas or public procurement while low scores lead to situations such as bans from commercial partnerships, job offers or restrictions on getting involved with public projects³³³. Moreover, the Chinese government has already had a website, with the help of Baidu, which provides information about the credit rating of the people, using data from 37 central government departments³³⁴.

Also, the document with the title “Warning and Punishment Mechanisms for Persons Subject to Enforcement for Trust-Breaking”, which was released on September 26, 2016 by the State Council General Office, updates this policy by providing penalization of untrustworthy behavior³³⁵. The most important principle of this official document is clear: “If trust is broken in one place, restrictions are imposed everywhere”³³⁶. People with low ratings will be subjects to “restrictive control on consumption within holiday areas or travel businesses”³³⁷. These are some of the penalties which are designated now, while the system is operating in a voluntary mode. But, from the year 2020 the system will have been mandatory and then the consequences of a good or bad act of a citizen or legal entity will be incorporated in a highly advanced and complex technological system where everything and everyone will be measured with a digital number. When, and if this system is finally fully implemented, then a change to its statute from voluntary to obligatory will also bring a change to its penalties and this is for certain a core change

³³⁰<https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

³³¹<https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/>

³³²<https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/>

³³³<http://www.medialaws.eu/chinas-social-credit-system-a-governance-model-in-the-era-of-big-data/>

³³⁴<https://www.newscientist.com/article/dn28314-inside-chinas-plan-to-give-every-citizen-a-character-score/>

³³⁵<https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

³³⁶<https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

³³⁷<https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

to Chinese's society and business operation model, that will also affect the West World in various ways.

The Chinese government considers this system as a direction to its chaotic, enormous and poor regulated market economy, to punish companies and people who try to downsize the vision of China's prosperity and to create a trustworthy social environment not only for individuals but also for enterprises and the government itself. From another point of view, westerners might confront this plan as an authoritarian system whose main focus is to manipulate and oppress the population of the biggest country in the world. However, according to Luciano Floridi, a professor of philosophy and ethics of information at the University of Oxford, we are now entering the fourth "de-centering shift" of our view in self-understanding³³⁸. He supports that this shift is happening with the merger of our online activity with an offline one, creating a new state of being³³⁹. This is what he calls on-life and it is a mixture of social, physical and virtual experiences³⁴⁰. This opinion is not just viewed from the example of Social Credit System. Western civilization is providing an environment where digital and actual life are combined and affect each other's decisions, engagements and reactions in multiple ways and matters. The angle of westerners' approach and policies is different but it does not mean that it is irrelevant to the Chinese point of view about the combination of technology and cultural and social heritage to the creation of a new social model.

4.3. JAPAN

Japan is one of the most advanced economies globally, providing technological innovation and research development in a world's wide scale. Among its achievements as a nation, Japan is also included in the top 10 of countries which are leading e-government development³⁴¹.

The Japanese Government promotes various initiatives around digital governance whose main tool, to succeed in this purpose, are data and information. One of the most prominent initiatives is the so called "Declaration to be the World's Advanced IT Nation". It is a governmental coordinated effort which is guided by the Deputy Chief Cabinet Secretariat for information technology and IT Strategic Headquarters³⁴². At the core of this initiative, lays the vision of the Japanese government to establish an environment, where the sharing of information and data between industry, universities, government and individuals, will enhance the development of an IT user society at the world's highest levels by the year 2020³⁴³.

Another strategy, which is highly connected to the previous one, is the Open Government Data Strategy. Initiated in 2012, this strategy is mainly focusing on

³³⁸<https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

³³⁹<https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

³⁴⁰<https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

³⁴¹United Nations E-Government Survey 2018: Gearing e-Government to support transformation toward sustainable and resilient societies, p 92.

³⁴²Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society: Declaration to be World's Most Advanced IT Nation, p 4.

³⁴³Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society: Declaration to be World's Most Advanced IT Nation, p 5-7.

promoting the use of public data while supporting open government with the understanding that public data is an asset of the people³⁴⁴. Moreover, based on the Open Government Data Strategy, Japan's Open Data Charter Action Plan was initiated in 2013. This plan combines the previous mentioned strategies with two other strategies, Roadmap for Promotion Open Data in Electronic Administration and Basic stance on public release of ministry information to encourage secondary use (guidelines), to provide a holistic approach around the promotion of open data in Japan³⁴⁵. Additionally, Japan is facing digital transformation providing two main strategies which use data and information at the center of their operations. IT Policy and Strategy "Society 5.0", and AI Technology Strategy are two strategies with the goal to offer an interconnected environment for governmental agencies, private sector and individuals, promoting new technologies that will enhance prosperity and productivity of the nation by safeguarding and boosting critical fields such as economy, industry, healthcare and welfare⁽³⁴⁶⁾⁽³⁴⁷⁾. Finally, Japan has a comprehensive "Digital Government Strategy" and a "Basic Plan for the Advancement of Utilizing Public and Private Sector Data"³⁴⁸.

Apart from these policies, Japan has a well-established law for data protection and privacy. The Act on the Protection of Personal Information (APPI), as it was amended in 2016, is providing the legal framework around data protection and privacy³⁴⁹. Its guidelines, provided by the independent agency (Personal Information Protection Commission) for the protection of personal information and its special guidelines for specific sectors (medical and financial), are providing the practices of this law³⁵⁰. Under the Amended APPI, processing of anonymized data and sharing of them between business operators for development and innovation purposes are applicable³⁵¹. Furthermore, this law establishes a specific provision for international data transfers by requiring the consent of the principal to international transfers of personal data except for certain cases³⁵². In addition to this law, the Act on the prohibition of Unauthorized Computer Access (APUCA), as it was enacted in 2012, and Social Security and Tax Number Act are laws which cover the areas of cybersecurity and social security and taxation purposes correspondingly, providing the legal framework around data protection and privacy³⁵³.

³⁴⁴IT Strategic Headquarters: Open Government Data Strategy, July 2012.

³⁴⁵Japan Open Data Charter Action Plan, 29 October 2013, p 1-3.

³⁴⁶Ministry of Internal Affairs and Communications (MIC), Japan: AI Strategy and Related Activities in Japan (overview), 25 October 2017.

³⁴⁷Ministry of Economy, Trade and Industry (METI), Japan: IT Policy in Japan, 20 February 2018.

³⁴⁸United Nations E-Government Survey 2018: Gearing e-Government to support transformation toward sustainable and resilient societies, p 92.

³⁴⁹The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 190.

³⁵⁰The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 190.

³⁵¹The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 192-193.

³⁵²The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 199.

³⁵³The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 193, 203-204.

4.4. SOUTH KOREA

The Republic of Korea is also considered a leader in the development and implementation of e-government policies. According to UN's Survey 2018 on e-government development, South Korea is ranked in the 3rd place worldwide³⁵⁴. Starting from 1980s with programs such as the National Basic Information System (NBIS) and later in the 1990s, with the streaming of applicable laws and institutions, South Korea initiated its first national e-Government agenda in 2001³⁵⁵. Since then, the Korean government had made major steps to provide digital government strategies, resulting on requests from governments of developing countries to teach them how to implement efficient and transparent e-Government solutions to their countries³⁵⁶. In addition to that, the Korean government has trained more than 4.000 public officials of other countries on e-government issues over the last 10 years³⁵⁷.

The Republic of Korea has established various projects around the sector of digital governance. The latest and most advanced plan is the so called "e-Government Master Plan 2020" and it is constructed upon five strategies³⁵⁸: developing all-digital government services, reforming public administration based on intelligent information, creating more digital friendly industries, building an e-government platform and solidifying a position in the global e-government as a major e-government exporter. It is a plan that promotes the most advanced digital government solutions, taking in consideration the latest technological achievements and the needs of its citizens. The most advanced and well established practices of their e-government plan are³⁵⁹: Electronic Procurement Service, Electronic Customs Clearance Service, Comprehensive Tax Services, Internet Civil Services, Patent Service, e-People: Online Petition & Discussion Portal, Single Window for Business Support Services, On-nara Business Process System (BPS), Shared Use of Administrative Information, National Computing & Information Agency (NCIA).

Another major initiative is the "E-Government 3.0". This is the 5th stage of Korea's e-Governance plans and its main task is to provide ICT innovation for service integration, investment in IOT, cloud computing technology, Big Data for creative economy and ICT-enabled growth and jobs³⁶⁰. Through this initiative, the Korean

³⁵⁴United Nations E-Government Survey 2018: Gearing e-Government to support transformation toward sustainable and resilient societies, p 90.

³⁵⁵Ministry of Public Administration and Security: e-Government of Korea-Best Practices, p 4.

³⁵⁶United Nations E-Government Survey 2018: Gearing e-Government to support transformation toward sustainable and resilient societies, p 90.

³⁵⁷United Nations E-Government Survey 2018: Gearing e-Government to support transformation toward sustainable and resilient societies, p 90.

³⁵⁸United Nations E-Government Survey 2018: Gearing e-Government to support transformation toward sustainable and resilient societies, p 137.

³⁵⁹United Nations E-Government Survey 2018: Gearing e-Government to support transformation toward sustainable and resilient societies, p 137.

³⁶⁰World Bank Group, Bringing Government into the 21st century: The Korean Digital Governance Experience, 2016, p 5.

government is enhancing and promoting open government data in order to create an innovative, transparent and efficient environment for people and businesses and is supporting this project through the Act on Promotion of the Provision and Use of Public Data (2013)³⁶¹.

These initiatives are the main projects of South Korean government for the next digital transformation period and they encompass all sector-oriented plans for the digital governance of this nation. Apart from that, the Republic of Korea has established a solid legal framework around data protection and privacy. The right to privacy is a fundamental right under the Constitution of Korea and the right to control one's personal information has recognized as a separate, from the one to privacy, right by the Constitutional Court of South Korea³⁶². The main act on the protection of personal data is the Personal Information Protection Act (PIPA), but there are also other sector-oriented acts which regulate personal data. The processing of personal information by online service providers and telecommunications is regulated by the Act on Promotion of Information Communication Network Usage and Information Protection (the Network Act), while the processing of (personal) credit information by financial institutions is regulated by the Act on Usage and Protection of Credit Information (the Credit Information Act)³⁶³. The PIPA is applicable on cybersecurity sector in general, although other acts, such as the Network Act and the Credit Information Act, are issued as well. Moreover, as South Korea is considered a country with strict data protection regulatory environment, and taking in consideration the consequences of this situation in a highly advanced economy, the Korean regulatory system enacted the Guidelines for De-Identification of Personal Information (2016) in order to balance the regulatory needs with the developments in IT industry³⁶⁴. In addition to these laws, there are several others that regulate the processing of specific types of personal information such as³⁶⁵: the Location Information Act, the Medical Service Act, the Pharmaceutical Affairs Act, the Act on Protection of Communication Secrecy and the Act on Real Name Financial Transactions and Confidentiality. Finally, South Korea has also got an act on cloud computing, the Act on Development of Cloud Computing and Protection of Users, which was enacted in 2015³⁶⁶.

In general, South Korea is driven to innovation and progress not only by the so called "chaebols", like Samsung, Hyundai, LG Electronics and Pohang Iron and Steel Company³⁶⁷. It is a mixed, private and public, force that has established a plan on the

³⁶¹<http://www.koreaitimes.com/news/articleView.html?idxno=58369>

³⁶²The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 206.

³⁶³The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 206.

³⁶⁴The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 207.

³⁶⁵The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 211-212.

³⁶⁶The Law Review: The Privacy, Data Protection and Cybersecurity. Law Review, Fourth Edition, 2017, p 212.

³⁶⁷Institute for Defense Analyses; Innovation Policies of South Korea, p 6.

prosperity and wealth of its people many decades ago and is now facing its future with confidence and strength.

4.5. DENMARK

Denmark is a country where governance, through digitization, is a top priority over the last fifteen years. Starting back in 2001, Denmark provided the digital signature to its citizens, through its first digital strategy³⁶⁸. Continuing, the establishment of NemKonto (mandatory default citizens' account for payments from the authorities), Virk.dk (digital public services web portal for businesses), Sundhed.dk (web portal providing personal access to all own health data), NemID (eID solution, public eID and digital signature), NemLog-in (federated user management and log-in to online public services) and Digital Post (digital mailbox for messages and communications from public authorities) are some of the achievements of Denmark's digital strategies for better governance³⁶⁹.

According to e- Government Survey 2018 of the UN, Denmark is leading e-government development and e-participation worldwide³⁷⁰. The latest strategy, Digital Strategy 2016-2020, builds on three goals³⁷¹:

- 1) Digital solutions must be easy to use, quick and ensure high quality.
- 2) Public sector digitization must provide good conditions for growth and security.
- 3) Confidence must be in focus at all times.

These goals are supported by focus areas, which include several initiatives to support the establishment of the three main goals. The first goal is supported by the focus areas of a user-friendly and simple digital public sector, better use of data and quicker case processing and better and more connected welfare services³⁷². The second goal is supported by the focus areas of better framework for business community, public sector's data as a growth driver and of an efficient-utilities sector while the third one is supported by the focus areas of a public sector which protects data, robust digital infrastructure and digitization for everyone³⁷³. This strategy aims to provide a solid and secure digital environment where the public institutions of every level (local, regional, national), the private sector and citizens contribute to the establishment and well-being of a stronger digital future.

Furthermore, Denmark has established various strategies around digital governance. The e-Government Strategy 2011-2015, Joint Public Digital Strategy: The Digital Road to Future Prosperity 2011-2015, was the predecessor of Digital Strategy 2016-2020, with its main goal to provide an environment where digital self-service solutions will be considered as a normal way for the citizens to interact with the public sector³⁷⁴. In addition, the Danish government, in collaboration with local

³⁶⁸A stronger and more secure Digital Denmark: Digital Strategy 2016-2020, May 2016, p 13.

³⁶⁹A stronger and more secure Digital Denmark: Digital Strategy 2016-2020, May 2016, p 13.

³⁷⁰United Nations E-Government Survey 2018: Gearing e-Government to support transformation toward sustainable and resilient societies, p 90, p 114.

³⁷¹A stronger and more secure Digital Denmark: Digital Strategy 2016-2020, May 2016, p 14.

³⁷²A stronger and more secure Digital Denmark: Digital Strategy 2016-2020, May 2016, p 15.

³⁷³A stronger and more secure Digital Denmark: Digital Strategy 2016-2020, May 2016, p 15.

³⁷⁴European Union, European Commission, Joinup, the ISA program: e-Government in Denmark, 2015, p14.

governments and Danish Regions, established another digital strategy back in 2013. The so called “Strategy for Digital Welfare 2013-2020” is a policy which aims to provide a stronger and more applicable environment in the areas of healthcare, care for the elder people, social services and education with the use of ICT and welfare technology³⁷⁵. Moreover, Denmark has launched two Open Government Action Plans, in 2012 and 2013, and is a member of the “Open Government Partnership”, which is an international initiative with the goal to promote good governance and democracy through transparent and inclusive governance solutions³⁷⁶. The current Open Government Action Plan aims to provide more and better open data, tailored data (well defined and accessible) to guarantee a basis for citizen’s participation, more collaboration between civil society and public authorities, for a stronger public sector and more contribution to global openness and transparency, and for governance through digital solutions³⁷⁷.

Besides these strategic initiatives, Denmark has legislated various laws around e-government, data protection and privacy. The Danish Parliament passed a legislation in June 2012, on mandatory digital self-service and on digital post as part of the joint e-government strategy 2011-2015³⁷⁸. Moreover, Denmark has passed Acts on Access to Public Administration Documents (2014), on the re-use of public sector information (2014), which implements the Directive 37/2013/EU, and many Acts around e-governance³⁷⁹: The Act on Electronic Signature (2000), which implements the EU Directive on a Community Framework for Electronic Signatures (Directive 1999/93/EC), the Act on Information Society Services and Electronic Commerce (2002), which implements Directive 2000/31/EC, the Act on Electronic Communications Networks and Services (2011), which implements the EU regulatory framework for electronic communications (Directives 2002/21/EC, 2002/20/EC, 2002/19/EC, 2002/22/EC, 2002/58/EC, which were amended with Directives 2009/140/EC and 2009/136/EC), the government order No 712 concerning the procedures for the award public works contracts, public supply contracts and public work contracts, which incorporates in its annex the exact text of EU Directive 2004/18/EC on the coordination of procedures for the award of public work contracts, public supply contracts and public service contracts. The Government order No 936 concerning procurement procedures of entities operating in the water, energy, transport and telecommunications sectors (2004), which incorporates in its annex EU Directive 2004/17/EC, known as “utilities directive”.

On the area of data protection and privacy, the Denmark Parliament passed, in 2018, a new Act on the protection of personal information, the Data Protection Act, which repeals the Act on Processing of Personal Data (2000) and implements and supplements the GDPR in the Danish law system³⁸⁰. Furthermore, the above

³⁷⁵European Union, European Commission, Joinup, the ISA program: e-Government in Denmark, 2015, p17.

³⁷⁶DIGITALERINGSSTYRELSEN, Open Government Partnership: National Action Plan 2017-2019, p 4.

³⁷⁷DIGITALERINGSSTYRELSEN, Open Government Partnership: National Action Plan 2017-2019.

³⁷⁸European Union, European Commission, Joinup, the ISA program: e-Government in Denmark, 2015, p 20.

³⁷⁹European Union, European Commission, Joinup, the ISA program: e-Government in Denmark, 2015, p 20, p 23.

³⁸⁰<https://www.twobirds.com/en/news/articles/2018/denmark/the-danish-data-protection-act-has-been-passed>

mentioned, Act on Electronic Communications Networks and Services and the Act on Marketing Practices (2013), which implement the Directive on privacy and electronic communications (Directive 2002/58/EC) conclude the Danish legislation on ³⁸¹data protection and privacy.

5. CASE STUDIES ON DG, DATA PROTECTION & PRIVACY

5.1. Maximilian Schrems case study

The case of Maximilian Schrems v Data Protection Commissioner, C – 362/14, in front of the Court is considered a milestone case to the area of data protection and privacy.

In 2011, Max Schrems, an Austrian law student passed a semester abroad at Santa Clara University in Silicon Valley³⁸². He took a class where a young lawyer of Facebook issued matters in response to European privacy law. That triggered him to request his personal data from Facebook for a college paper and the social network send him back 1.200 pages of his personal data³⁸³. These files included every like and message over his Facebook profile, even messages related to the health condition of one of his friends, that were supposed to be deleted³⁸⁴.

After that, he started sending complaints to the Irish Data Protection Commissioner³⁸⁵, who was located at the city of Portarlinton (with a population of 8.000 residents), with minimum financial and human recourses. The complaints were considering Facebook's use on like buttons for user-tracking, facial-recognition technology that automatically tagged users in photos of their friends' profiles and "shadow" profiles³⁸⁶.

At first some of his complaints were transformed to acts on behalf of Facebook. Facebook, turned off facial recognition for EU users, enhanced users' access to their information and gave more clarity on how third party apps would use their data³⁸⁷. Afterwards, in February 2012 he had a meeting with two staff members of Facebook in Vienna, where he expressed his concerns on privacy policies of the

³⁸¹European Union, European Commission, Joinup, the ISA program: e-Government in Denmark, 2015, p 21.

³⁸²<https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544>

³⁸³<https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544>

³⁸⁴<https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544>

³⁸⁵Facebook's Headquarters in EU are located in Ireland.

³⁸⁶<https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544>

³⁸⁷<https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544>

firm, but they dealt with him with general and abstract arguments³⁸⁸. One year and four months after this meeting, Edward Snowden leaked to the press detailed PowerPoints with various mass surveillance programs of US' federal agencies. One of them, PRISM program, had under the umbrella of its operations many technology giant companies, including Facebook. Among many things, Edward Snowden revealed that Facebook's users' data were harvested by NSA for mass surveillance issues, even if Facebook had signed and was a participant of the Safe Harbor Decision, which at that time was the agreed legal framework for the protection of data transfers and personal data protection between EU and USA, under the legal obligations of Data Protection Directive³⁸⁹.

The leaks of E.Snowden gave the opportunity to Max Shrems to come back to the Irish Commissioner and file another complaint against Facebook Ireland Ltd in the same month of the revelations. However, the Commissioner of Ireland stated that the complaint was "frivolous and vexatious" and rejected it, stating that it had no duty to investigate this case further³⁹⁰. After that, M.Schrems filled in an application for judicial review in the Irish High Court over the inaction by the Irish DPC, which was granted³⁹¹. In contrast to the opinion of the Irish Commissioner, the High Court of Ireland stated that even if Schrems was not able to make available, to the Court, evidence of his own personal data being used in the ways he alleged, it was not required for him to be able to prove his own data being subject of surveillance, given the evidence of such happenings on a mass scale³⁹². Furthermore, the High Court addressed a set of questions to the CJEU based on Article 267 of the Treaty on the Functioning of the EU (TFEU)³⁹³. The request for a preliminary ruling, based on Article 267 TFEU, was with regard to the validity of the Commission's Decision 200/520/EC (Safe Harbor Decision) and the interpretation of Articles 25(6) and 28 of the DPD 95/46/EU in the light of Articles 7, 8 and 47 of the EU Charter of Fundamental Rights³⁹⁴. Also, the High Court of Ireland questioned the power of national supervisory authorities, seeing that the DPC was of the view that the complaint of M.Schrems lacked of evidence, that he was not required to investigate

³⁸⁸ <https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544>

³⁸⁹ <https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544>

³⁹⁰ <https://www.rte.ie/news/2013/0726/464770-data-protection/>

³⁹¹ <https://www.telegraph.co.uk/technology/facebook/10401419/Facebook-PRISM-decision-to-be-reviewed-by-Irish-High-Court.html>

³⁹² High Court of Ireland, Maximillian Schrems v. Data Protection Commissioner (2013 No. 725JR), par. 74-75.

³⁹³ <http://curia.europa.eu/juris/document/document.jsf?jsessionid=ECA5CABC7309F5635838FDABA24DAD49?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3335726>

³⁹⁴ <http://curia.europa.eu/juris/document/document.jsf?jsessionid=ECA5CABC7309F5635838FDABA24DAD49?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3335726>

further and because the Safe Harbor Decision determined the adequacy requirements of data transfers³⁹⁵.

On October 6, 2015, the CJEU came to the conclusion that national supervisory authorities have the capacity to examine individuals' claims which could dare the compatibility of the Commission's adequacy levels of protection, as read from the perspective of Article 28 of the Directive 95/46/EU in the light of Article 8 of the EU Charter³⁹⁶. So, the CJEU ruled that national supervisory authorities have the ability and possibility to examine claims such as this one. In addition, CJEU made Articles 1 and 3 of the Safe Harbor Decision invalid, because they could not be complied with Article 25(6) of the DPD and since these articles could not be separated from the Safe Harbor Decision, the whole decision was rendered invalid³⁹⁷.

The Safe Harbor mechanism was a creation between the US Department of Commerce and the European Commission, in order to address the protection of privacy of EU citizens for data transfers between USA and EU. It was also, a decision that did not only provided the required legal basis for the protection of individuals' privacy but moreover, it was a decision that was established for the purpose of collection and use of economic advantages, agreed upon statutory framework, of data transfers. But, the Safe Harbor mechanism had many flaws on providing guarantees for supporting the adequate level of protection on privacy issues³⁹⁸. This is the main reason for its invalidation by the CJEU. Following this decision, the US and EU authorities started negotiating another agreement upon adequacy level of protection for transatlantic data transfers. The consequence was the so called "EU-US Privacy Shield", which was announced on February 2, 2016³⁹⁹, released on February 29, 2016⁴⁰⁰ and on July 12, 2016, the EC deemed the EU-US Privacy Shield Framework adequate to enable data transfers under EU law⁴⁰¹. The press release of the Privacy Shield was followed by President Obama's signing of the Judicial Redress Act, which empowers EU citizens to enforce their data protection rights to the US courts⁴⁰². The

³⁹⁵ <http://curia.europa.eu/juris/document/document.jsf?jsessionid=ECA5CABC7309F5635838FDABA24DAD49?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3335726>

³⁹⁶ <http://curia.europa.eu/juris/document/document.jsf?jsessionid=ECA5CABC7309F5635838FDABA24DAD49?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3335726>

³⁹⁷ <http://curia.europa.eu/juris/document/document.jsf?jsessionid=ECA5CABC7309F5635838FDABA24DAD49?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3335726>

³⁹⁸ Maximillian Schrems v. Data Protection Commissioner, C- 362/14, Opinion of Advocate General, par. 134-138, 141-144, 161-168.

³⁹⁹ <https://www.reuters.com/article/us-eu-dataprotection-usa-accord-idUSKCN0VB1RN>

⁴⁰⁰ <https://iapp.org/resources/article/eu-u-s-privacy-shield-full-text/>

⁴⁰¹ <https://www.privacyshield.gov/program-overview>

⁴⁰² <https://www.congress.gov/bill/114th-congress/house-bill/1428/all-info>

Privacy Shield is intended to be a mechanism of transparency, reliability and accountability for data transfers between USA and EU with the goal to enhance data protection under its context and the context of GDPR.

The Article 29 Data Protection Working Party⁴⁰³, in its first annual joint review on EU-US Privacy Shield, expressed its concerns on issues, such as the commercial aspects of the Privacy Shield and on the derogations of the Privacy Shield to allow access to data for Law Enforcement and National Security purposes⁴⁰⁴, but also recognized the progress of the Privacy Shield in comparison to the Safe Harbor Decision⁴⁰⁵.

Maximillian Schrems's case study, proved that laws and policies on data protection and privacy, which are abetting sectors of data governance, are not a one-way deal but they are evolving in accordance to the technology improvements and to the views of governments, enterprises and individuals on how data should be governed and what standards should be applied to the procedures of legal and technological environment of the 21th century. Furthermore, it addressed that basic principles of DG, such as integrity, transparency, accountability and standardization, should be taken in consideration not only with the existing laws but in addition to the establishment of new legislations and policies for better understanding and applicability of an environment which evolves and is becoming crucial to the development of our technological-based societies. Finally, it demonstrates the fact that the power of individual rights can be protected and enhanced if individuals have the will to pursue the development of a society, where balance between corporates' interests, social integrity and legal respect and prosperity, in general, are at the center of every legal debate.

5.2 “THIS IS YOUR DIGITAL LIFE” CASE STUDY

In 2007, two doctoral candidates, Michal Kosinski and David Stillwell, from Cambridge University, developed an app questionnaire (myPersonality), through Facebook, which allowed them, to study personality characteristics of those who took the questionnaire, in comparison with their data (likes, shares, posts, gender, age etc.) from the social media's platform⁴⁰⁶.

This study was based on the OCEAN model, which was developed in the 1980s by psychologists, in order to evaluate human beings based on five personality traits (openness, conscientiousness, extroversion, agreeableness and neuroticism), known also as the “Big Five”⁴⁰⁷. The users, who took the questionnaire, received a personality profile based on the evaluation of the OCEAN model, but also had the

⁴⁰³The Art.29 WP was an advisory body made up of representatives from the data protection authorities of each EU Member State and on 25 May 2018 was replaced by the European Data Protection Board (EDPB) under the GDPR.

⁴⁰⁴Article 29 Data Protection Working Party: EU-US Privacy Shield- First Annual Joint Review, 28 November 2017.

⁴⁰⁵Article 29 Data Protection Working Party: EU-US Privacy Shield- First Annual Joint Review, 28 November 2017, p 20.

⁴⁰⁶<https://www.rollingstone.com/culture/culture-news/cambridge-analytica-what-we-know-about-the-facebook-data-scandal-202308/>

⁴⁰⁷https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

ability to opt-in, to share their Facebook data with the researchers⁴⁰⁸. The correspondence of users, who took the questionnaire, was far from the expectations of these two researchers and it offered them one enormous dataset, which combined psychographics (psychometric scores) with Facebook profiles⁴⁰⁹. Five years after this initiative (2012), Michal Kosinski proved, among other things, that, on the basis of an average of 68 Facebook likes by a user, it was possible to predict the color of their skin (with 95% accuracy), their sexual orientation (with 88% accuracy) and even their affiliation to the Republican or Democratic Party (with 85% accuracy)⁴¹⁰. Other personality traits of a user, like intelligence, religious beliefs, alcohol and drug use, could also be determined with this method⁴¹¹. In 2013, the two scientists published their findings of the study in the Proceedings of the National Academy of Sciences⁴¹² and a few weeks later, Facebook changed its policies around “likes” to private by default⁴¹³.

In the meantime, Facebook has enabled third party app-developers to have access, after user’s consent, in a few private data of a user since May 2007⁴¹⁴, with Facebook’s Developer Platform⁴¹⁵ and in 2010, it announced the launch of Open Graph⁴¹⁶. In its announcement, Facebook’s CEO, Mark Zuckerberg called this change as the most transformative thing they had ever done for the web⁴¹⁷ and according to Facebook, this platform would create an easier environment for the users to share information from all over the internet and that their data could be found on Facebook.com and other sites⁴¹⁸. Beside these updates, the first version of Open Graph API (Application Programming Interface) gave the permission to third party

⁴⁰⁸, https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

⁴⁰⁹ https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

⁴¹⁰, https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

⁴¹¹ https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

⁴¹² <https://www.rollingstone.com/culture/culture-news/cambridge-analytica-what-we-know-about-the-facebook-data-scandal-202308/>

⁴¹³, https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

⁴¹⁴ <https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/>

⁴¹⁵ https://mashable.com/2012/05/24/facebook-developer-platform-infographic/?europa=true#xihAoB_B.ZqF

⁴¹⁶, <http://edition.cnn.com/2010/TECH/04/21/facebook.changes.f8/index.html>

⁴¹⁷ <http://edition.cnn.com/2010/TECH/04/21/facebook.changes.f8/index.html>

⁴¹⁸ <http://edition.cnn.com/2010/TECH/04/21/facebook.changes.f8/index.html>

app-developers to request access from Facebook users' to their personal data and to access their Facebook friends' personal data as well⁴¹⁹. With a user's permission, these applications could had access to many personal data such as⁴²⁰: a user's name, location, education, political preferences, religious views, gender, online status etc. Also, with additional permissions, external developers could gain access to private messages of a user⁴²¹. After the announcement of Open Graph, concerns around people's protection of privacy were expressed because of the integration of Facebook with other web sites⁴²².

Moreover, Facebook came to a settlement, in 2011, with the US Federal Trade Commission (FTC) for privacy complaints against the social network. The subject of these complaints, which were filed by the Electronic Privacy Information Center and a coalition of consumer groups, were Facebook's practices on privacy matters⁴²³. The FTC charged the social network "that it deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public"⁴²⁴. According to the order of the FTC, Facebook allowed to advertisers to gather personal information of users with outside application developers in contrast to what it promised to its users⁴²⁵. The settlement for "unfair and deceptive" practices on privacy required the company to respect the privacy desires of its users before it changed the way it shared their data, but also to acquire periodic evaluation of its privacy practices by independent auditors for the next 20 years⁴²⁶. The FTC did not levy Facebook with fines, neither did it accuse it of breaking the law on purpose but it ordered that if Facebook violated this settlement in the future, would have to pay a penalty of 16.000 US dollars per day for each violation⁴²⁷.

⁴¹⁹ <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>

⁴²⁰ <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>

⁴²¹ <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>

⁴²² <http://edition.cnn.com/2010/TECH/04/21/facebook.changes.f8/index.html>

⁴²³ <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>

⁴²⁴ <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>

⁴²⁵ <https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html>

⁴²⁶ <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>

⁴²⁷ <https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html>

Three years after this decision, another Cambridge based academic, Alexander Kogan, created a, similar to Kosinski's and Stillwell's., app, the so called "this is your digital life". Using the tools that Facebook provided at that time, A.Kogan harvested the data, of those who took his psychographic questionnaire (almost 300.000 users) and gave their consent to mine their Facebook's data but also took the data of the users' friends on Facebook. This kind of access to data of outside developers was known and allowed by Facebook through its policies and terms of service, at that time. However, what was not allowed to third party developers, was to transfer or sell Facebook's data (including anonymous, aggregate or derived data) to ad networks, data brokers or other advertising or monetization-related service⁴²⁸. The same year that A.Kogan created his psychographic questionnaire, Facebook changed its developer application programming interface (API) by restricting the access of a third party developer to a user's friends' data without obtaining permission in first place⁴²⁹.

Meanwhile, in 2013, Strategic Communication Laboratories Group (SCL), a UK based company, founded in 1993 as a political advertising agency⁴³⁰ and worked for governments, politicians and militaries, founded Cambridge Analytica, a shell company with a license to psychographics⁴³¹. This political consulting firm had based its strategic operations on the investments of a wealthy Republican donor, Robert Mercer, the connections of Stephen Bannon⁴³² and the ideas of Christopher Wylie, a Canadian data scientist, who had studied at London School of Economics and at that time was studying for a PhD in fashion forecasting⁴³³.

Cristopher Wylie read the paper of M.Kosinski and D.Stillwellby chance and tried to apply it to Liberal Democrats (UK) at first⁴³⁴. However, they didn't want to base their elections' strategy on the model that was presented to them by C.Wylie and after that, a Liberal Democrat connection introduced Wylie to SCL Group and to its subsidiary, SCL Elections, which was run by Alexander Nix (CEO)⁴³⁵. C.Wylie

⁴²⁸, <https://www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data>

⁴²⁹ <https://www.cnn.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>

⁴³⁰, <https://www.forbes.com/sites/courtstroud/2018/04/30/cambridge-analytica-the-turning-point-in-the-crisis-about-big-data/#516c99e448ec>

⁴³¹ <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

⁴³²Who is an American media executive, political figure, former investment banker, former executive chairman of Breitbart News, later advisor to Trump campaign and recently former chief strategist in the White House, in the administration of President Donald Trump.

⁴³³, <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

⁴³⁴, <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

⁴³⁵, <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

became an employee of A.Nix and A.Nix met Steve Bannon by chance⁴³⁶. In autumn 2013, Steve Bannon met C.Wylie and the former was fascinated by the idea of using personality traits to target voters⁴³⁷. He transferred the idea to Robert Mercer and his daughter Rebekah, who later became a board member of Cambridge Analytica. The two of them were interested, but they wanted actual results in order to invest in this firm⁴³⁸. But in order to produce results using psychographic traits on a national scale, for elections, Cambridge Analytica needed data that they could not get without enormous expense⁴³⁹. In the first place, C.Wylie's company addressed to Cambridge University Psychometrics Centre and especially to M.Kosinski but their relation did not work out and after that A.Kogan offered to produce the data that Cambridge Analytica was in need for. An executed contract, dated back in 2014, which was provided to the press by C.Wylie, proved that the parent company, SCL Group, came to a commercial agreement with the company which was founded by A.Kogan, Global Science Research (GSR)⁴⁴⁰. A.Kogan harvested the data of more than 80 million Facebook users between June and August 2014 and then sold the data, through GSR, to Cambridge Analytica for 1 million US dollars⁴⁴¹.

This action was against Facebook's terms of use and UK's data protection laws, which prohibit the sale or use of personal data to third party without consent of the users⁴⁴². According to C.Wylie, who later became a whistleblower to the case, "Facebook could see it was happening. Their security protocols were triggered because Kogan's apps were pulling this enormous amount of data, but apparently Kogan told them it was for academic use. So there were like 'Fine' "⁴⁴³. According to A.Kogan, his app had, as one of the terms of service, the possibility to sell or transfer data, which was against Facebook's terms of use, but no one from Facebook did anything to prevent this action⁴⁴⁴.

In December 2015, a report from the Guardian claimed that Cambridge Analytica had acquired Facebook's data and used them to support Ted Cruz in his

⁴³⁶ <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

⁴³⁷ <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

⁴³⁸ <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

⁴³⁹ <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

⁴⁴⁰ <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

⁴⁴¹ <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

⁴⁴² https://www.washingtonpost.com/business/understanding-the-facebook-cambridge-analytica-story-quicktake/2018/04/11/071f8c84-3d97-11e8-955b-7d2e19b79966_story.html?utm_term=.280c3b5bddeb

⁴⁴³ <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

⁴⁴⁴ <https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook/>

presidency campaign⁴⁴⁵. After the publication of this report, the social network stated that it was investigating the situation carefully and removed A.Kogan's app from its website⁴⁴⁶. In the meantime, Senator Ted Cruz had lost Republicans' confirmation to become a US President and Cambridge Analytica turned to Donald Trump in order to help him become the 45th President of USA⁴⁴⁷. Cambridge Analytica was paid nearly 6 million US dollars for its operations and services from the Trump campaign and the first payment to the company was on July 29, 2016, according to Federal Election Commission records⁴⁴⁸. According to C.Wylie's revelations, the data which were sold from A.Kogan to Cambridge Analytica were later used to target voters on the Trump campaign⁴⁴⁹. Also, according to former officials of the Trump campaign, Cambridge Analytica helped them with target advertising of voters based on psychographic traits mixed with other sources (voter records, demographic data)⁴⁵⁰. In this way, Cambridge Analytica helped them create a strategic map of voters for the campaign. Furthermore, according to an internal document of the company, which was obtained by the Guardian, Cambridge Analytica used Google, Snapchat, Facebook, Twitter and YouTube to impose intensive survey research, data modelling and performance-optimizing algorithms through 10.000 different advertisements, which were viewed billions of times⁴⁵¹. Besides that, an article on Campaign, a magazine for the marketing and advertising industries, in February 2016, revealed that Cambridge Analytica was teamed up with Nigel Farage's Leave EU campaign, which was a Brexit campaign group⁴⁵² and later in 2018, the whist blower C.Wylie revealed, to British members of the Parliament, that EU Brexit was won through fraud and that Cambridge Analytica worked on shifting the results of UK's referendum⁴⁵³.

⁴⁴⁵<https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>

⁴⁴⁶<https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

⁴⁴⁷<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

⁴⁴⁸<https://www.foxnews.com/politics/cambridge-analytica-reached-out-to-wikileaks-about-clinton-emails-ceo-says>

⁴⁴⁹<https://www.cnn.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html>

⁴⁵⁰<https://www.rollingstone.com/culture/culture-news/cambridge-analytica-what-we-know-about-the-facebook-data-scandal-202308/>

⁴⁵¹<https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory>

⁴⁵²<https://www.independent.co.uk/news/uk/home-news/cambridge-analytica-alexander-nix-christopher-wylie-trump-brexit-election-who-data-white-house-a8267591.html>

⁴⁵³<https://www.theguardian.com/uk-news/2018/mar/27/brexit-groups-had-common-plan-to-avoid-election-spending-laws-says-wylie>

The Facebook-Cambridge Analytica scandal finally erupted after reports on New York Times, The Guardian and The Observer in March 2018. With the revelations of the former employee of Cambridge Analytica, C.Wylie, who had left the company in 2014, and the reports of major news organizations, Cambridge Analytica and Facebook came under the microscope of EU and US authorities concerning their role in major-shifting political events such as Trump's election and Brexit. Politicians and regulators across the two sides of the Atlantic Ocean demanded answers from the two companies. Facebook's CEO, Mark Zuckerberg testified to US Congress in April 2018 and to EU representatives of the EU Parliament in May 2018 about the role of his company to the scandal.

The first publishes in mid-March exposed how Cambridge Analytica used the harvested data of 50 million Facebook users to implement its operational strategies but the numbers of the users who gave unwillingly their personal data was revised later from Facebook to 87 million users⁴⁵⁴. In addition to that, Facebook admitted publicly for the first time, even if the story had already started with the report of Harry Davies in December 2015, that when it learned about Kogan's app, in 2015, it demanded and received certification that the data had been destroyed⁴⁵⁵. According to C.Wylie, Facebook's lawyers communicated with him about the illegal harvested data in August 2016⁴⁵⁶. Moreover, Cambridge Analytica officials at first denied that they had obtained or used Facebook's data and later in a statement to The Times admitted that they took the data but they blamed A.Kogan for the violation of Facebook policies⁴⁵⁷ and claimed that they deleted them in cooperation with Facebook in 2015⁴⁵⁸.

From its side, the social network also admitted publicly for the first time that Cambridge Analytica had collected millions of Facebook users' data without their consent and against the policies of it and suspended C.Wylie, Cambridge Analytica and A.Kogan from its website⁴⁵⁹. On April 4, 2018, Facebook's CTO, Mike Schroepfer admitted that the number of "infected" profiles was much higher than previously believed and it reached up to 87 million users and Mark Zuckerberg portrayed this breach as a breach of trust between Kogan, Cambridge Analytica and Facebook and as a breach of trust between Facebook and its users⁴⁶⁰. In addition, he

⁴⁵⁴ <https://www.cnn.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>

⁴⁵⁵ <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

⁴⁵⁶ <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump>

⁴⁵⁷ <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

⁴⁵⁸ <https://www.independent.co.uk/news/uk/home-news/cambridge-analytica-alexander-nix-christopher-wylie-trump-brexit-election-who-data-white-house-a8267591.html>

⁴⁵⁹ <http://time.com/5205314/facebook-cambridge-analytica-breach/>

⁴⁶⁰ <http://time.com/5205314/facebook-cambridge-analytica-breach/>

announced new restrictions to third party developers' access to Facebook users' data and audits for all apps with access to vast amount of data before 2014. Also, Facebook's Chief Operating Officer Sheryl Sandberg announced that Facebook will ban developers who misused or misuse personal data⁴⁶¹. Furthermore, Facebook started to notify its users if their data were shared with Cambridge Analytica, since April 9, 2018, 3 years after it stated the fact that it learned about the leak and four after it actually happened⁴⁶².

In the meantime, and after the reports on newspapers, the FTC opened an investigation into whether Facebook violated the settlement, over users' privacy protection, that occurred in 2011⁴⁶³ and according to former FTC officials (Jessica Rish and David Vladek) Facebook could be found guilty that violated the 2011 settlement under the Cambridge Analytica scandal⁴⁶⁴. Also, the special counsel of US Department of Justice, Robert Mueller, who is investigating the Russian interference in 2016 US elections, in which Facebook is also linked as it was used by Russian hackers to influence the Presidential elections⁴⁶⁵, demanded the emails of Cambridge Analytica employees who worked for the Trump campaign⁴⁶⁶. According to his investigations, the Russian interference started back in 2014 and it used the power of US social media, including Facebook⁴⁶⁷.

In May 2018, Cambridge Analytica filed for bankruptcy under Chapter 7 of bankruptcy protection in the US⁴⁶⁸ and after this announcement, UK's data protection regulator claimed that it will continue civil and criminal investigations of the firm and of its employees and directors⁴⁶⁹. In July 2018, a British MP, Damian Collins told to CNN, that the harvested data of Cambridge Analytica scandal were accessed in Russia and the UK's data protection office (ICO) confirmed later that it had proofs of

⁴⁶¹<http://time.com/5205314/facebook-cambridge-analytica-breach/>

⁴⁶²<https://www.cnn.com/2018/04/26/facebook-cto-admits-firm-didnt-read-terms-of-aleksandr-kogans-app.html>

⁴⁶³<https://www.cnn.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>

⁴⁶⁴<http://fortune.com/2018/03/29/cambridge-analytica-facebook-scandal/>

⁴⁶⁵<http://fortune.com/2018/03/29/cambridge-analytica-facebook-scandal/>

⁴⁶⁶<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

⁴⁶⁷<https://www.theguardian.com/uk-news/2018/mar/27/brexit-groups-had-common-plan-to-avoid-election-spending-laws-says-wylie>

⁴⁶⁸<https://variety.com/2018/digital/news/cambridge-analytica-bankruptcy-facebook-1202815370/>

⁴⁶⁹<https://www.reuters.com/article/us-facebook-privacy/cambridge-analytica-and-british-parent-shut-down-after-facebook-scandal-idUSKBN1I32L7>

this access from Russians⁴⁷⁰. According to an email dated back in July 17, 2014, which was sent from A.Nix (former CEO of Cambridge Analytica) to C.Wylie, Cambridge Analytica had to make a memo about its services to a Russian oil and gas company, Lukoil⁴⁷¹. Also, in that email A.Nix explained that “they understand behavioral micro targeting in the context of elections” but they were unable to connect this approach with the consumers of their company, referring to Lukoil⁴⁷². Finally, he mentioned that their work will be shared to the CEO of Lukoil, VagitAlekperov, a former Soviet oil minister and associate of President Putin⁴⁷³. But, still there is no, public provided, evidence that Cambridge Analytica worked with or for Lukoil or even that it gave Facebook’s data to the Russians. The documents of C.Wylie show that a giant Russian company was informed on micro targeting, Facebook and election disturbance back in 2014⁴⁷⁴.

While the investigations on Facebook-Cambridge Analytica scandal keep going on and UK’s data protection office fined Facebook with a 660.000 US dollars fine for its involvement to the Cambridge Analytica’s harvesting of data⁴⁷⁵, an enormous data breach, the biggest of Facebook’s history, occurred in September 2018. At least 30 million accounts have been affected from this hack, which allowed to hackers to access personal information of the users including names, relationship status, religion, workplaces, birthdate, search history, location check-ins and even private messages⁽⁴⁷⁶⁾⁽⁴⁷⁷⁾. According to the reports, Facebook’s engineers found an unusual activity on the social media platform’s networks in mid-September and it

⁴⁷⁰<https://www.businessinsider.com/cambridge-analytica-facebook-data-accessed-in-russia-2018-7>

⁴⁷¹<https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

⁴⁷²<https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

⁴⁷³<https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

⁴⁷⁴<https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

⁴⁷⁵<https://www.forbes.com/sites/thomasbrewster/2018/07/11/facebooks-ico-fine-is-tiny-but-what-of-its-reputation/#51ec60725519>

⁴⁷⁶<https://edition.cnn.com/2018/10/04/tech/facebook-hack-explainer/index.html>

⁴⁷⁷<https://www.theguardian.com/technology/2018/oct/12/facebook-data-breach-personal-information-hackers>

took them 11 days to stop it⁴⁷⁸. The attackers used three separate vulnerabilities in Facebook's code in order to penetrate into the system and extracted private information from users⁴⁷⁹. According to Facebook, the vulnerabilities to its code had existed since July 2017⁴⁸⁰.

This breach was not characterized as a breach of trust, like it happened with the data that were harvested illicitly by A.Kogan and then sold to SCL Group and Cambridge Analytica. This one, by definition an actual data breach, the biggest one so far, for the social media giant. According to US Department of Health and Human Services "a data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so"⁴⁸¹. Also ISO/IEC 27040 defines a data breach as "a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed"⁴⁸².

After the eruption of this political and technological scandal in mid-March 2018, Facebook's CEO Mark Zuckerberg broke his silence four days after the first publishes in New York Times, the Observer and the Guardian⁴⁸³ and he characterized this breach as breach of trust between his company, A.Kogan and Cambridge Analytica but also as a breach of trust between Facebook and its users⁴⁸⁴. But statements from persons such as Sandy Parakilas, who had worked on Facebook as a platform operations manager (specializing in third party advertising, privacy and policy compliance) and Mike Schoepfer, who is the current CTO lead to the conclusion that Cambridge Analytica scandal, it was more than a breach of trust. Mike Schoepfer said to UK legislators at a parliamentary committee hearing, that they - meaning Facebook Inc. - did not read all of the terms and conditions and also mentioned that Facebook did not notify UK's data protection authority (ICO) after it had learned about the sharing of data with Cambridge Analytica⁴⁸⁵, while Sandy

⁴⁷⁸<https://edition.cnn.com/2018/10/04/tech/facebook-hack-explainer/index.html>

⁴⁷⁹<https://edition.cnn.com/2018/10/04/tech/facebook-hack-explainer/index.html>

⁴⁸⁰<https://edition.cnn.com/2018/10/04/tech/facebook-hack-explainer/index.html>

⁴⁸¹<https://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf>

⁴⁸²https://en.wikipedia.org/wiki/Data_breach

⁴⁸³<https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>

⁴⁸⁴<http://time.com/5205314/facebook-cambridge-analytica-breach/>

⁴⁸⁵<https://www.cnbc.com/2018/04/26/facebook-cto-admits-firm-didnt-read-terms-of-aleksandr-kogans-app.html>

Parakilas stated to an interview to Lesley Stahl, and i quote⁴⁸⁶: “Well they didn’t want to know in the sense that if they didn’t know, then they could say they didn’t know and they weren’t liable, where as if they knew they would actually have to do something about it. And one of the things that I was concerned about, was that applications or developers of applications would receive all of this Facebook data, and that once they received it, there was no insight, Facebook had no control or view over what they were doing with the data”. Also, he mentioned that once the data left Facebook, the social network had no way to find what happened to the data⁴⁸⁷.

Furthermore, two days after the breakup of the first stories in the press about Facebook-Cambridge Analytica scandal, the New York Times revealed that the Chief Security Officer of Facebook was stepping down after disagreements with the leadership of the social media giant about how Facebook should be more transparent on Russia’s use of the social network to spread disinformation during the period of US 2016 elections⁴⁸⁸. The day that this report was published, Facebook lost 37 billion US dollars in market cap during one day of trading⁴⁸⁹.

Currently, Facebook’s market value is estimated in 415 billion US dollars. It is a technological giant, which has established its value as a social media “godfather” and has built the foundations for fast and interactive communication in the dawn of a digital society. But, the statements and actions of former and current executives of Facebook prove otherwise, as they take actions on the social network concerning the handling of Cambridge Analytica scandal and of the last data breach. According to Sinan Aral, a professor at MIT, Facebook faces a “transparency paradox” because of the need to be more transparent and at the same time to increase the security of its data⁴⁹⁰. Facebook is a technological giant in crisis because of its complexity of operations and its connection and integration with other sectors of human activity (third party developers, data brokers, advertisers etc.) that provide more than communication between people. At first, that was the original purpose of the social network, but it is logical for such a network to provide more. It is criticized, among other allegations that it violates humans’ privacy, that it is a tool for political manipulation and that it isolates people more than it connects them.

Recently, in December 2018, new allegations about the privacy and general policies around the governance of data of the social network came into light from the press and British lawmakers. While, Facebook is under investigation from the Department of Justice, the Securities and Exchange Commission and the Federal

⁴⁸⁶<https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook/>

⁴⁸⁷<https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook/>

⁴⁸⁸<https://www.nytimes.com/2018/03/19/technology/facebook-alex-stamos.html>

⁴⁸⁹<https://www.technologyreview.com/s/610577/the-cambridge-analytica-affair-reveals-facebooks-transparency-paradox/>

⁴⁹⁰<https://www.technologyreview.com/s/610577/the-cambridge-analytica-affair-reveals-facebooks-transparency-paradox/>

Trade Commission about its involvement in the data-scandal of Cambridge Analytica⁴⁹¹, the British lawmakers gave 250 pages of internal emails between executives and employees of Facebook to the public⁴⁹². In these pages the ambitions of Facebook's executives are revealed, concerning the collection of more data from users, extraction of privileges from developers and eradication of possible competitors⁴⁹³.

Following this revelation, the New York Times revealed some of the data-sharing practices of the company with others, such as⁴⁹⁴: Amazon, Netflix, Spotify, Yahoo, Microsoft, Sony, the Royal Bank of Canada, Huawei and even a Russian search company called Yandex. These internal documents of Facebook's data-sharing practices with other companies reveal special arrangements, through which, every part had benefits. In some cases, Facebook allowed to other enterprises to see names of all Facebook users' friends without consent (Microsoft's Bing search engine) and to acquire users' names and contact information through their friends (Amazon), while in other cases Facebook even allowed to companies and even a bank to have access on Facebook's users' private messages (Netflix, Spotify, the Royal Bank of Canada)⁴⁹⁵. Some of these deals are located back to 2010 and according to the revelations, all had been still in active mode since 2017. More than 150 enterprises including tech companies, entertainment websites, automakers, online stores and media corporations were benefited from these special agreements with Facebook, gaining hundreds of millions of Facebook's users' data monthly⁴⁹⁶. In exchange, Facebook got more users, increasing its advertising revenue and powering up its growth as a worldwide enterprise⁴⁹⁷. According to the social network, the most of these partnerships are under an exemption to the consent decree agreement with the FTC, dated back in 2011, because these partner-companies are service providers, which use the data of Facebook "for and at the direction" of it⁴⁹⁸. Facebook characterizes these partner-companies as integration partners which serve as an extension of it and which are reviewed by Facebook, according to its arguments⁴⁹⁹.

⁴⁹¹<https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

⁴⁹²<https://www.nytimes.com/2018/12/05/technology/facebook-emails-privacy-data.html>

⁴⁹³<https://www.nytimes.com/2018/12/05/technology/facebook-emails-privacy-data.html>

⁴⁹⁴<https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

⁴⁹⁵<https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

⁴⁹⁶<https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

⁴⁹⁷<https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

⁴⁹⁸<https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

⁴⁹⁹<https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

Finally, during the same month (December 2018), Privacy International⁵⁰⁰ published a research which showed that more than 20 Android apps shared users' data with Facebook, without the consent of the users, and even did the same with those who do not have a Facebook account⁵⁰¹. The names of prestigious and worldwide known companies were included among those apps, such as⁵⁰² : Spotify, Shazam, Skyscanner, Yelp and Kayak.

But even if all these allegations proved to be true, still Facebook could and should help to the social, environmental, technological and economic evolution and salvation of this planet. If data is translated to power, then Facebook is a perfect tool that has the ability to contribute to a better future for humanity and this is the reason why it is in need of a stronger data governance model. A model that will provide transparency for its operations and for the operations of others on Facebook, liability and accountability for its executives and leadership, solid stewardship and most of all integrity for its 2 billion users worldwide. The scandals and allegations around the privacy policies of the social network which occurred in 2018 prove that Facebook is in need of a restructured or new data governance model. This is necessary not only for lifting its market value but more importantly for its reestablishment as an enterprise that provides truly transparent democratic procedures, ideas and values for its users, but also for the world's growth and prosperity in general.

6. CONCLUSION

In the beginning of the 21th century the word “data” and the use of it, was spread only among a small number of states, international organizations and private corporations. Before the dawn of the new millennium and the “technological revolution” that we live today, EU had been the first body with legislative, executive and judicial power, on international scale, which had developed and implemented legislation around the sector of protection of data and privacy with the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Moreover, the European Union had developed and is still developing coherent policies and legislation on how data could be used in order to offer prosperity, welfare and economic boost to its residents and corporations, private or public. Strategies such as the Digital Agenda for Europe, the Digital Single Market Strategy, the e-Government Action Plan 2016-2020, the Horizon 2020, the Open Science Cloud, the Urban Agenda and European Smart Cities initiative, are some of the various strategies and policies that EU is developing and

⁵⁰⁰Privacy International is a UK-based charity that promotes the right to privacy at an international level.

⁵⁰¹<https://channels.theinnovationenterprise.com/articles/facebook-used-more-than-20-android-apps-data-without-user-consent>

⁵⁰²<https://www.lawspot.gr/nomika-nea/pos-oi-efarmoges-sto-android-moirazontai-dedomena-me-facebook-akoma-kai-den-ehete>

implementing in order to offer a consistent and prosperous future for the industrial, economic, social, technological and geopolitical growth of its operations and for the protection of the life of its residents. Furthermore, legislative innovations such as the GDPR (Regulation 2016/679) and the anticipated, in 2019, e-Privacy Regulation are giving to EU the opportunity to be an important regulator in an international scale, concerning the topic of how data should be governed by governments, international institutions and private corporations. Additionally, these legislations and policies are also promoting a future where respect on the right of privacy and data protection of the subjects, are at the center of every dispute either in judicial, executive or legislative level. Paradigms like the Maximillian Schrems's case and the Cambridge Analytica scandal and their outcomes, show that EU is thinking and acting as an entity that firstly seeks for the human flourishing and prosperity and secondly considers the consequences of its activities as a judicial, executive and legislative body. Also, the institutionalization of the right of privacy and the right of data protection as separate and fundamental rights in the Charter of Fundamental Rights of EU demonstrate the willingness of the EU to operate as an entity which tries to balance individuals' interests with corporates' and governmental ones in order to adjust to a digitized world where data collection, use and storage are necessities for the development, establishment, growth and conservation of every political, economic and corporate system.

On the contrary, the United States of America and the People's Republic of China are functioning in a more government and corporate centric structure in order to establish policies and legislation on the sector of data governance. The first one has established many sector-based laws around data protection, privacy and data governance. The Federal Privacy Act (1974), the Federal Trade Commission Act, the Gramm-Leach-Bliley Act (GLBA), the Fair and Accurate Credit Transactions Act, the Health Information Technology for Economic and Clinical Health Act (HITECH), the Cybersecurity Information Sharing Act (CISA), the Digital Accountability and Transparency Act (DATA Act) and The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) are some of the many laws that the USA have established in federal level. Many states have also established laws on this topic, such as California's Consumer Privacy Act, which is a GDPR-like regulation and all of them have passed data breach notification legislations. Moreover, the policies that were promoted by the Obama Administration (the Digital Government Strategy, the Open Government Directive, the Open Government Partnership, etc.) and the last one, the Trump Administration (the Federal Data Strategy), show that the US Federal government considers data as an asset with strategic importance for its operations and well-being. But the cases of Cambridge Analytica scandal, the Yahoo data breaches⁵⁰³ and the Equifax data breach⁵⁰⁴ are the proper examples which can show that the USA are in need of a new model on the sector of DG. The "Corporate-America" has to be controlled with stricter laws that will provide coherent and clear policies, with respect to its citizens' life and protection, in a federal level, in order to avoid situations like these or worse than these, in the future. As for the People's Republic of China the situation is not much more different. Through its policies (National Cyberspace

⁵⁰³ <https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html>

⁵⁰⁴ <https://www.ftc.gov/equifax-data-breach>

Strategy, International Strategy for Cooperation in Cyberspace, 13th Five-Year Plan for Information, 13th Five-Year Plan for Major Science and Technology Projects, the Next Generation Artificial Intelligence Development Plan, Healthy China 2030, the Social Credit System, etc.) and laws (the National Security Law, the Counter-Terrorism Law and the Cyber Security Law, the Consumer Rights Protection Law, the Tort Liability Law, etc.), China is trying to change its brand name to a country that will lead the world in the following decades, not only economically but also technologically. To do so, China is using data and technologies of data science at the center of its strategies. Controversial projects such as the Social Credit System reflect the ambitions and willingness of China's leadership to change the way the world sees China but also reveal possible menaces to the foundations of democratic values and ideas, like the right of the individuals to privacy, the right of people to integrity and freedom of expression, which the western civilization is built on.

Last but not least, countries such as Japan and South Korea prove that even if they are geographically located in the east, their way of thinking and acting in governmental and enterprise level is moving closer towards the west. Those two nations are considered as innovators in the technological area. Furthermore, their policies and laws prove that they strategically operate in a high speed level in order to provide a wealthier and stable future to their residents but also to the world. To do so, they integrate data and information technologies to every aspect of social life by respecting individuality but also promoting collectivity as prerequisites of digital governance and governance of data.

Essentially, Data Governance is not the solution to every problem of the operating model of a country, organization or private corporation. It is a tool that was created by the need of integrating people's necessities, processing responsibilities and technological achievements into a unified system of decision rights and accountabilities. The models of DG differ depending on the structure, needs and implementation of their operations. Also, DG is not the only instrument that is needed for proper, accountable, auditable and transparent collection and use of data. Master Data Management and Data Management are important systems of data utilities, while IT and Information Governance interconnect with DG and they all together form the most suitable package for accountable and transparent collection and use of data and information from every private or public organization. Nowadays, data collection, control and use are highly needed for the economic and structural growth of an operation either it is public or private. Data is a strategic asset but also a resource of wealth for every society which strives to integrate technological achievements into its inhabitants' everyday life. However, data is not useful without models which will term how it will be harvested, controlled and implemented. These define the importance of DG operations and also the importance of accountable, transparent and integral procedures, standards and policies on the sector of Data Governance. The integration of data sciences in every sector of human activities is coming fast, in a not presented scale and with more advantages than disadvantages for the prosperity, growth and stability of our societies. The questions that remain to be answered are: firstly, what will be the impact of this way of governance in the structure, function and efficiency of our world's social and governmental models and secondly, whether it will be exploited by international regulators and occupants of economic, social and political power in order to offer a future where justice, respect to human integrity, social stability and balanced economic growth between people and businesses are factors which define and shape the establishment and implementation of policies and laws around this new field of governance. In conclusion, the global

law and order demands radical changes to its structure and implementation in order to adjust in a world that combines digital technologies to real life and the needs of it. Now, more than ever, data science and technology are at the center of every practical public or private operation. At the same time, the historical period of our times is crucial because of this transition that our world is facing through the introduction and implementation of digital technologies to everything, from daily activities of a citizen to defense operations of a country. Stakes are higher than ever and demands for liable, transparent and accountable strategies, policies and laws have to be also a top priority from governments, international institutions and private corporations. This is why solid and clear data governance plans and policies, working as a useful toolkit of data science, are so much needed in a world that is changing economically, politically and socially faster than ever before.