DATA PROTECTION IN A SMART CITY BIKE SYSTEM: THE EXAMPLE OF TURKU

University of Turku

Faculty of Law

Master's degree of Law and Information Society

Vera Fovet (602451)

September 2018

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

UNIVERSITY OF TURKU

Faculty of Law

FOVET VERA: Data protection in a smart city bike system: the example of Turku

Master Thesis, x + 77 pages

Master's Degree Programme in Law and Information Society

September 2018

This study aims at analysing the data protection measures necessary in the city of Turku's bike system. The city of Turku, Finland, has launched a city bike service, handled by the public transportation service 'Föli' and providing 300 bikes for rental all over the city. This new city feature makes Turku attractive, easily discoverable, eco-friendly and smart. For the purpose of this thesis, Turku is even considered as a smart city, as together with other smart services the city bikes allow for smart transportation and enhances urban life.

Yet, as smart as the city can be, data protection should not be despised. The new General Data Protection Regulation 2016/679 (GDPR), enforceable on May 25th 2018, changes the rules for processing personal data and organisations are required to get compliant with it. Compliance with the GDPR encompasses several aspects, both from a technical and a legal point of view.

This thesis analyses Turku's city bike system and particularly all the steps requiring processing of personal data. This paper examines the possible technical risks, the actors involved and their liability under the GDPR, the applicable data protection requirements as well as the possible solutions for a smooth processing of personal data. The research has been made in concertation with Turku's city bike system team with the aim of identifying the legal steps necessary to this system for a lawful processing of personal data.

Keywords: city bikes, GDPR, data protection, smart city, security, personal data processing, consent, privacy

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I am extremely grateful to the city of Turku for giving me the opportunity to write my thesis on one of the city's projects. I am particularly thankful towards the city bike team, namely Topias Pihlava, Lauri Markkula, Stella Aaltonen and Päivi Kynkäänniemi for the numerous meetings and their useful assistance.

I would also like to thank my supervisor Juha Lavapuro for being my first link with the city of Turku and for his helpful reviews.

Finally, I am grateful to my family for their unconditional encouragements and support.

BIBLIOGRAPHY

Books

- European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European data protection law*, 2014
- Inman Harvey, Ann Cavoukian, George Tomko, Donald Borrett, Hon Kwan, D, Hatzinakos, *SmartData, When privacy meets evolutionary robotics*, Springer, 2013
- Lawrence Lessig*, Code version 2.0*, Basic Books, 2006
- Bruce Schneier, *Data and Goliath*, W.W. Norton, 2015
- Anthony M. Townsend, *Smart cities: big data, civic hackers, and the quest for a new utopia*. W. W. Norton, 2013
- Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017

Articles

- Mary C. Ah Kioon, Zaho Wang, Shubra Deb Das, *Security Analysis of MD5 algorithm in Password Storage*, Applied Mechanics and Materials Vols. 347-350 (2013) pp 2706-2711, 2013
- Imtiaz Ahmad, A. Shoba Das, *Hardware implementation analysis of SHA-256 and SHA-512 algorithms on FPGAs*, Computers and Electrical Engineering 31 (2005) 345–360, Elsevier, 2005
- Jan Philipp Albrecht, *How the GDPR Will Change the World*, EDPL, 3|2016
- Majed Alshammari, Andrew Simpson, *"Towards a Principled Approach for Engineering Privacy by Design"*, in Privacy Technologies and Policy, 5th Annual privacy Forum APF 2017, Springer, 2017
- David Berend, Bernhard Jungk, Shivam Bhasin, *"There Goes Your PIN Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting"*, 2017

- Reuben Binns, *Personal Data Empowerment and the Ideal Observer*, Digital Enlightenment Yearbook 2014, 2014
- Center for Information Policy Leadership (CIPL), "*Examples of Legitimate Interest Grounds for Processing of Personal Data"*, 2017
- Ann Cavoukian, *Privacy by Design and the Promise of SmartData*, SmartData: Privacy Meets Evolutionary Robotics, Springer, 2013
- Dipankar Dasgupta, Arunava Roy, Abhijit Nag, *Authentication Basics Key to the kingdom – Access a Computing System, Advances in User authentication*, p.1 – 36, Springer International Publishing AG 2017
- Lilian Edwards, "*Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*", European Data Protection Law Review (Lexxion), 2016
- Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing, Everything*, 2011, Cisco
- Kevin Fu and Wenyuan Xu, *"Risks of trusting the physics of sensors; Protecting the Internet of Things with embedded security*" Communications of the ACM, feb.2018, vol. 61, n.2
- Miguel Helft, *Is There a Privacy Risk in Google Flu Trends?,* 2008 available at: https://bits.blogs.nytimes.com/2008/11/13/does-google-flu-trends-raises-new-privacy-risks/
- Woongryul Jeon , Jeeyeon Kim , Youngsook Lee , and Dongho Won, *"Practical analysis of Smartphone Security*", M.J. Smith, G. Salvendy (Eds.): Human Interface, Part I, HCII 2011, LNCS 6771, pp. 311–320, 2011. © Springer-Verlag Berlin Heidelberg 2011
- Bert-Jaap Koopsand, Ronald E. Leenes, "*Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law*", International Review of Law, Computers & Technology, 2014 Vol. 28, No. 2, 159–171, http://dx.doi.org/10.1080/13600869.2013.801589
- Gabriel Maldoff, *The Risk-Based Approach in the GDPR: Interpretation and Implications*, CIPP/US, IAPP Westin Fellow
- Alan Mitchell, *"GDPR: Evolutionary or Revolutionary?"* Journal of Direct, Data and Digital Marketing Practice, 2016

- Paul Ohm, Broken promises of privacy: responding to the surprising failure of anonymization, UCLA Law Review, 2010
- Michael E. Porter, James E. Heppelmann How smart, connected products are transforming companies, harward business review, 2015
- Ira S. Rubinstein and Woodrow Hartzog, "*Anonymization and Risk*" (2015). New York University Public Law and Legal Theory Working Papers. Paper 530
- Bruce Schneier, "*The internet of things is wildly insecure — and often unpatchable*", Opinion, Wired magazine, 2014
- Bruce Schneier, "*The Importance of Strong Encryption to Security"*, 2016, available at: https://www.schneier.com/blog/archives/2016/02/the_importance_.html
- Bruce Schneier, "*The value of Encryption*", Schneier on Security blog, 2016, available at: https://www.schneier.com/essays/archives/2016/04/the_value_of_encrypt.html
- Bruce Schneier, "*The Eternal Value of Privacy*", available at: https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html , 2006
- Dana Simberkoff, "*Privacy and Security by Design: The New Default under GDPR*", AvePoint blog, available at: https://www.avepoint.com/blog/protect/privacy-and-security-by-design-gdpr/
- Sarah Spiekermann, Alexander Novotny, *A vision for global privacy bridges: technical and legal measures for international data markets*, Computer Law and Security Review, 2015, 181-200
- Latanya Sweeney, "*k-Anonymity: A model for protecting privacy*", International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570
- Omer Tene and Jules Polonetsky, *Privacy in the age of big data, A time for big decisions*, Feb. 2012, Stanford Law Review
- Marianthi Theoharidou, Alexios Mylonas, Dimitris Gritzalis (2012) *"A Risk Assessment Method for Smartphones",* In: Gritzalis D., Furnell S., Theoharidou M. (eds) Information Security and Privacy Research. SEC

2012. IFIP Advances in Information and Communication Technology, vol 376. Springer, Berlin, Heidelberg

- George Tomko, *SmartData: The Need, the Goal and the Challenge*, SmartData: privacy meets evolutionary Robotics", Springer, 2013
- MariaVasilevskaya and Simin Nadjm-Tehrani, *"Quantifying Risks to Data Assets Using Formal Metrics in Embedded System Design"*, Springer, 2015
- Felix Wortmann and Kristina Flüchter, *Internet of Things Technology and Value Added*, Springer, 2015
- Bart W. Schermer, Bart Custers, Simone van der Hof, *The crisis of consent: how stronger legal protection may lead to weaker consent in data protection*, Springer, Ethics Inf Technol (2014) 16:171–182

Opinions and guidelines from the article 29 Working Party

- Opinion 03/2013 on Purpose Limitation, 00569/13/EN, WP 203, 2013
- Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN, WP 216, 2014
- Guidelines on Consent under Regulation 2016/679, 'adopted, but still to be finalized', 17/EN, WP 259, 2017
- Guidelines on Transparency under Regulation2016/679, 'adopted, but still to be finalized', 17/EN, WP 260

Case law

- Data Protection Commissioner, Case Study 2015*, Failure to update customer's address compromises the confidentiality of personal data* available at: *https://dataprotection.ie/viewdoc.asp?DocID=1620&ad=1#201511*
- Google Spain v. Agencia Espanola de proteccion de datos ('Google Spain'), C-131/12, 2014

Websites

- Web learning resources for the EU General Data Protection Regulation, available at www.gdpreu.org
- French 'National Commission on Informatics and Liberty' (CNIL), available in English at: https://www.cnil.fr/en/home
- The European data protection supervisor (EDPS), homepage available at: https://edps.europa.eu/
- The Finnish national legislation database, available at: https://www.finlex.fi/sv/

Reports

- University of Cambridge Judge Business School, *Personal Data Stores*, 2014-2015, Opinion 9/2016
- The European data protection supervisor (EDPS), *Opinion on Personal Information Management Systems, towards more user empowerment in managing and processing personal data*, Opinion 9/2016
- Antti Poikola, Kai Kuikkaniemi, Harri Honko, *MyData, A Nordic model for human-centered personal data management and processing,* Finnish ministry of Transport and Communication
- Boston Consulting Group (BCG) and Liberty Global, *The value of our digital identity*, 2012

Video conferences

Professor Martyn Thomas CBE, *Big Data: The Broken Promise of Anonymisation*, 2016, available at: https://www.youtube.com/watch?v=q5c7a7Jd9Kk

- Professor Gideon Samid, Hashing: *Why and How?,* 2013, available at: https://www.youtube.com/watch?v=yXmNmckX4sI&t=185s

ABBREVIATIONS

CNIL: National Commission on Informatics and Liberty
ECJ: European Court of Justice
EU: European Union
GDPR: General Data Protection Regulation 2016/679
PIN: Personal identification number
TFEU: The Treaty of the Functioning of the European Union (TFEU)
The Charter: The Charter of Fundamental Rights of the European Union
VPN: Virtual private Network
WP 29: Article 29 working party

I. INTRODUCTION

1.1 City bikes in the smart city trend

The first shared city bikes in Europe were launched in Copenhagen in 1995, and the idea has ever since spread to 22 European countries and throughout the world. Nowadays, most big cities in Europe are offering the bike service, which enables citizens to easily rent a bike on an hourly fee, usually paid by credit card. The city bike concept is fashionable, eco-friendly and is a major element in the smart city trend.

The aim and need of a smart city are public. All "smart" technologies and services implemented by a smart city are designed to serve the city and all the people living therein. The city bikes are no exception, and although their rental requires a small fee, they belong to the smart city dynamic and the ambition to make the way of life in cities *smarter*.

Although a smart city does not yet have a single definition, some are defining them by the implementation of digital instruments capable of steering the way cities are configured and managed[1]. In this interpretation, surveillance cameras, smart sensors, smart meters and other smart networked and digital devices are the core of the smart city. All these devices, main constituents of the Internet of Things (IoTs) collect real-time data which the city uses to provide its services. The public devices are supplemented by personal ones, such as smart phones and connected cars in order to create an urban environment where every movement, action and condition is measured and collected for further use. Others consider that these digital tools are promotors of citizen-centric models, which aim at focusing on the citizen as the core element of the city, encouraging civic engagement, developing better communication tools between the government and the citizens in order for the latter to be heard.

[1] Kitchin, R. (2016) Getting smarter about smart cities: Improving data privacy and data security. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland

Some sceptical scholars like Townsend[2] follow the evolution of smart cities with a critical eye, fearing that all this information technology, "*combined with the urban infrastructure, architecture, everyday used objects and even our bodies*" will only lead to produce vulnerable, "buggy", "brittle" and hackable systems. Information technologies are not failure proof, and in particular in smart cities, one of the objects at risk is personal data.

Yet, all definitions share the common idea that a smart city is a place where the connection of digital devices and new technologies allow for a faster and a smoother handling of all kinds of city-situations. These city-situations are all from faster medical care, eco-friendly street lights and well-adapted transportation services, with no fuss. The smart city concept is expected to make the urban life easier.

City bikes are an intelligent solution adopted by several cities to take a step further in the smart revolution. Bikes facilitate citizens to move around quickly without any carbon footprint. Copenhagen, in Denmark, has efficiently adopted *Bycyklen*, an electric city bike the city is very proud of and which constitutes a core element in their smart project[3]. Amsterdam, another main bicycle hub, is even taking a step forward by launching FindMyBicycle: a paying GPS solution to be installed on private bikes, and aiming at connecting all bikes together. With the installed device, each owner is able to watch their bike through a mobile application. A simple, privately-owned bike would ultimately become a *smart bicycle*," capable of connecting with other smart bicycles and smart cities' infrastructures, creating a system of bicycles." [4] Hopefully, such a system of bicycles would ultimately reduce bike thefts.

As stated above, these great innovations come with a vulnerability, namely the protection of personal data. Although city bikes are part of a public service, usually offered by a public entity, their use require the process of personal data.

The protection of personal data is legally referred to as data protection and applies to any information which relates to an identifiable or identified natural person. In Europe,

[2] Townsend, A. (2013) Smart Cities: Big data, Civic Hackers, and the Quest for a New Utopia

[3] See Visit Copenhagen website and the bycyklen project, available at http://www.visitcopenhagen.com/copenhagen/bycyklen-gdk495345

[4] See Smart Amsterdam website and the FindMyBicycle project, available at https://amsterdamsmartcity.com/products/find-my-bicycle

the protection of such data has been enhanced with the adoption of the General Data Protection Regulation 2016/679 (GDPR), adopted on April 27th, 2016 and entering into force on May 25th 2018. It sets the new rules for all processing of personal data within the Union and repeals the previous data protection directive 95/46/EC. As a regulation, the GDPR is directly applicable into the national laws; the member states do not need to transcribe the laws into national ones apart for some exceptional provisions which are subject to being transposed into national law. This direct applicability facilitates its adoption in the member states, which need to reasonably justify any divergence with it.

The GDPR has been developed as to fit the digital age and treats data protection as a fundamental right. The recital of the GDPR states that "*the protection of natural persons in relation to the processing of their personal data is a fundamental right*", which means that it is a right *"considered by a Court to be explicitly or implicitly expressed in a Constitution […] [and which can only be limited] if there is a compelling State interest."* as defined by the Meriam Webster Dictionary of Law. The entitlement of "fundamental right" takes its roots from the article 8(1) of the Charter of Fundamental Rights of the European Union which provides that "*Everyone has the right to the protection of personal data concerning him or her*", and from the article 16(1) of the Treaty of the Functioning of the European Union which states that "*Everyone has the right to the protection of personal data concerning them*". The protection of personal data should thus be prioritized when designing the structures and the technologies of smart cities, in order to avoid any violation with citizens' personal data.

This fundamental right to protection applies to personal data. In its article 4 (1), the GDPR defines personal data as *"any information relating to an identified or identifiable natural person"*. In fact, data gets linked to an identifiable person rather quickly. For instance, it suffices that two sets of "anonymous" data be linked together to transform the sum into personal data. For example, a name alone, like "Maria", does not easily lead to the identification of a person. But if "Maria" is linked to a birthday, it becomes easier to identify this person, as the sum of these two strings of data narrows down the amount of 'Marias' being born on that exact birthday. The more data is linked together, the easier it is to identify a person; and when the data allows to identify a person, it is referred to as *personal data*.

This works as well for data not as obvious as names or birthdays. An IP address as such is not per se personal data - merely a set of numbers. However, when linked to another set of information, such as the Internet Service Provider (ISP) used, the user's name or even the smartphone's GPS location, the information becomes personal. As stated by Lessig[5]:*" The Web must know an IP address; ISPs require identification before they assign an IP address to a customer. So long as the log records of the ISP are kept, the transaction is traceable. Bottom line: If you want anonymity, use a pay phone!"*

The GDPR also receives considerable attention as it encompasses more personal data than the superseded directive. The latter identifies a natural person *"by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*"; in comparison, the GDPR considers that a natural person can *also* be identified by "*a name*", "*an identification number", "location data", "an online identifier*" as well as "*genetic*" identity, on top of those listed in the Directive. In that sense, the GDPR widens the sources of identifiers requiring protection.

It is nonetheless important to keep in mind that it is not prohibited to use personal data for a service. Many services do actually need to process personal data for a better and more tailored activity. As a matter of fact, the whole smart city concept is based on the usage of data on a real-time basis, Turku's city bike system makes no exception. It is not the personal data alone which is the main focus of the GDPR, but the way it is *processed*. As wide as the definition of personal data can be, the GDPR also englobes a whole set of processing activities and provides rules for protecting personal data in the event of it being processed. According to the article 4 (2), the processing of data refers to *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."*

In addition, the GDPR also reforms the directive by adding another element, that is the data user's control over her personal data. The regulation strives for making the

[5] See L.Lessig, Code 2.0 in the chapter "architecture of control"

protection of personal data user-centred, and as clearly indicated in Recital 7, "*natural persons should have control of their own personal data*".

In theory, an individual's personal data is not protected as soon as he or she steps out in a public area, like into a street or a mall. What this individual does in the public space, who he talks to and where he goes is all data that is not per se protectable[6]. However, the *processing* of this data is regulated. In other words, as soon as the actions of an individual walking in the street are recorded, it becomes protectable. The GDPR, as described in the previous section, lists all the different kinds of operations considered as "processing" and which gives the right to protect the processed data.

The smart city is by definition a huge producer of data. Many see data as the fuel of the city of the future. As formulated in the Economist, "*data are to this century what oil was to the last one: a driver of growth and change*[7]". All kinds of data emanating from all kinds of different sensors and monitors are of interest, and most importantly, the data is real-time data. Data is therefore sensed all the time and most of it emanates from the citizens themselves, as they connect to a public WIFI with their smartphone or their laptop, as they use smart parking with their car or as the smart street light senses pedestrians walking by. This thesis will attempt to identify the different processing steps undertaken by Turku's public transport service Föli and their processors.

Daily, large amounts of data are produced and a wide amount of this data is categorized as personal data. This data is to be duly protected against leaks or misuses as it is inherent to each person's privacy. Many are the organisations, companies and even individuals unaware of the vulnerability of personal data and the right for accurate protection, and usually measures are taken only once problems occur. However, when the data is out it might be too late: identity theft is a fact and, as

[6] Lessig, *Code 2.0*

[7] The Economist, (2017), Fuel of the Future: Data is giving rise to a new economy, [online] Available at: http:// https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy

reported in Cifas' 2018 report[8], 175 000 cases of identity frauds were counted in 2017, in 90% of which a victim's home address had been used. It is an idea largely supported by scholars: data protection works best if considered proactively.

As stated previously, the GDPR's recital's first sentence stresses the fact that the protection of personal data is a fundamental right, with reference to the article 8(1) of the Charter and to the article 16(1) of the TFEU. Data protection as a fundamental right goes along with the right to privacy, which is a pillar of freedom in our society. Schneier, in his article "*The eternal value of privacy*"[9] considers that if privacy is despised and personal data ignored, our very individuality is lost, "*because everything we do is observable and recordable*".

The city of Turku starts glowing as a modern city in full smart-revolution. The initiative to launch a city bike project in the city is one of the smart steps, among several others such as smart bus stops or 'the Smart and Wise Turku' project. The city of Turku is, in the case of the city bikes, the controlling authority, however this control is intended to switch to Föli in a couple of years. Föli is a public department in the city of Turku which will for now operate the city bikes, and for these reasons the city of Turku will hereinafter be referred to as Föli in this thesis.

The city bike project aims at lending out city bikes to individuals for a small fee. The bike is made available from bike stations, of which there are 34, situated throughout the city of Turku. The whole city bike system is expected to count 300 bikes, to start with. The lending time for each bike is limited to 5 hours, allowing the users to travel from one point to another within the city, also enabling the bikes to be regularly available for everyone wishing to rent one.

For facilitated management purposes as well as payment security and statistical purposes, data is collected from the bike users, including personal data. Some data, which initially does not constitute personal data, becomes personal after association with other data, thus enabling the identification of a natural person. The city bike

[8] Cifas Fraudscape 2018, available at: https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Fraudscape%202018-Final.pdf

[9] See Bruce Schneier, The Eternal Value of Privacy, available at: https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html , 2006

project of Turku does therefore process personal data, making the GDPR applicable. The regulation is also applicable as Turku, city of Finland, is located in the European Union.

1.2 Research question and thesis structure

City bikes are obviously a trend adopted by more and more cities around the world. But what the city bike systems fail to show to the public is the legal issues involved, and in particular the data protection side. For billing and maintenance purposes, the bike user's personal data is required, such as her name, her address and her credit card credentials. Usually, and at least in the case of Föli, the city bikes are equipped with a GPS which could potentially track the movements of the users. In order to avoid identity thefts and other misuses of personal data, as well as being in compliance with the GDPR, it becomes crucial to consider data protection when designing or updating the processing activities. It also becomes important to identify the different actors involved in the system and their respective liability. Furthermore, the awareness of the technical risks and the technical solutions is essential for a global protection of the personal data.

With the support of Turku's city bike team, this thesis will attempt to answer to the question: how is personal data processed in Turku's city bike system and which legal and technical requirements should be considered with regard to the GDPR?

This thesis will first analyse the technology and its application in the city bike system (II). It will then identify the different actors involved (III), the GDPR requirements applicable to Turku's city bike system (IV) and finally the possible solutions for a secure processing of personal data (V).

Meetings with the city bike team were organized approximately once a month and provided me with a great understanding of the city bike system's design, as well as raised legal questions I hope I was able to answer to in this thesis.

II. THE TECHNOLOGY AND ITS APPLICATION IN THE TURKU CITY BIKE SYSTEM

New technologies are the core of the smart city, the mechanism which makes it smart. As it was made clear in several conferences in the Smart City Expo Barcelona[10] in 2016, data in a smart city flows fast and is dependent on three main features: sensors, cloud or server storage and a strong WIFI connection. The city bike project launched by the city of Turku is dependent on the same tools, in addition with Bluetooth connection used by the beacon technologies[11]. All these features have important risks with regard to data protection, and these risks are substantially linked to the citizen's ability to give consent.

This section identifies the technologies used in the Föli bike services and the technical risks linked therein. For instance, Föli's bike system is composed of bikes, equipped with small transmitters called beacons to which connection is possible through a smartphone. The smartphone also enables to pay for the bike and to get further information on the Föli system.

2.1 The sensors involved in the project

Although the whole city bike project of Turku gravitates around bikes, there are a few sensors involved in it. Despite the fact that they are necessary for the smooth running of the bike system, they are also technologically weak compounds which need particular attention, especially with regard to data protection.

[10] In conferences such as:

- "Big data for more responsive and humane cities" with Josep Missé Cortina ;
- "Strategies to protect critical infrastructure and ensure digital safety" with Joe Paiva, Bernard Ewah, Swadheen Kshatriya and Alfredo Pironti ;
- "Finding the balance between Privacy and Security", with Eduardo Bohorquez, Victoria Beltran and Mohamed Amin Hasbini

[11] More information on the beacon technology available in section 2.1.2

2.1.1 Sensors in the city are part of the Internet of Things movement

Before analysing the sensor technology, it is important to understand the dynamic it is involved in, namely the Internet of Things (IoT). Although it is quite difficult to specifically define due to its broadness, the Internet of Things refers to the communion of physical and digital characteristics aimed at creating novel products and services. The concept is still under development and its value as a business opportunity is no longer questioned: its value has even been estimated as to reach $7.1 trillion by 2020[12].

Usually, the novelty adds new digital software to an old physical product. As an example, let's consider a lightbulb. The primary function of the lightbulb would be to be lit-up and to be switched off. If IOT technologies, such as a software programming, were to be included in the design of the lightbulb, it would not only serve the purpose of lighting up, but it could also detect movement and even have face-recognition features. From a simple lightbulb, IoT could turn it to be a security and an energy-saving tool.

More and more services function through transfers of digital information. Those transfers occur fast and on a real-time basis, between Internet-connected objects. These objects can be computers, smartphones, watches, glasses, cars, fridges… Cisco predicts that 50 billion devices will be connected to the Internet by 2020[13].

The enhancement of simple urban devices is very much what a smart city is about. Following the same pattern as the lightbulb, most smart cities are attempting to identify how traditional items could be turned into *smart* items.

The city of Barcelona gives an excellent example on a large implementation of IoT throughout the city. As a matter of fact, Barcelona has already implemented a vast number of sensors, especially placed on the street light poles. These sensors, disseminated all over the city run on timers and detect movement – which is aimed at reducing the energy consumption – but other than lightning up the streets they also

[12]F. Wortmann and K. Flüchter, *Internet of Things Technology and Value Added*, 2015, Springer

[13] Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing, Everything*, 2011, Cisco, available at: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

enable gathering environment information and provide a free Internet access in the city. [14]

"Smart waste" is another example of large implementation of IoT in the city of Amsterdam. Among other projects, the city is installing new sensors in traditional public trash bins, enabling the city to control and monitor remotely their location in order to see where they need to be emptied, their security as well as their content. This sensor is even able to provide rates and statistical data on each household's contribution to the trash bins[15].

In Turku, the users' smartphones, the beacons and the GPS devices installed on the city bikes are all sensors capable of collecting and sending data. The smartphone, for instance, can be used through the "Turku Public Transport Application" (the Föli app) for payment and can also receive the information sent out by the beacon. The beacons get connected to the smartphone by Bluetooth connection and enables the user to get cultural and real-time information about the city. The GPS device facilitates a good management of the bikes and keeps track of their availability throughout the city. These features facilitate the use of the city bike project, both for the users as for the managers.

With the city bikes, Turku signs up in a smart trend already adopted by several cities, and it might only be the beginning in a large series of technical innovations.

Yet, connected devices are complex hardware which require special attention.

2.1.2 The connected devices: technical description

As analysed by Porter and Heppelmann[16], all connected devices have in common three elements: the physical element, the smart element and the connectivity element. The physical elements are the tangible parts, such as the electric and the mechanical components; the smart elements are the sensors, the microprocessors, the software, the

[14] see Smart Barcelona on livingmap.com, available at: https://www.livingmap.com/smart-city/smart-barcelona-its-all-about-people/

[15] see Amsterdam Smart City and the smart waste city by citibrain, available at: https://amsterdamsmartcity.com/products/smart-waste-citibrain

[16] See Michael E. Porter, James E. Heppelmann, How smart, connected products are transforming companies

embedded operating systems, the digital user interface and the data storage solutions; the connectivity elements are the ones enabling communication, such as antennas, ports and networks. Together, all these elements allow for the Internet of Things and Föli is using all of them.

In a smart city, the sensors play a crucial role as they are the means through which the city can obtain real-time information from the citizens. usually a hardware which is designed to capture an event; such as light, movement, temperature, touch or sounds; to record it, and to respond to it. By the means of sensors, the citizens themselves can also transmit data to the city. A sensor could be a smart light bulb which detects movement, as well as a feature on a smartphone.

The smartphone

The smartphone is becoming the sensor most people carry along with them. It is needed in the city bike project as a means of payment, a way of checking the free bike station spots as well as the device through which the information from the beacon is obtained. Defined by researchers [17]as "a mobile phone that offers more advanced computing ability and connectivity than a contemporary basic feature phone", it produces a lot of data. However only the sensor data is of interest in this section.

The smartphone produces and collects sensor data through the following hardware: the camera and the microphone, the GPS sensor, the accelerometer and the gyroscope, the magnetometer (digital compass) as well as a proximity sensor[18]. All these sensors' aim is to measure the exact location of the device, its orientation, the way it is moving and its heading location. By device, it is naturally the smartphone user who is the source of the movement.

In Turku, the bike user might use its smartphone as a mean of payment, through the application "Turku Public Transport", commonly named the "Föli app" and operated by PayIQ Oy. The application might also detect the GPS location of the closest bike stations and their bike parking availability.

[17] W. Jeon , J. Kim , Y. Lee , and D. Won, "Practical analysis of Smartphone Security", 2011

[18] M. Theoharidou, A. Mylonas, D. Gritzalis, *A Risk Assessment Method for Smartphones*

The beacons

Each bike will carry along a beacon. A beacon is a small device which transmits information via Bluetooth to a smartphone or a similar mobile device on a range of approximately 50 meters[19]. Already implemented in 170 buses in Turku, the beacons situated on the bikes will allow the user to connect and get information on the history of Turku, its cultural events and happenings as well as general information on the weather forecast. Some of the information will be drafted and made available by high school students.

The bike's GPS

Each bike is also carrying around a GPS sensor. This sensore nables the operator Nextbike Polska S.A to quickly locate the bikes for maintenance and management purposes. By knowing the bike's location, it becomes easy to monitor an equal provisioning of bikes on every station. This GPS, being attached to the bike, only refers to the bike's location. However, as for the smartphone, the device usually has a user; it goes the same for the bike. The bike user, by choosing the bike and paying for it, gets registered with the bike. Although the user cannot use the GPS as such, the possibility to track the bike's location thus enables to track the user. The GPS information is obtained through satellite. The navigation compound receives GPS satellite signals, determines its position relative to the surface of the earth and the result is read in the form of latitude and longitude.

2.2 Sensors' security environment and the risks linked therein

Sensors have a huge role today in the Internet of things and in the development of smart cities. Although their purpose is to be smart, their design might not be. Bad design and the ability for remote connections make sensors fragile technologies vulnerable to attacks.

2.2.1 Weak design

Sensors appear to be complex small computers designed for the very purpose they are used for. Embedded devices are presenting many vulnerabilities, caused by weak design that could invite attacks on the system.

[19] Definition taken from www.webopedia.com , "the online tech dictionary for students, Educators and IT professionals"

The wide and growing implementation of sensors in our everyday life is subject to a vivid debate. Arguing are the tech fanatics, excited about all the advantages the sensors bring; and the others, concerned about the risks sensors could carry along.

Embedded devices are usually cheap to produce and usually security has not been the priority during the design-phase. The difficulty to evaluate the designed level of security of embedded devices makes it very hard to guarantee secure systems[20], leading us to install unsecure sensors in our systems. This mass-spread adoption in increasing parts of our daily lives is criticized among scholars.

Townsend[21] is specialized in smart cities and keeps a very sceptical eye on the use and the spread of sensors and other technical tools around the city. In his opinion, their massive spread might cause the downfall of the smart cities as these technologies produce "*buggy, brittle and hackable systems*", as they might be designed from the very beginning with defaults. He adds that even though their code is flawless, smart cities will finally collapse as they will become too complex and will occasion accidents for which the size of the consequences is yet to measure. Schneier is of the same opinion[22] as Townsend and sees no good way of coping with the embedded systems' vulnerabilities.

2.2.2 Possible attacks

Although it is difficult to know whether sensors were by design faulty, most of them are weak compounds, with very little or no embedded security measures, and thus easy targets for attacks. Research[23] has for instance been made on the "zero-permission" sensors, which analyses the risk for unintentional leakage of personal data through embedded sensors in smartphones. The zero-permission sensors, accessible without

[20] M. Vasilevskaya and S. Nadjm-Tehrani, "Quantifying Risks to Data Assets Using Formal Metrics in Embedded System Design", 2015, available at: https://www.ida.liu.se/labs/rtslab/publications/2015/Vasilevskaya_Nadjm-Tehrani_RisksToDataAssets.pdf

[21] Townsend, Anthony M.,*"Smart cities: big data, civic hackers, and the quest for a new utopia*", W. W. Norton, 2013

[22] B. Schneier, "*The internet of things is wildly insecure — and often unpatchable*", Opinion, Wired magazine, 2014

[23] D. Berend, B. Jung, S. Bhasin, *"There Goes Your PIN: Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting",* 2017

the user's permission, can thus be hacked by an attacker without the user's knowledge, leading to the leakage of personal identification numbers (PIN) and movement patterns, leading to behavioural profiling, the recovery of the user's PIN codes and geo-localization.

Transduction attacks also refer to the weak design of the embedded devices and many researches warn for the risk they are to privacy. Transduction attacks aim at manipulating the physical properties of devices. As a consequence, sensors and embedded devices stop functioning the way they should. The behaviour of the sensor is manipulated, and whatever the information it is supposed to obtain or give out is changed. For example, a test was made on a Tesla car where its obstacle sensor was attacked, and thus mislead the driver on the real distance to the obstacle[24].

It remains difficult to forecast whether the systems set in place in the city of Turku will be victim of attacks such as those described in this section. However, the goal should not be to observe whether attacks have occurred, but to prevent them. Risk prevention starts by awareness and is completed by technical measures such as regular updates of the sensors software (applicable to the bikes' GPS system and the beacons). The smartphone users could also disable their sensors while making sensitive operations with their smartphone, when for example checking their bank account.

2.2.3 Loss or theft of devices

As an addition to the technical security of the embedded devices, all the other components of the IoT present security risks. Although they will not all be analysed in this thesis, the risk of loss or theft of devices is worth mentioning, as well as its implication on the protection of personal data. In the event that a Föli employee's work computer is stolen, what are the risks that personal data from bike users gets in the wrong hands?

[24] K. Fu and W.Xu, "Risks of trusting the physics of sensors; Protecting the Internet of Things with embedded security" Communications of the ACM, feb.2018, vol. 61, n.2

2.3 Basic security features

The risks announced in the previous sections are just a glimpse on what the city bike project could risk with its technical infrastructure. A proper risk analysis by security experts would be much more thorough and applicable. However, some basic security features could be taken into account without having identified all the technical risks involved in the bike project.

2.3.1 Updates

All software and hardware tools should be regularly updated. Updating is important, as an old system becomes obsolete and technically weak with time and thus more easily hackable by attackers.

2.3.2 Encryption

As a palliative to the weakness of the sensors, one solution could be to encrypt all the data emanating from the devices. Encryption is a way of encoding and protecting information so that only the legitimate parties can access the data, and is considered as "appropriate safeguards", together with pseudonymisation *[article 6 GDPR]*. Without the encryption key, the information shows as gibberish. Encrypting the data is widely used for civilian purposes and is considered as a basic security tool. As stated by the founder of Crypto Party Harlem[25], *"an unencrypted internet-connected app or webtool [is like] a window without curtains"*, meaning that anyone could theoretically see what data this is about.

There exist three different methods of encryption: hashing, symmetric encryption and asymmetric encryption.

The password hashes

The hashing method consists in creating a unique signature, a "hash", for one data-set. As perfectly explained by the professor Gideon Samid[26], the created hash is in one way only, making it impossible to go backwards from the hash to the data-set.

For example, if the content is "abc1234", the hash might be "45fg".

[25] Matthew Mitchell, founder of the security training organization 'Crypto Party Harlem'. More information on crypto parties available at: https://www.cryptoparty.in/

[26] Professor Gideon Samid from the University of Maryland and Chief Technology Officer at BitMint. His lecture on hashing "*Hashing: Why and How?*" is available at: https://www.youtube.com/watch?v=yXmNmckX4sI&t=185s

This signature is sometimes called ‘digital signature’ or even ‘digital fingerprint’. As this number is unique, any change to the data-set radically alters the signature. The signature is thus like a sum up to what is in the data-set; if the data-set is changed somewhere, for instance if a letter is changed in the title, the hash is going to show completely differently.

> For example, if “**a**bc1234” is modified to become “**b**bc1234”, the hash might become “aaa8”.

The idea with the hashing encryption is to obtain a signature number which identifies the original data-set and authenticates it. Hashing does not per se hide the data-set, but will show if there are errors in the data-set or if the data-set has been modified by a hacker.
For example, Alice has a file and generates a hash based on this file. Bob claims that he has the same file. Because Alice is sceptical, she asks Bob to hash his file and to show the obtained signature. If the hash obtained by Bob is the same as Alice’s, then the two documents are the same.
One main advantage with hashing is that an attacker cannot recover the content of the data-set by using a hash. Password hashing is therefore a perfect tool to use when building a password-based protection, and specifications such as SHA-256 and SHA-512[27] seem to be the best.

Symmetric encryption

Symmetric encryption, or single-key encryption, might be the most commonly known method of encryption. A perfect example is the use of a password on a word processing document. The idea is to encrypt the data-set with an algorithm, and to create a decrypting key. As easily as a key opens a door, the key decrypts the data-sets and allows for the recipient to access the content. Both the sender and the receiver

[27] More detailed information on the different hash functions explained in the article “Hardware implementation analysis of SHA-256 and SHA-512 algorithms on FPGAs”, by I. Ahmad and S. Das, 2005

share the same key as there is only one key which allows for decryption. This system is a basic encryption method easily performed.

Asymmetric encryption

The asymmetric encryption, or public key, functions on the same basis as the symmetric encryption apart from the fact that two different and mathematically linked keys are used: one for encrypting the data-set, and one for decrypting it. The sender, encrypting the file, uses one key, and the receiver, decrypting it, uses the other, making this whole process a little bit more secure than the symmetric version.

2.3.3 Storing passwords

One of the most basic security features independent of any technology is the storing of passwords. Passwords are keys which enable access to a protected content, and might be used internally in the organisation, as well as by the users. All passwords, including the ones chosen by the users to access their user portal, do possibly have to be stored by the organisations. And it goes without saying that this storage has to be very secure.

There are several different methods of storing password and the different operating systems seem to all have their own storing system. However, there are a few tips[28] on how *not* to store passwords: First, passwords should never be stored in the organisation's system in plain text in an unencrypted excel file, as this would be facilitating the job for potential hackers! Second, symmetric encryption is not either recommended, nor is hashing surprisingly, as many users have the same passwords (such as '12345' or 'Password1') which then generate the same hash! This is also the reason for choosing a very secured password, preferably based on letters, numbers and signs.

[28] These recommendations were excellently presented by Tom Scott on the channel 'Computerphile', available at: https://www.youtube.com/watch?v=b4b8ktEV4Bg&t=393s

Password managing companies[29] do in practice store passwords by 'hashing with salt' and this method is also widely recommended among scholars[30]. Hashing with salt implies that a random and different string of characters is produced for every single user, thus making it impossible to guess similar passwords.

> For example, even though two users have the same passwords '12345', they will both be hashed with salt differently, on being hashed into '78gfd' and the other into '34sir'.

The hashing with salt method therefore allows an organisation to store the usernames next to their password, making it very impractical for hackers to access the 'real' password behind the hash.

Embedded devices are being widely adopted and installed, both on the city scale as on the private side. Their use facilitates many services and changes them, making them faster and more personalized. The city bikes of Turku are using embedded services for a smooth management, both for the users as for the service providers. However, sensors have shown technical vulnerabilities which could threaten the whole systems with attacks and theft of data. As countermeasures, it appears important to be aware of these threats and react accordingly by regularly updating the systems and encrypting the data issued by the sensors, as well as storing all data securely with a secure hashing with salt method.

[29] Password managers such as Dashlane, Sticky Password and Password Boss

[30] M. C. Ah Kioon, Z. Wang, S.Deb Das, *Security Analysis of MD5 algorithm in Password Storage*, Applied Mechanics and Materials Vols. 347-350 (2013) pp 2706-2711, 2013

III. THE CITY BIKE ACTORS, ROLES AND RESPONSIBILITIES UNDER THE GENERAL DATA PROTECTION REGULATION (GDPR)

The actors involved in the use and the smooth management of Turku city bikes are several, and stretch from the very bike manufacturer to the user. This section aims at listing all the actors involved in the city bike project, at identifying their production of data (personal and non-personal) and their share of responsibility on personal data protection.

3.1 Architectural description of Turku's city bike service

This section studies the different actors involved in the city bike project, from the user to the manufacturer.

3.1.1 The bike user

The bike user is the most important source of personal data as it directly refers to a natural person. It is therefore important to have a thorough overview over all the data collected from her, either as given voluntarily or as collected through other services.

In order to use the rental bike, the user needs to pay a small fee. To access the service and pay, either performed on the internet, through the Föli smartphone application or in the Föli customer office, the user needs to provide her name, her date of birth, her address and her bank account number. These sets of information constitute personal information which requires thoughtful protection in line with the GDPR. The bike gets accessible once the user validates its payment method.

3.1.2 Föli

- *Föli as a controller*

Föli is the controller in the city bike service. According to the article 4(7) GDPR, a controller means *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data […]"*

Föli is at the head of the city bike service and launched the project. It is designing the service, and decides what information is required from the users for a smooth running

of the service and for the billing system. Föli sets the means of collection of the users' data and is sole liable towards the users. Föli is in fact the only body running a feedback system and having any exchange with the bike users.

- *Föli as a processor*

Föli does also wear the processor cap. A processor is being defined under article 4(8) GDPR as" *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".*

Föli is collecting the users' personal data and their biking route information from different sources. This information is for the most becoming personal data once transferred to Föli from different service providers. The manufacturing and maintenance company Nextbike Polska S.A is for instance providing Föli with the exact GPS information for every bike. The ticketing system Init, ensuring that the user can pay for a bike with its chosen payment method, provides Föli with the card ID of each user having used a bike. Put together, the GPS information linked to the user name give the ability to know *who* took *which bike*, *where* and at *what time*. Föli collects all this data, stores it and might come to analyze it. These actions are processing activities and makes Föli a processor.

3.1.3 The service providers

A total number of six (6) service providers are involved in the city bike rental service.

- *Nextbike Polska S.A*

Nextbike Polska S.A, is a Polish company specialized in self-service city bikes. They design and manufacture the bikes and their service includes the maintenance of the bikes and the management of their location in the city of Turku. They are thus liable for repairs and fixing flat tires, as well as making sure that a relatively equal number of bikes can be found on all the 34 stations available in Turku. Their service comprehends the design, manufacture and maintenance of the bike racks. Their service is enabled through maintenance vans and GPS trackers, located on every single bike. The GPS tracker allows for fast and accurate localization of the bikes and facilitates counting them and organizing their location. The station alone has no intelligence.

In the event that a bike has been damaged on purpose, Nextbike Polska S.A could request compensation from the author of the damages, and would in this case need to

access the user's name and contact information. This would lead to a transaction of personal data between Föli and Nextbike Polska S.A which needs to be duly reported in their terms and agreements, as well as in the report of processing activities *[article 30 GDPR]*

- *Init*[31]

Init is a ticketing service provider in charge of the ticketing system over all the Föli network. It is functioning in all the buses and is to be operational for the city bikes as well. Init's ticketing system is based on the user card's ID. The card ID only provides information about the user's account, which is a number. This number, needed for the management of the bus or bike trips, is stored and managed in real time in the back-office system.

However, once this number is transferred to Föli, it becomes personal data as it gets connected to the user's information connected to the account number. As stated on their website, Init might come to process personal data when establishing an identity and secure verifications. For these reasons, they are to be considered as processors.

- *Western systems*

Western systems are a Finnish software company providing Föli with several services inherent to the city bike renting project. By their services, they collect mass amounts of data concerning the bike users, such as their name, the time spent on the bike… All this data is stored in the same storage as Föli's. Föli can therefore access this personal information. By collecting and storing this data, Western systems is processing it and is thus considered as a processor according to the article 4(8) of the GDPR. Western System have access to the whole Föli system, write its code and maintain it, it is therefore very important that a record is kept between Föli and Western Systems on all the processing activities.

- *Nets*

Nets is the payment system used by Föli to charge the bike users when they load money through their bank account. Payment can be performed in different ways: either with loaded money by bank card on the user's bus card; or with the user's phone number

[31] More information on INIT available at: https://www.initse.com/ende/news-events/knowledge-database/articles/2016/initiative02-turku.html

and PIN code (this latter method requires previous registration and payment with Western Systems). Nets' system operates the same security as bank transactions. It assures that money is transferred from the user's bank account to Föli's. It charges the users according to their wished amount, and makes this "payment credit" available on their Föli card. The activities undertaken by Nets make them a processor. Any cash transaction will not be undertaken by Nets but by Init.

- *PayIQ app*

The Pay IQ app is a mobile payment solution used by Föli to provide their users with a "Föli app". This application enables a secured payment to Föli's transport services, including the city bikes. The service is cloud-based. The Pay IQ company providing the service is processing personal data through its software product, which makes it a processor with regard to the GDPR. However, some delay in the implementation of the service makes this analysis difficult, in addition to the fact that Pay IQ might even be considered as controllers as they have their own customer registry.

- *Globeon*

Globeon is a Finnish company producing beacons and are subcontractors to Föli's marketing company Ulkomainosyhtiö Laulava Ovipumppu Oy. In the city bike case, Föli provides Globeon with a physical support to the small devices, namely the bikes: each bike carries one beacon. Globeon collects and stores the data emitted by the beacons and the information providing from the connecting Bluetooth. The service provided by the beacons is not necessary for the bike service as such and is not under the control of Föli, apart from the information that is transmitted through them. Globeon is responsible for the technology and its updates, and therefore they are their own controller. Föli is thus not liable for any incident that would occur through the beacon technology, and this should be made clear in the contract between Globeon and Föli.

3.2 Controller and processors' liability in accordance with the GDPR

Turku's city bike service involves several actors, Föli being the controller and for the others being for the most processors. The processor is, as much as the controller, bound by the legal requirements of the GDPR. The GDPR does provide how the relationship

between controller and processor has to be organized, as well as all parts of responsibility towards the regulation.

3.2.1 The relationship controller/processor

The controller is, according to the article 4(7) GDPR the authority determining the purposes and the means of the processing of the personal data. By this duty, the controller is also choosing the bodies processing the personal data on its behalf. The controller might indeed need other actors' services for the collection or the storage of the personal data; these actors are defined by the GDPR as processors.

The article 28 GDPR provides with the legal requirements for the relationship between the controller and the processor.

- *The processor is bound to the controller by contract*

According to the article 28(3) GDPR, the processor and the controller are to be bound by contract, in which the processor's activities have to be well defined. The article provides that *"processing by a processor shall be governed by a contract or other legal act under the Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and [the] duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller"*.

By this contract, the processor agrees to process the personal data *"only on documented instructions from the controller" [article 28(3)(a) GDPR],* and to ensure that *"persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality" [article 28(3)(b) GDPR]*

As to be compliant with the GDPR, Föli is therefore obliged to draft contracts with each of its processors taking into account these mentioned points.

- *The controller can only use processors compliant with the GDPR*

Although bound by contract, the controller needs to ensure that it is solely using processors compliant with the GDPR. As stated by the article 28 (1) GDPR, *"where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements*

of this Regulation and ensure the protection of the rights of the data subject." In other words, the controller cannot choose anybody to process personal data, but needs to make sure that the chosen processor will follow its instructions and process data in accordance with the GDPR.

By pointing out in detail the elements to be included in the contract between processors and controllers, the article 28 of the GDPR does not only give liability to the processors, but also to the controller. While the processor performs the processing tasks, the controller is legally bound to dictate the processing activities and monitor the good compliance with the regulation.

In the situation at hand, Föli is to monitor the processing of personal data involved in the city bike project, and overview all the activities undertaken by its subcontractors.

3.2.2 The legal requirements incumbent on the controller

The GDPR provides with several obligations incumbent on the controller alone.

- *The contract and the record of processing activities*

As mentioned in the previous section, the controller has to choose a processor compliant with the requirements set out in the GDPR. Once chosen, it has to draft a contract defining in detail the handling of the personal data. The controller will be the sole authority instructing the processor on the processing activities.

The article 30 GDPR also directs the controller and the processor to keep a record of the processing activities, listing what personal data is processed, how and by whom, as well as the contact details to the controller and the processor.

- *Guarantor for a lawful processing of personal data*

Alone, the controller has the liability to guarantee compliance of the processing activities with the GDPR. The article 5(2) states that "*the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1*", namely the five principles relating to the processing of personal data[32]. For this purpose, it shall implement measures and tools so that it can ensure and demonstrate this compliance.

[32] See section 4.1.2

The article 24 (1) GDPR states that *"taking into account the nature, scope, context and purposes or processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."*

On the grid of liability, the controller is placed above the processor. This article gives the controller additional obligations incumbent to itself, as it should be able to prove that all processing of data is performed in accordance with the GDPR and protects personal data.

- Appropriate technical and organisational measures

To counter the level of risks and ensure a safe processing of personal data, the controller shall ensure compliance with the GDPR by implementing *"appropriate technical and organisational measures" [article 24 GDPR]*. In other words, it is the controller's responsibility to adopt and decide the way the personal data will be handled. The Recital 78 provides with more explanation on the notion of "appropriate measures" by stating that *"such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features."*

The list is non-exhaustive and reviews and updates should be considered very seriously, as stated in the article 24.

Föli, being the controller in the city bike project, should always be aware of what kind of personal data is processed, what way and for how long. It should keep in mind possible updates and systems to improve the security for the processed data.

- Assessment of the risks

The possible risks and the likelihood of these risks for the rights and freedoms of the data subjects should be evaluated. This evaluation needs to be performed in order to implement the right measures corresponding to the level of the risk. Undeniably, the

existence of a risk and its severity are to be considered when defining the responsibility of the controller and the measures to be adopted for the processing of the personal data.

It is up to the controller to assess the risk.

The Recital 75 provides with examples on the possible risks which may result from personal data processing. The list is long and covers all kinds of damages, physical, material and non-material, such as *"where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data"* or *"where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles"*.

The risks' severity can vary from very high to low. Where a type of processing is likely to result in a high risk, the GDPR states that the controller should carry out a "data protection impact assessment" *[article 35 (1) GDPR]*. The high-risk processing activities are those using new technologies, systematic and extensive evaluation or personal aspects relating to natural persons which is based on automated processing; processing on large scales of special categories of data, such as, i.a., genetic data or data revealing ethnic origin; and the activities requiring systematic monitoring of a publicly accessible area on a large scale.

The processing activities of Föli do not appear to include any high-risk processing activities, and do not either present a high risk to the rights and freedoms of the data subjects. However, personal data are processed by Föli, although they are not "special categories" of data; still they require careful attention and adapted security measures such as encryption, safe storage and data minimization[33].

3.2.3 The legal requirements incumbent both on the controller and on the processor

Together with the processor, the controller shall ensure that all necessary measures are adopted to guarantee a sufficient level of security for the personal data.

[33] The possible solutions for secured data processing methods are analysed in the chapter V.

As provided by the article 32 GDPR, *"Taking into account the state of the art, the costs of implementation and the nature, the scope, the context and the purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."*

The risk having been evaluated, the controller shall then ensure that the processor has implemented enough measures and tools for a secure processing of the personal data. It shall also make sure that the tools are regularly updated, and that the processing instructions are followed and respected by any person acting under the authority of the processor.

The pseudonymisation and the encryption of personal data, the testing of the effectiveness of the technical and the organisational measures, the ability to ensure confidentiality and resilience of the processing systems and the ability to provide with a backup to personal data in the event of a physical or technical incident are all measures provided in the article 32 GDPR as appropriate for secure processing. According to this article, they should be taken into account both by the processor and by the controller.

In the city bike project, the data becomes personal once it reaches Föli's databases, as Föli combines all the data belonging to one data subject. GPS data, previously only showing a route, is in Föli's database put together with the identity of the user. It is therefore very important that Föli's internal system provides with the best security features, that these features are regularly tested and updated and that the data contained in Föli's servers is protected.

3.2.4 The legal requirements incumbent on the processor

The processor processes personal data on behalf of the controller. As presented above, the relationship between the controller and the processor is governed by a contract, which should stipulate *"the subject-matter and the duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller." [article 28 (3) GDPR]*

- *Approved code of conducts and certification*

The processors used by Föli should provide with sufficient guarantees as to ensure that all data processing follows the requirements of the GDPR *[article 28 (1) GDPR]*. Although it is Föli's obligation as a controller to make sure their processors are compliant with the regulation, the processors need to follow certain rules.

As referred to in the article 28 (5) GDPR, processors can demonstrate compliance with the regulation by adhering to approved code of conducts or approved certification mechanisms. These approved codes of conducts and certifications are based on international standards and are issued by certification bodies, as specified in the article 43 GDPR. IAPP[34] for instance organizes exams accrediting GDPR certifications to organisations.

In the bike project, none of the processors have adhered to an approved code of conduct or to an approved certification relevant to the GDPR. However, some have a privacy policy which ensures the protection of personal data. Pay IQ [35] has a code of conduct and a privacy policy but there is made no mention of the GDPR. Nets [36] are aware of the GDPR and they ensure compliance with the Regulation, however without having an official GDPR certification. Nextbike Polska s.a [37]does also have a privacy policy, but it does not mention the GDPR. Init[38] has a privacy policy, listing all the possible event where they might process personal data. Western Systems are in the course of drafting theirs.

- *Process based on documented instructions from the controller*

Based on the article 28(3)(a) GDPR, the processor shall *"process the personal data only on documented instructions from the controller"*. It is thus tied to respect these instructions, and it could be held liable if they were not respected.

[34] IAPP refers to the International Association of Privacy Professionals, more information available at: https://iapp.org/

[35] Pay IQ's privacy policy available at https://payiq.net/en-us/pol_privacy.html

[36] Nets'" privacy policy" or GDPR page, available at https://www.nets.eu/Pages/GDPR.aspx

[37] Nextbike Polska S.A's privacy policy available at https://nextbike.pl/wp-content/uploads/2017/02/Privacy-Policy-Nextbike-Polska-S.A..pdf

[38] Init's privacy policy available at https://www.initse.com/ende/us/footer-meta/privacy-policy.html

This article also provides Föli, as a controller, with the obligation of indicating all processing instructions to the processors working in their behalf.

- *Removal of personal data*

The article (article 28(3)(g)) also provides the processor with the obligation to delete or return all the personal data to the controller after the end of the provision of services relating to processing. This obligation implies good organisational measures from the processor's side in order to be able to retrieve all the data in a timely manner.

Turku's city bike system is controlled by Föli and englobes six other players acting as processors. Both the controller and the processors have defined responsibilities towards the GDPR so that personal data is processed lawfully and in accordance with its original purpose.

IV. THE GDPR REQUIREMENTS APPLICABLE TO FÖLI'S CITY BIKES

4.1 The notion of "processing"

The notion of processing is at the heart of the GDPR. It encompasses a wide range of activities and the controller needs to follow defined rules in order to make the processing lawful.

Processing personal data is what the GDPR is all about and as such, it considers protecting the processing of personal data as a fundamental right. The regulation therefore frames all the processing activities by defining them, as well as the actors performing the processing. The article 4 is aimed at defining all the notions inherent to the protection of personal data, and states in the paragraph 4 that processing *"means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."*

This article encompasses what seems to be all the activities which could be performed with data, sometimes at the great desperation of the IT professionals. In general, the GDPR provides with stricter rules than previous data protection tools. The idea is however pretty simple: as soon as personal data concerning a natural person is handled by someone else than the data subject, this handling, or "processing" should follow the requirements of the GDPR.

The processed data should belong to a living natural person *[recital 27]*. The text also makes clear that the natural person could be of any nationality and reside anywhere, even outside the EU *[recital 14]*, and that the data holder should be identifiable *[recital 26]*. The regulation is not applicable to the processing of data concerning legal persons *[recital 14]*. The processing of personal data needs to have a connection with professional or commercial activity, without which it is considered as personal activity and therefore not covered by the regulation.

The city bike project controlled by Föli consists of processing personal data concerning natural persons, namely names, home addresses, phone numbers, bank account details and GPS locations, as it involves the personal data of the bike users being collected through several means; them being stored; possibly consulted from time to time and likely erased after a set period of time. These reasons lead to affirming that the GDPR is applicable and should be respected by Föli and all the processors involved in the city bike project.

4.2 The features for lawful processing

The notion of processing within the GDPR is particularly framed. Two articles refer to it, namely the article 5, which states the principles relating to processing of personal data, and the article 6 determining the lawfulness of processing activities.

The article 5 states six processing principles:

4.2.1 Fair and transparent processing

The first paragraph of the article 5 provides that "*personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*". The notion of *fair processing* is already a fundamental right with regard to the article 8(2) of the European Charter of Fundamental Rights, and as referred to in the Directive 95/46/EC. However, it goes differently with the notion of *transparency*, which is merely mentioned in the recital of the repealed Directive. However, the notion of transparency is much stronger in the new regulation and could even be considered as a requirement. Although no legal definition is made of the notion, the recital designs it as: *"It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right*

to obtain confirmation and communication of personal data concerning them which are being processed[39] *…"*

The idea of transparency appears as a logical suite of the user-centred principle held by the GDPR, i.e. the natural persons and data subjects should have control over their personal data. Transparency would give control, as the data subjects would know by whom and for what purpose the data concerning them is used.

The Article 29 Working Party (hereinafter WP 29) identifies[40] three areas of application of the principle of transparency. Shall be transparent "(1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights".

Transparency refers to the way communication with the data subject is handled, and therefore all information inherent to the processing of personal data needs to be easily obtained. The article 12 GDPR provides that the information relating to processing should be given to the data subject:

- In a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- Free of charge;
- In writing, by electronic means when appropriate, and even orally, if requested so by an identified data subject

As an example, the data protection WP 29 identifies in its guidelines a set of phrases which are not considered transparent enough and therefore should not be used in any communication with a data subject:

- ""*We may use your personal data to develop new services" (as it is unclear what the services are or how the data will help develop them);*
- *"We may use your personal data for research purposes" (as it is unclear what kind of research this refers to); and*

[39] Recital §39

[40] WP 29, Guidelines on transparency under Regulation 2016/679, 2017

- *"We may use your personal data to offer personalised services" (as it is unclear what the personalisation entails)."*

It is recommended to use active form in writing and avoid circumstantial qualifiers such as "might", "may", "some", "possible" or "often". That way the information should be straight forward and give the data subject knowledge on the processing of data concerning her.

1. Specific purpose

The notion of specific purpose refers to the collection of personal data. The article 5 (1)(b) GDPR refers to the processing purpose as a principle, stating that the data should only be collected "*for specified, explicit and legitimate purposes*" and that all processing that follows should respect these purposes. This notion is not new: it was already a principle in the latter Directive 95/46/EC; it is mentioned as a crucial factor for data protection in the Convention 108[41] signed in 1981; and it is considered as a key for a lawful processing by the European Union Charter of Fundamental Rights[42].

a) Same or compatible purpose throughout the processing of the personal data

The purpose of processing defined in the beginning of the processing activity needs to remain the same or compatible with the initial one throughout the whole processing of that data. For example, if a data subject's address is collected as a detail for payment, the processor cannot use this address to send advertisement or use the address for city planning purposes. In order to use the data subject's address for several different purposes, the processor needs consent. The initial purpose needs to be respected and all further processing should not be processed in a manner that is incompatible with it. Exception is however made for "*archiving purposes in the public interest, scientific or historical research" [article 5 1(b) GDPR],* which are considered compatible with the initial purpose, under the condition that they are subject to "appropriate safeguards" *[article 89 (1)].*

[41] See the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1981. This convention, among other instruments from the Council of Europe, is considered to be one of the pillars of the data protection law as we know it today.

[42] See article 8 of the Charter:"*[…] [personal] data must be processed fairly for specified purposes"*

The WP 29 issued an opinion on purpose limitation in 2013 based on the previous directive 95/46/EC. The latter directive already put great importance on purpose limitation, and the WP 29 even considers it as "*an essential first step in applying data protection laws and designing data protection safeguards for any processing operation*[43]". Although the opinion bases its reflection on the repealed Directive and no other opinion has been issued after the adoption of the GDPR, it is likely that the listed advice still are applicable.

In its opinion, the WP 29 identifies several aspects of purpose limitation. Firstly, the purpose needs to be specified prior to, or at the latest at the time of the collection of the personal data. In the case of Föli, it is important that the bike user is kept aware on the purpose of the collection of her data.

Second, the purpose needs to describe what kind of processing will be performed on the collected data. For example, it should clearly state whether the data will be used for payment purposes, or whether the data will allow the system to send advertisements. The purpose could also state what kind of processing is not performed on the data. The opinion considers that purposes such as "'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research'" -without more detail- would be too general and not sufficiently clear for the principle of purpose requirement.

In the case at hand, Föli collects the bikes' GPS coordinates and stores them in its server. At this point, it would be worth reflecting on the reason for storing this identifiable GPS data and whether it would be necessary at all. In case it is considered necessary, the reason for this processing should be clarified to the bike user. For example, Föli could consider that the collected GPS data could improve their services and thus 'the users' experience'. It might therefore be worth describing the purpose of this collection by stating, for example, that "GPS data, after having been minimized (as Föli's intention is to make the GPS data as anonymous as possible), will be collected and used for city planning purposes by analysing the most popular bike routes used".

[43] See WP 29 Opinion 3/2013 on purpose limitation (WP 203), p. 4

b) Additional safeguards in case of purpose change

In theory, a set of data is collected for a specific purpose or set of purposes. Yet, this purpose might come to evolve or change if the controller decides, for example, to add a new service to its business model. In this scenario, the controller cannot assume that the data subject's consent is automatically transferred to the new use of data. The first consent obtained by the data subject only applies to the initial purpose or set of purposes, and if a new service involves a new purpose or set of purposes, the controller should make sure to obtain a new consent. The WP 29 refers in these case to "additional safeguards" which the controller should use, requesting informed consent from the data subjects for the new purpose.

For example, let's consider a company selling flowers through a mobile application. Users can purchase flowers and get them delivered to the address they indicate on the mobile payment bill. At this point, the company processes the user's address and possibly their name to deliver the flowers. After a while, the flower company decides to evolve their service and use the users' mobile GPS and the phone number provided in the bill to send pop-up notifications on the different sorts of flowers they can find on their way. In this case, the initial purpose of selling and delivering flowers has evolved. The flower company should request the users' consent for processing the GPS data and sending the notifications.

c) Purpose needs to be described in detail by the controller to all processors

As stated in section 3.2.2, it is the controller's responsibility to ensure that the purpose is well-defined, that the subject-matter and the duration of the processing are established as well as "*the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller*." *[article 28 (3) (a) GDPR]*. All these descriptive details need to be agreed upon and written down in the contract signed between the controller and the processor.

It goes without saying that the processor needs to respect the purpose limitation defined by the controller and described in the contract. The processor is only to process data based on the documented instructions given by the controller.

4.2.2 Adequate, relevant and limited

According to the third paragraph of the article 5 GDPR, the data shall be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*. The article refers to the notion of "data minimisation", which is an underlying principle in the whole regulation, together with purpose limitation.

The core idea behind data minimisation is to implement data protection already before the data is being processed. By limiting the amount and the nature of the data collected, the risks would shrink, as only the necessary data for the initial purpose will be processed. For example, a company selling flowers would only process data relating to the shipment address, and does not need to collect the date of birth or the marital status of its customers.

a) Data minimisation in the age of big data

Although this paragraph could potentially be the title of a whole thesis, it merely aims at identifying why many scholars vividly criticise the principle of data minimisation in the GDPR. Big data refers to the collection of massive amounts of data for a future analysis. One of the ideas behind it is to allow for an analysis based on a large variety of information, thus providing with a complete research result. Tene and Polonetsky[44] provide a good example of a successful big data approach, namely the Google Flue Trend. The Google Flue Trend used to be a web service operated by google and analysing the influenza activity in 25 countries all over the world. The aim was to predict flu outbreaks by analysing queries filled by individuals. The IP address of the queries were then identified and permitted their localization. However, although the web service was considered to support public health, the privacy concerns and the lack of transparency on the methods used were considered too important for the service to be continued[45]. Still, during the five years it was operational, it gathered 50 million queries a week, which makes it a good example of big data analysis.

[44] O. Tene and J. Polonetsky, Privacy in the age of big data, A time for big decisions, Feb. 2012

[45] See article in the New York Times, M. Helft, Is There a Privacy Risk in Google Flu Trends?, nov. 2008, available at: https://bits.blogs.nytimes.com/2008/11/13/does-google-flu-trends-raises-new-privacy-risks/

Yet the GDPR tends to follow the minimalism rule of art that "less is more". This trend is in fact rather logical, keeping in mind that the bigger the amount of the processed data, the larger the security measures and the organisational measures. The articles of the GDPR thus essentially encourage the collection of specific data, and not large amounts of information. Following this logic, data minimisation does not appear to go hand in hand with big data trends, and it could therefore be concluded that the GDPR might not be well designed for big data analytics.

b) Föli and data minimisation

In the case of Föli and the city bikes, the amount of data needed is not what so ever comparable to large scales such as Google's Flu Trend. The information necessary for any services undertaken by Föli is quite focused and serves specific aims. Föli needs the bike user's name and address for billing purposes, as well as the user's bank account details, although the latter are handled by secured mechanisms operated by Nets. They do also need the user's status, for example whether she is a student or whether she is retired, in order to provide with discounts. All this personal data is necessary for lending out bikes. Let's imagine that Föli were also to ask the user of her place of birth or for her marital status. Neither of these sets of information are necessary nor relevant for renting a city bike, and would therefore go against the principle of data minimisation.

The principle of data minimisation confers a duty to Föli's service designer to measure the amount and the nature of the data needed; and to evaluate which personal data is necessary in order to perform the service.

4.2.3 Accurate

The article 5(1)(d) GDPR requires that the data processed should be *"accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')"*.

This provision quite clearly allocates administrative duty to the controller and to the processor to keep the personal data registers under control, permanently. It implies that

the processed personal data should be monitored regularly, so that it is accurate and kept up to date; and if it is not considered necessary anymore, rectified or deleted.

Accurate data refers to data that is correct and which corresponds to the individual it is linked to. Any company in need of personal data usually requires this data to be true so that the individual can be contacted, for example. However, personal data can sometimes change; in the case of a name change, or when a person moves to another address, and it becomes then important to update the data stored in the service's database. Commonly, the data holder should inform the company on this change of personal data, and the company should then make the effort to retrieve the inaccurate data and correct it or delete it.

A case study of 2015[46] investigated by the Irish Data Protection Commissioner illustrates a bank's failure to rectify personal data, leading to the disclosure of confidential information to third parties. In this case, a bank customer requested his bank, the Allied Irish Bank, to update his address. The demand, although repeated several times, was not answered, and the bank continued sending mail to the customer's previous address. The unknown third parties residing at the previous address thus received confidential information intended the customer. The Commissioner decided that the bank had failed to take appropriate security measures and reminded of the importance of keeping personal data updated at all times.

This provision does also have an underlying obligation in keeping all the personal data well organised in the system. Keeping in mind that the data holder gets the rights, according to the article 16 and 17, to rectify and erase data; and according to the article 20, to data portability, it is clever to organise the personal data in a way which facilitates its access.

Föli is in a favourable situation as the city bike project is new and that no bike user's data has just started to be processed. Föli thus has the possibility to organise the

[46] Data Protection Commissioner, Case Study 2015*, Failure to update customer's address compromises the confidentiality of personal data*, available at: https://dataprotection.ie/viewdoc.asp?DocID=1620&ad=1#201511

processed data so as to facilitate its access, and thus its possible rectification and future deletion.

4.2.4 Defined storage period

The 5th paragraph of the article 5 GDPR concerns the amount of time personal data should be stored. It states that data should be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed"*. In other words, personal data should be kept for the strict maximum of time required by the purpose. For example, let's imagine that a museum collects the visitors' phone number in order to send informative text-messages during the museum visit. In this scenario, the museum needs to delete the phone numbers once the visitors have left the premises of the museum. The initial purpose of the processing was to send information, not to be able to contact the visitors later nor to send advertisement (unless the museum asks the visitors for permission to do so).

This paragraph concerns all kinds of processing activities which enable the identification of data holders, and not only the 'storage' of the data. The processing time could last from a few minutes to several years, depending on the purpose for which the data is used.

Exception is however given to data stored for archiving purposes "*in the public interest, scientific, historical research purposes or statistical purposes in accordance with Article 89(1)*" (relating to archives), in which case personal data can be stored for a longer time than the initial purpose.

In the city bike system, Föli is not processing personal data for archiving purposes. They therefore need to make sure to delete all personal data which is still available after the initial purpose has ended. For instance, the bike user's information should be

deleted from the Föli database once the user cancels her subscription. The Finnish law [47] does not provide any other timeframe.

4.2.5 Appropriate security measures

The last paragraph concerns the security features concerning the processing of the personal data. It states that personal data shall be *"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*". This provision is stated as a principle, and can be read together with the article 32 referring to the "security of processing" and asserting that *" [...] the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [...]"* A more detailed analysis on the possible security measures available to Föli will be made in the fifth section.

The first part of this section aimed at identifying the 6 main principles concerning processing of personal data. The controller, in this case Föli, is held responsible for ensuring that these principles are respected, and should therefore take all necessary safeguards in order to guarantee that.

4.3 The notion of "consent"

The GDPR requires obtaining consent before processing personal data. This consent mechanism is subject to several modalities and the controller should make sure that the consent is lawful.

[47] See the paragraph 34 of the law on personal data 22.4.1999/523 "Henkilörekisteri, joka ei ole enää rekisterinpitäjän toiminnan kannalta tarpeellinen, on hävitettävä, jollei siihen talletettuja tietoja ole erikseen säädetty tai määrätty säilytettäviksi tai jollei rekisteriä siirretä 35 §:ssä tarkoitetulla tavalla arkistoon".

4.3.1 Consent is one of the lawful grounds for processing personal data

The obtention of consent has a core importance in making the data processing lawful. Consent is not an obligation, as processing could be performed without it in specific cases, but in the event that the processing is not necessary for some contractual or legal obligation, the obtention of consent from the data subject is mandatory. The notion of consent presented by the GDPR has evolved since the latter Directive 95/46/EC, yet it remains one of the six lawful grounds for processing personal data, among others listed in the article 6 GDPR.

The processing of personal data is thus lawful either when consent has been obtained from the data holder, or when the processing is necessary for:

- *"the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
- *compliance with a legal obligation to which the controller is subject;*
- *protecting the vital interests of the data subject or of another natural person;*
- *the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
- *purposes of the legitimate interests pursued by the controller or by a third party […]"*

Although all provisions' scope seem quite clear, it goes differently with the last one. A wave of legal debate has arisen in interpreting the notion of 'legitimate interest', which, according to the last bullet point, could constitute a lawful ground for processing personal data without obtaining consent. This provision catches attention as it would offer an "easier" way to process personal data, without requesting consent. Although 'legitimate interests' are widely used as lawful grounds for processing in crime or fraud prevention[48], their utilization is still legally monitored. To start with,

[48] More examples on legitimate interests available in the discussion draft by the Center for Information Policy Leadership (CIPL), 2017, available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_16_march_2017.pdf

the processing of personal data needs to be necessary and proportionate to the purposes of the legitimate interests. The requirement of 'necessity' implies that if the interests of the controller can be pursued in any other way, they should, by for instance obtaining the data holder's consent.

Furthermore, 'legitimate interests' is also explained and limited in recital 47. It states that processing on the basis of legitimate interests could only be lawful:

- if "*the interests or the fundamental rights and freedoms of the data subject are not overriding*";
- when the processing is not performed "*by public authorities in the performance of their tasks."*

In other words, legitimate interests seem to be used as lawful processing grounds if they are necessary and proportionate, if the fundamental rights of the data holders are not overriding and when processing is not performed by public authorities. As discussed among the Center for Information Policy Leadership, most of the examples lawfully grounding their processing on 'legitimate interests' are anti-fraud purposes or crime prevention, anti-money laundry watchlists and other preventive and detection services.

Föli is under obligation to request consent from the bike users in order to process their personal data. The contractual bike hiring service does not justify processing on the grounds of 'the performance of a contract', as personal data is not actually necessary for renting a bike (compared to services where the actual service consists in processing personal data). No legal obligation, public interests or vital interests of the data subject are either applicable in this case. Nor is legitimate interests, as Föli cannot possibly argue that their need to process all the bike users' personal data is clearly more important than the fundamental rights of the client.

4.3.2 Definition and features for a valid consent

Despite not being a novel principle, the GDPR defines consent in the article 4 (11) as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

According to this definition, the data holder needs to give a free, specific, unambiguous and informed consent. All these conditions have to be met. The WP 29 makes a thorough study on each element constituting valid consent in their guidelines on consent, starting with the notion of 'free consent'.

Freely given

The data holder's consent needs to be freely given, without impeachment of any kind. The data holder should have real control over her personal data and she should not feel obligated to give her consent. Recital 43 provides additional explanations on 'free consent'. There is no free consent if the consent cannot be separately given to distinct sets of processing operations where these operations could actually be consented for individually. For example, if a flower company requires consent for processing the client's address for flower delivery, it should not include in the same consent mechanism the right of processing the client's GPS data for notifications not linked to the flower delivery. The data holder should in this case be able to consent to the processing of her address separately from the processing of her GPS data.

There is not free consent either if a service is dependent on consent and consent is not actually necessary for that kind of performance.

The notion of free consent is also linked to the concept of personal autonomy. As Rawls [49]describes it based on an argument held by Kant: "*a person is acting autonomously when the principles of his action are chosen by him as the most adequate possible expression of his nature as a free and equal rational being*". In other words, a person would give free consent and be autonomous when he bases his decision on his own perception. A data holder should thus give her consent and tick the box when, after reflexion, she considers that she is willing to share her personal data for this specific purpose. By doing so, the data holder gives the authorization to the controller to process her personal data. This authorization should be given autonomously and should not be forced, thus constituting a free consent.

The concept of personal autonomy also calls back to the right to 'informational self-determination', where the data holder has the right to choose how, when and what

[49] J. Rawls, The theory of Justice, Oxford University Press, 1973

personal data will be processed. Strictly speaking, it is the same notion as the empowerment of data subjects that the GDPR is striving for. As stated in the very beginning of the regulation in Recital 7, *"Natural persons should have control over their own personal data*", and free consent might just be the first condition for fulfilling it.

In practice, free consent is obtained by giving the data holder the possibility to read the purpose for the personal data processing as well as the different conditions relating to it. Consent can be obtained orally or by writing. In the case of Föli, it seems more likely that consent will be given by writing, and therefore two elements have to be respected:

- ✓ Föli can request the data subject to tick a box, as a sign for approval after having read the purpose and the conditions
- ✓ Föli should allow the data subject to check and set the technical settings. This is a way of obtaining consent for separate purposes than the initial one, for example acquiring the authorization to send news to the data subject's email address.

No box should be ticked by default, and no technical settings should be agreed upon by default. Silence and inactivity do not count either as acceptance by the data holder since that would go against the principle of free and autonomous consent.

Specific

Consent needs to be specific to one or several purposes, as provided by the article 6(1). The aim of this specificity is to ensure transparency of the data processing, so that the data subject knows for what purpose she has consented to provide her personal data. It implies that the controller specifies in detail the purpose, both to the data holder and to the processors. It also means that the purpose or the set of purposes need to be respected, and that in the event that the purpose changes, a new consent is requested from the data holder[50].

[50] See "Additional safeguards in case of purpose change" in section 4.1.2

Informed

Consent has to be informed. This requires that the data subject gets access to information relating to the processing of her personal data, namely the purpose of the processing, as well as the circumstances under which it will be processed: what kind of data, for how long it will be processed, where and for how long it will be stored… The right to information goes hand in hand with the principle of transparency defined in the article 5 and in the section 4.1.2 of this paper.

The WP 29 identifies six pieces of information that need to be made available to the data subjects, of which four are applicable to Föli, namely:

- the controller's identity
- the purpose of each operation for which the specific consent is requested
- the kind of data which is processed
- the data subject's right to withdraw consent

The GDPR lets understand that any format for this information is possible, such as written and oral statements, as well as video or audio messages. Recital 32 and the article 7(2) provide thorough indications on how to inform the data holder. First, seeking consent should be done in "*a manner which is clearly distinguishable from the other matters*", which means that the information relating to the processing operations and the boxes to be ticked need to be well put forward. Second, this information should be forwarded in "*an intelligible and easily accessible form, using clear and plain language*" or as Einstein stated, "*if you can't explain it to a six-year old, you don't understand it yourself*.". This does naturally apply to the way the information is provided, it could for example be clever to avoid a lot of small and compact text to be read from a mobile device.

The aim of having an informed consent is to make sure the data holder knows what she is consenting to. Yet, a problem has been identified as to know how 'real' the consent actually is in practice. Numerous studies have come to the conclusion that although the law requires consent mechanisms to be put in place, many are the data holders who give their consent without acknowledging what they are consenting to. Basically, they are ticking the box and scrolling down for a fast access to the wanted service. Legally, consent may still be given, but how is this consent perceived from a moral point of view? This issue questions the efficacity of the consent mechanism as

we know it today, and hopefully tickles the imagination for new ways of informing the data subjects and catching their attention.

Unambiguous

Finally, the consent needs to be unambiguous in order to be valid. It means that the data subject needs to give its authorization for processing her personal data by "*a statement or a clear affirmative act*", as indicated in the article 4(11) GDPR. Even though the best way of obtaining affirmative consent would be to get a written statement by the data subject writing what she is consenting to, this method seems unrealistic, as indicated by the WP 29. It would thus suffice with a box to tick after the enouncement of intelligible and easily-understood terms and conditions.

Electronic means

Föli will most likely obtain consent and inform their bike users on the existing terms and conditions by electronic means. These means are specially considered by the GDPR. For instance, as provided by Recital 32, if consent is requested through electronic means, "the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided." In other words, Föli has to make sure that consent is requested, and in this precise case of city bikes, that it is made sure that the data subject's attention is caught. The WP 29 makes clear that the GDPR approves of physical motions as clear affirmative actions, such as for example "turning a smartphone around clockwise". However, just scrolling down do not count as an affirmative action as it is too easy and therefore could be unambiguous.

Valid consent requires several different elements, which all have to be respected. The subject of consent is of particular importance within the GDPR, as it is the tool through which control is given to the data subject on the processing of her data. The rules to follow for companies, and in particular Föli, are therefore quite precise and practical indications can be given. The concept of explicit concent was not described in this paper as it does not concern Föli[51].

[51] Explicit consent from the data subject is only required in specific cases when specific categories of data are processed, when data is transferred to third countries or international organisations without additional safeguards or when processing is performed by automatic decision-making, including profiling. See the article 9 GDPR.

4.4 The notion of "storage"

Storing information is considered as one way of processing data. It therefore has to be legally framed, and it is under the responsibility of the controller. The mode of storage, either on the controller's or the processor's own physical server or in a cloud, need to be chosen and respected throughout the processing of the data.

Föli intends to store the collected personal data in a physical server in Turku.

The GDPR keeps silent on the methods of storage to be used and the best ways to keep them secure. However, the French CNIL provides with guidelines[52] for secure storages, in particular for physical servers. The CNIL recommends that:

- Access to the server should be limited to special staff. The CNIL recommends that the servers should only be accessible by authorized staff, including the servers' tools and interfaces.

- Updates should be carried out regularly. The CNIL suggests an automatic update scanner every week.

- Passwords should be considered seriously and changed regularly, especially when staff members are changing.

- Safeguards should be performed regularly. The GDPR provides in the article 32(1)(c) that the controller and the processer shall ensure *"the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident"*. In other words, there should be a backup if the server fails.

[52] Guidelines on securing physical servers by CNIL available at: https://www.cnil.fr/fr/securite-securiser-les-serveurs (in French)

- Cryptography should be considered as a good means of securing the server network. CNIL recommends using 'Transport Layer Security' (TLS), in replacement of the nowadays prohibited SSL (Secure Sockets Layer). The aim of TLS is to guarantee good privacy security between communicating computer applications.

The CNIL disapproves on using unsecure services and on using the host server for other uses than the management of the stored data.

The management of data storage is not very well documented, yet it is considered as an act of processing personal data and is therefore to be taken seriously. Storage, in addition to being secure, should also be well organized in order to allow quick access in order to ensure the rights of the data subject.

4.5 The rights of the data subject

The GDPR is innovative in the fact that it strives to provide the data subject with as many rights as possible in order to keep control over her personal data. As stated in Recital 7, "*natural persons should have control over their own personal data*" and this control results from a set of rights provided by the regulation. This section identifies the rights and the provisions relevant to Föli.

4.5.1 Right of access

First, the data holder needs to be informed whether personal data concerning her is being processed. This information should be given by the controller, who also should give access to the personal data. The article 15 states that the controller should inform the data holder on:

- "*the purposes of the processing*";
- "*the categories of personal data concerned*";
- the recipient of the personal data;
- the period of time during which the personal data will be stored "*or, if not possible, the criteria used to determine that period*";

- "*the existence of the right to request from the controller rectification or restriction of personal data or restriction of processing or personal data*";
- The possibility for lodging complaints with a supervisory authority, in Finland the supervisor authority being the data protection Ombudsman (Tietosuojavaltuutettu),
- The source of the personal data, in the event that it has not been collected from the data holder,
- The existence of automated decision-making, if any.

The right to access does in practice give the data holder the right to obtain a copy of the personal data being processed. This copy could be delivered in paper or through electronic means. Although the content of the information is practically similar, the right to access is different from the consent mechanism and the notion of 'informed consent'. The right to access is actually to be considered as a fulfilment of the principle of fairness and transparency, as it enables the data holder to review the data that is being processed and under which circumstances. The request for information occurs while the data is being processed, not before, as it is the case with the information contained in the terms and conditions and to which consent is given. The Recital 63 tells that the aim of giving the data subject access to her processed personal data is to give her the possibility to be aware and to verify the lawfulness of the processing. In other words, giving her control over personal data concerning her.

All communication for the exercise of the right of the data holder are subject to certain rules, as submitted by the article 12. The article 15 on the right of access is one of them. The article 12 states that:

> 1) the controller shall always communicate with the data holder "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*";
>
> 2) the controller shall not hinder the exercise of the data subject's right to access;
>
> 3) the controller has one month to answer to the data subject's requests, either positively or negatively. However, if the controller is refusing to act on the

request, the "unfounded or excessive character of the request" should be well demonstrated.

This right to access of the data subject is however subject to one limitation, namely the rights and freedoms of others.

For Föli and for the city bike project, the right of access means that every bike user could request a copy of all personal data concerning her that is being processed, as well as all details presented in the article 15. After receiving a request, Föli has one month to provide the data holder with a copy, unless the request is unfounded or goes against the rights and freedoms of others, in which case Föli should inform the requesting data subject about its decision.

4.5.2 Right to rectification

It is conceivable that personal data changes during the time it is being processed. It is thus usually in the data subject's interest to rectify inaccurate personal data concerning her. The GDPR provides in the article 16 the right to rectification, giving the data holder the right to "obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her". The same goes for data that needs to be completed.

For example, a Föli user could move and thus her home address would be inaccurate. After request from the user, Föli should rectify the user's address in the database. A perfect example of a failed right to rectification is provided by the case law of 2015 investigated by the Irish Data Protection Commissioner and presented earlier in this thesis[53]. As of today, it appears that Föli's users are able to rectify their personal data directly through Föli's user platform.

4.5.3 Right to erasure or 'right to be forgotten'

Hot debates in Europe resulted in 'the right to be forgotten', especially after the case law *Google Spain v. Agencia Espanola de proteccion de datos ('Google Spain')* in 2014. This right is still controversial and its practical applicability is still raising vivid questions among scholars. In practice, the right to be forgotten or the right to erasure gives the right to a data holder to request total erasure of data concerning her without

[53] See section 4.2.3 on "accurate"

undue delay, as provided in the article 17 GDPR. The undue delay refers to a period of one month, as stated in the article 12(3). In the case *Google Spain*, The European court of Justice was questioned on the applicability of the Directive 95/46 to search engines, as a Spanish national wanted all information concerning him from his attachment and garnishment proceedings dated 1998 to be deleted from Google Inc, Google Spain and the newspaper La Vanguardia. The Court ruled that search engines operators should remove personal data if so requested by the data holder when this data has been published by third party websites. However, the data subject's right should also be balanced against the interest of the public.

The GDPR's article 17 respects this decision and defines a set of situations where the right to be forgotten is applicable. It does even go further by obliging the controller to inform all third parties of the data holder's request to be forgotten, in particular when the data has been made public *[article 17(2) GDPR]*. In Föli's case, the personal data should never be made public. Yet Föli, as a controller, should make sure that all processors are deleting the personal data concerning the requesting data holder.

Among all grounds listed by the GDPR, Föli should consider that the bike user has the right to erasure when:

- "*the personal data are no longer necessary in relation to the purpose for which they were collected or otherwise processed*": if Föli for example shut down the whole bike system, the bike users would get the right to demand the right to erasure, and delete all personal data concerning them from Föli's database.
- "*the data subject withdraws consent […]*": as clearly stated, if the data subject withdraws her consent, she can also request the right to erasure, obliging Föli to delete all data concerning her from their database.
- "*the personal data has been unlawfully processed*": if Föli has for example failed to obtain consent before processing personal data, the data holder could request the erasure of the personal data concerning her.

Yet, as ruled by the ECJ, there are a few limitations to this right. Föli can therefore not respond to the right to erasure when the processing of the data is necessary "*for exercising the right of freedom of expression and information", "for compliance with a legal obligation […] to which the controller is subject or for the performance of a task carried out in the public interest", "for archiving purposes in the public interest,*

scientific or historical purposes or statistical purposes" and "for the establishment, exercise of defence of legal claims". [article 17(3) GDPR] However, Föli still has the obligation to communicate its decision to the data holder, and explain the grounds for which they refuse to respond to the request for erasure.

4.5.4 Right to data portability

- The concept of data portability

The article 20 of the GDPR creates a new right in the data protection field, giving the possibility for data holders to "*receive personal data concerning her […] in a structured, commonly used and machine -readable format*". Once in possession of her personal data, the data subject can choose to transmit this personal data to another controller, or can directly request that the personal data be transmitted from one controller to another. Yet, this does not mean that the personal data is erased from the controller's database, and the data subject can continue to use the controller's services as long as her personal data is being processed by them. As pointed out by the WP 29, this right empowers the data subject with more control over her personal data. Data portability is aimed at supporting the free flow of data in the European Union and will tighten the competition between service providers. The GDPR prohibits controllers from hindering the exercise of this right and the transmission of personal data to another controller upon request.

The personal data subject to the right to data portability is the personal data that has been provided to the controller by the data holder. This includes any data which has been produced while using the service, as the WP 29 identifies as 'raw data'. For example, the GPS route linked and assembled to the data subject constitutes raw data and will therefore be subject to the right to data portability. The personal data does undoubtedly need to concern the requesting data subject only.

- Föli as a sending data controller

In the event that Föli need to answer to a right to portability, they should ensure that the data they are about to transmit corresponds to the data the data subject wants to transfer. For example, if a data subject wants to change her city bike provider, but still

keep Föli as a bus service, Föli should be careful to only transfer the personal data required for the bike service.

Föli would also need to make sure that all processors are cooperative to answer to the request. The WP 29 recommends implementing special procedures between the controller and the processors in order to easily answer to a right to portability. As for pretty much all the provisions under the GDPR, good organisational measures seem to facilitate many sets of operations, including data portability.

- Föli as a receiving data controller

In case Föli become the receiving controller, obtaining personal data from another controller on the request of a data holder, they become responsible for the new personal data. As with any personal data, they will have to respect the article 5 GDPR and its principles, namely fairness, lawfulness and transparency, data minimization, purpose limitation, integrity, accuracy as well as confidentiality, storage limitation and accountability.

For the purpose of data minimisation, Föli would have to ensure that the received personal data is relevant and limited to what is necessary for the purpose. The purpose will have to be communicated to the data holder before collecting her consent. All data received which is not considered as relevant to what is necessary to the city bike system should not be kept nor processed. As a matter of fact, Föli, as a receiving controller, do never have the obligation to accept all transmitted data resulting from a data portability request.

- Limits to data portability

The right to data portability does also contain limits. To start with, although the 'sending data controller' has no choice but to facilitate the exercise of this right and possibly transmit the portable data to another controller, the 'receiving data controller' can refuse to accept the data. That could be the case, for example, if the 'receiving data controller' considers that the data is not relevant to the service it is providing.

Second, the right to portability can only be performed if no other rights of other data subjects are prejudiced. No personal data belonging to a third party can be included in

the set of data to be transmitted, as this would hinder the third parties to exercise their right of access, for example.

- The way personal data is transferred in practice
    - Authenticating the requesting data subject

Before transmitting personal data, the controller needs to ascertain the identity of the requested data subject. While the GDPR is silent on the procedures to use in order to verify someone's identity, the WP 29 recommends that "*all requesting data subjects' identity should be controlled before handing over any personal data*". For instance, the controller can request additional information from the data holder, without however collecting too much additional personal information. Ideally, verification would be enabled through the already existing personal data, and authentication could be performed by using the user account, her username and password. A secret question for which the answer is known both by the controller and by the data subject could also be used.

Additionally to what WP 29 recommends, there also exist solutions for identity managements. Developed for instance by Microsoft[54] and considered by Lessig[55], identity managements are IT programs which enable the user to only give out the minimum necessary information needed. For example, if Föli would need to know whether the user is a student who would benefit from a discount, only that bit of information will be revealed. Such a solution goes further than merely authenticating the requesting data subject, as it also minimises the amount of data processed by the controller. The controller would thus be sure of the identity of the data holder and only get the minimum necessary information, which would ultimately increase security and privacy. As such, an identity management solution would already be an interesting security feature.

    - Time frame

As for the other rights of the data subject, the controller has one month to respond to a data subject's request, including data portability, as provided in the article 12(3).

[54] See Microsoft's Azure identity management technology, available at: https://www.microsoft.com/en-us/cloud-platform/identity-management

[55] See L.Lessig, Code 2.0, chapter on 'regulating code'

However, the WP 29 states that this one-month period can be extended to three months "*for complex cases, provided that the data subject has been informed about the reasons for such delay within one month of the original request*".

- Personal data formats

The article 20(1) indicates that the personal data being transmitted from the controller to the requesting data holder should be in a "*structured, commonly used and machine-readable format"*. Here again, the GDPR does not provide with a model of transmission which would ensure the interoperability of all systems, as that is most likely impossible. However, the WP 29 suggests using "*the most commonly used opened formats*", such as JSON, XML, CSV… to cite just a few.

- Secured transmission of personal data

Securing personal data might be one of the most challenging duties of the controller. Within the right to portability, this duty might even be more difficult to guarantee, as the controller needs to be sure to authenticate the requesting data holder.

The controller also needs to somehow transmit the requested data from a point A to a point B, from one server to another. There is made no mention of the methods to adopt, neither in the GDPR nor in the WP 29's guidelines. However, taking into consideration the controller's obligation under the article 5(1)(f) to ensure "*appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures*", it seems obvious that all means should be taken to transfer the data safely, for example by encrypting it and handing it out physically to the requesting data holder in a memory stick.

The data subject is given several rights under the GDPR, all aimed at giving her control over the personal data concerning her. Only the right to data portability is a 'new' right and possibly triggers the most questions and debates. The controller should make sure that these rights can be exercised by the data holder. Among all these rights, the right to object does not appear to be an applicable right in the case of Föli, as it is only applicable to situations where data processing is necessary "*for the performance*

of a task carried out in the public interest" or "for the purposes of the legitimate interests pursued by the controller" *[article 21(1) GDPR]*.

V. POSSIBLE SOLUTIONS FOR ENHANCED PRIVACY SECURITY IN THE CITY BIKE SYSTEM

Protecting personal data is what the GDPR is all about. Several security methods exist, but no clear policy provides a clear methodology on how to efficiently protect personal data. This chapter aims at analysing the most common security techniques and the most convenient ones for Föli.

5.1 The reasons for adopting security solutions

Before analysing the different methods, it is worth understanding why such methods should be considered and possibly adopted. Nowadays, data is rarely collected to be used once, and same goes with personal data. The controller is required to have a clear and defined purpose for processing personal data, yet additional purposes such as research, real-time information and statistics could also benefit from this data. For this reason, it would be convenient to obscure the elements enabling the identification of an individual, and only keep data which does not require any data protection.

Föli has shown interest in these methods as they have plans to adopt a smart grid based on a heat map capable of showing the most used traffic routes in real time. For that purpose, they would require real-time GPS data from the bike users.

However, managing and protection all the personal data relating to the real-time behaviour of the users can be challenging, and the controller has a big responsibility in doing so. The GDPR summons the controller and the processors to actively protect all personal data they are processing. For these kinds of situations and in order to prevent violations of data protections, the GDPR strongly recommends adopting security measures, such as anonymisation techniques, or privacy by design solutions such as pseudonomisation or data minimisation. On top of examining these recommendations, this chapter analyses the ‘personal data systems’ as a viable solution for protection personal data.

5.2 Anonymisation of the personal data

Föli could in theory benefit from anonymising the biking routes for city planning purposes, but might need to identify the method that fits them best as the GDPR does not define nor mention anonymisation techniques as a solution for secure processing. The reason for this is stated in the Recital 26, as the GDPR considers that "*the principles of data protection should [...] not apply to anonymous information*". In other words, the GDPR only applies to information which relates to an identifiable or identified natural person. Anonymized data unable identification of a natural person, and is therefore not covered by this regulation.

Anonymisation would be a drastic solution for the controller who wants to process data without being bound by data protection rules. Anonymisation would allow for continued use of data, without fearing violating someone's integrity. Obtaining consent would no longer be needed, data could be transferred freely… As explained by the WP 29[56], "*once a dataset is truly anonymised and individuals are no longer identifiable, European data protection law no longer applies*."

Anonymisation techniques are quite commonly used as a way of securing personal data. Yet, anonymisation requires that an operation is performed on the personal data in order to render in anonymous. The data has to be separated from the 'identifier', and several techniques have been explored for that end.

All techniques have the same aim: to irreversibly separate the identifying elements from a set of data. This would result in data that no longer can be related to an identified or identifiable natural person.

5.2.1 Anonymity criteria

The WP 29 has come up with three criteria aimed at identifying whether data is anonymous, which are:

- *Single out*: Is it possible to single out an individual?

[56] WP 29, Opinion 05/2014 on Anonymisation Techniques, 2014

- *Linkability*: Is it possible to link two sets of data belonging to one same individual?
- *Inference*: Is it possible to deduce, with a high probability, information on an individual?

If none of these questions is answered positively, the data is theoretically anonymous. However, it suffices that one of these criteria is fulfilled to not be classified as anonymous data, and to require a thorough analysis of the possible risks of reidentification.

5.2.2 Anonymity methods

Vivid debates are still ongoing among computer scientists as to know what anonymization method is the best, and whether any at all functions in practice. Several methods exist, yet all of them present risks of reidentification.

The professor Martyn Thomas[57] identifies four ways to anonymise data (perturbation, generalisation, suppression and replacement) and the WP 29 regroup these four into two main families, namely generalisation and randomisation.

Generalisation

The aim of the technique of generalisation is to replace the specificity of the identifier by a general information, for example a data of birth can be replaced by the birth year, a city can be replaced by a region… Generalisation offers good guarantees against the possibility to single out identifiable information, but remains quite risky considering the risks of 'linkability' and 'inference'. The family of the generalisation techniques encompass technical methods such as the k-anonymity, where identifiers are deleted or generalised.

[57] See the presentation from Professor Martyn Thomas CBE, *Big Data: The Broken Promise of Anonymisation*

For example, in this table[58], the name and the religion of the individuals have been deleted, and their age have been generalised and minimised to the year of birth.

Race	Birth	Gender	ZIP	Problem
Black	1964	f	0213*	obesity
Black	1964	m	0213*	chest pain
White	1964	m	0213*	chest pain

The result thus shows that a black woman, born in 1964 and domiciled in the area which ZIP corresponds to 0213 is obese. However, although some information has been erased and some other generalised, the data left is at risk of being relinked to individuals, and thus reidentified. Each element narrows down the amount of people concerned and could, if crossed with other details, single out an individual. If that occurs, the anonymization would have failed.

Randomisation

Randomising data refers to the action of randomly changing it and altering its veracity in order to weaken the risk of linking the data to the individual. Randomization englobes several techniques, such as *noise addition*, *permutation*, and *differential privacy*. An example of noise addition would be, for example, to change a user's biking distance with an accuracy of +-5 kilometres, diminishing drastically the chances of linking the distance to a specific individual. It is important that the randomization is performed so that it becomes impossible to figure out how the data has been randomized.

The WP 29 points out that data can be both randomized and generalized, which will result in increased privacy protection. Nevertheless, all methods of anonymisation present risks of reidentification.

[58] This table is taken from a larger table named 'figure 2, an example of k-anonymity', and taken from Latanya Sweeney, "*k-Anonymity: A model for protecting privacy*", International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570

5.2.3 The risks of anonymising data

The large majority of scholars analysing anonymising techniques consider that anonymization does not guarantee the end it aims for. Some do even talk about "the failure of anonymization". Paul Ohm believes that "*data can be either useful or perfectly anonymous but never both";* Rubinstein and Hartzog[59] consider that *"perfect anonymization is a myth*".

The reason for this is that the first aim of anonymising personal data, namely irreversibly separate identifying elements from a set of data so that the natural person behind the data no longer can be identified, is very risky. As pointed out by Martyn Thomas, a very little amount of details is actually needed to identify someone. He illustrates his statement by an identifying test taken in the US in 2000, where 62% of Americans were uniquely identified by their zip code (which in itself narrowed down the amount of people from nearly 300 million to 7500), their gender and their date of birth. Based on these three sets of data, all objectively anonymous if considered separately, people were uniquely identified. A date of birth alone is only a number, but added to one or more (anonymous) details, the probability for identifying the natural person it concerns rises. This is what the WP 29 identifies as the risks of 'linkability' and of 'inference', where identifiable data is established by linking to sets of anonymous data or deducing with a high probability the identity of a data holder.

5.2.4 Föli and anonymization

Although there are risks, Föli would profit from anonymising data in order to use it for city planning and heat map projects. Föli's heat map, imagined showing the most used routes by bikes, would ideally be based on the bike's GPS information, all other data concerning the user being either deleted or generalised, thus applying the k-anonymity method. However, the situation gets tricky because the heat map would get more useful if being in real-time, enabling users to know and follow how the bikes are

[59] Ira S. Rubinstein and Woodrow Hartzog, "*Anonymization and Risk*" (2015)

moving on a real-time basis. Real time maps showing the ongoing status of traffic do exist, and anonymization is sometimes performed by automated means. For example, the service HERE available at wego.here.com base their service on location data and shows through maps the state of traffic and the intensity of traffic jams. The data is collected through satellite and HERE vehicles driving around. In order to guarantee privacy, the service uses privacy[60] algorithms and detection rates aiming at blurring all faces and licence plates which are caught on the map pictures. In the event that these automated means miss an identifying element, they encourage the individuals to report their concerns through their internet website. This privacy solution is also used by Google maps street view. However, blurring a face or hiding a licence plate still shows identifiable elements such as the person and the colour of the car. Although the person and the car cannot with certainty be identified, there would still be a high probability of reidentification.

Whatever method Föli choses to adopt, a thorough risk analysis should be performed in order to lessen the probability of reidentification.

5.3 Encryption

One practical tool used for securing data is encryption. Schneier considers it as a "critical component of security[61]" and thinks that it is possible to create "unbreakable encryption", in other words really strong encryption systems with no backdoor. Such encryption allows employers to communicate without risking for the communication to fall in the wrong hands, and allows for data to be sent safely. Further analysis on the different methods of encryption is developed in the section 2.3.2.

Encryption is defined by Oxford's Dictionary of the Internet as *"the process of transforming some text known as the plain text into a form which cannot be read by anyone who does not have knowledge of the mechanisms used to carry out the encryption*." To access the encrypted data, the reader needs a key.

[60] FAQ about HERE cars and map data available at: https://www.here.com/en/drive-schedule

[61] See B. Schneier, *The Importance of Strong Encryption to Security*, 2016

Föli should consider encrypting the personal data they are processing as well as securing their internal communications through Virtual Private Networks (VPN). Encryption is also a solution to be considered when users use their right to data portability and request for all their data to be sent to them: the transfer of data is still a processing of data and needs to be secured. Encryption is a good way for securing the transfers and ensuring that the data reaches the right destination.

5.4 Privacy by design

5.4.1 The concept

Privacy by design is a fairly new concept of privacy protection launched by Ann Cavoukian in the early 2000s. In 2010, this framework was passed by the International Assembly of Privacy and Data Protection Authorities in Jerusalem as an International Privacy Standard. Today, privacy by design is considered as one of the main security solutions by the GDPR and is embodied in the article 25.

Ann Cavoukian considers[62] by 'privacy by design', *" embedding privacy up front, into the design specifications and architecture of new systems and processes, so that protecting personal data becomes the default condition. Instead of treating privacy as an after thought, […] PbD is proactive and preventative in nature – it is essentially "baked in" right from the outset."*

The notion 'privacy by design' says it all: tools ensuring privacy should be built in *by design* into the data processing mechanism in order to guarantee a sufficient level or data protection. Data protection compliance should be built in from the start and would block privacy-violating behaviors. Lessig provides with a good example[63] when he argues in favor of "code is law": he describes a virtual world owned and built by its residents, and compares it with the real world, in particular with the example of trespassing. Lessig observes that in the real world, laws can penalize individuals for trespassing on someone else's property, but the physical action of trespassing is still possible, whereas in the virtual world, the virtual individuals simply cannot trespass. The virtual world's code is designed so as to unable trespassing. It goes the same with

[62] A. Cavoukian, Privacy by Design and the Promise of SmartData

[63] See L.Lessig, Code 2.0, in the chapter on 'cyberspaces'

privacy by design, apart from the fact that this is not a virtual world: the processing system should be designed as to guarantee compliance with the GDPR and to protect the processed personal data.

The Information Commissioner's Office (ICO) encourages[64] organisations and service providers to implement privacy by design by, in particular when:

- "building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes."

Föli is in a favourable situation as the city bike system is brand new from scratch. It becomes thus easier to implement data protection compliance tools from the beginning. Proactively protecting personal data allows to identify potential problems at an early stage, respect the GDPR, increase awareness of data protection across the company and ultimately avoid misusing individuals' personal data. It is also to be mentioned that it is far cheaper to design privacy solutions in advance rather than 'repairing' misuses later: prevention is better than cure.

The GDPR in the article 25 respects this idea and discloses that "*the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."* The GDPR goes even further and adds in the second paragraph the requirement for data protection by default, requiring that the controller shall only process personal data "*which are necessary for each specific purpose of the processing*".

[64] ICO recommendations with regard to privacy by design available at: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

In this article, the GDPR thus suggests four elements which are important for data protection by design and by default.

1. Proactive timing

The concept of privacy by design is groundbreaking as it requires that protective measures be setup *before* processing data. It makes it a proactive approach. With regard to privacy by design, the GDPR considers that security measures should be set up "*both at the time of the determination of the means of the processing and at the time of the processing itself* ", This requires from the controller that the privacy tools are decided in advance and possibly updated and improved during the processing operations.

2. Pseudonymisation

Mention is also made of pseudonymisation as a technical and organisational tool aimed at ensuring privacy. The concept of pseudonymisation consists in replacing all identifiable elements by a pseudonym, thus hindering the direct identification of the data holder. It is a version of anonymisation techniques with the difference that it produces anonymous data on an individual basis. If applied well, the data holder would not be identifiable, and the data could be processed more freely. For example, the bike users' name could be pseudonymised and replaced by numbers and the retrieval of the 'real' name would require a key.

Yet, as pointed out in Recital 26, personal data which has be pseudonymised "*could be attributed to a natural person by the use of additional information*". Pseudonymisation is therefore not an irreversible method and would still permit for the data user to be identified, but is still considered as a functioning measure in order to reduce the risks to the concerned data holders. Furthermore, by applying pseudonymisation, the controller and the processor do more easily meet their data protection obligations.

3. Data minimisation

Data minimisation is a considered as a privacy architecture by computer scientists, and is strongly encouraged by the European Commission. As a matter of fact, data minimisation is one of the core principles of the GDPR and requires that the personal

data processed should be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5(c) GDPR].*

In other words: where personal data is needed, make sure to process only what is necessary. Föli should for example focus on processing only the name and the year of birth, and not the marital status or the users' nationality. By reducing the amount of data collected, the controller diminishes the amount of data which is processed and thus should be protected. Furthermore, it facilitates the application of anonymising procedures, as the amount of data to anonymise is less. The more data, the more details which can lead to reidentification. It is also to be noted that data minimisation goes hand in hand with the requirement put on the controller in article 5 (2) to make sure that no superfluous data is processed.

5.4.2 An obligation on controllers and IT designers?

The requirement for privacy by design presented in the GDPR under article 25 clearly puts an obligation on the controller. The controller becomes liable for ensuring that privacy by design is implemented, as it is the controller who determines the means of processing.

The notion of privacy by design, although aimed at the controller, indicates 'design'. Several scholars have therefore raised the question whether privacy by design also should be an obligation aimed at the designers of the technologies processing the data. Koops et al[65], with reference to more literature, observe that "*the ideal of the notion of privacy by design [...] could be read to be that all relevant data protection provisions will be encoded in software or hardware to the greatest extent possible.*" They decide to name this ideal 'hard privacy by design', but quickly come to the conclusion that it is in practice impossible, as the law is far too vague for technologies. Although some specific legal provisions could benefit from some hard-coding, most of the legal provisions and in particular the GDPR have very wide notions. Just considering the fact that the article 25 of the GDPR is "taking into account the state of the art" of the processing activites refers to the fact that they require flexibility, "breathing space". Technologies, albeit updateable, are usally designed and coded in a certain way.

[65] See Koops et al, 2013

Another hot debate is also to know whether privacy by design is a good solution at all, considering that most of the existing data processing organisations do not have designed security systems, and that becoming compliant with the article 25 could require changes which might get very expensive[66].

5.5 Personal Data Stores

Alongside the GDPR and all the national data protection laws, scholars have attempted to develop an alternative way for protecting personal data in practice. The idea of 'Personal Data Stores', also known as "Personal Information Management Services" (PIMS), "MyData[67]", "SelfData[68]", "SmartData", "Vendor Relationship Management", "Internet of Me", is to empower the individuals with the control and the management of their personal data. Cavoukian presents it[69] as "*SmartData consists of autonomous, Internet-based agents that act as a data subject's online surrogate – securely storing personal information and intelligently disclosing it in accordance with the user's instructions*." The idea, which is "*the embodiment of privacy by design*[70]", is to allow the data to protect itself as it will be linked and protected by a SmartData agent. Tomko[71] vividly argues in favour of the implementation of SmartData systems and stresses how secure the storage and the processing of the personal data would be.

Personal data stores (PDS) are a way of rethinking data protection and changing the control-centre. By giving the data subject control over her personal data, the PDS system would enable full transparency both for the processing entity as well as for the data subject and facilitate data management and liability issues.

In what way would it be different from our current data protection system?

---

[66] See AvePoint blog, article Privacy and Security by Design: The New Default under GDPR"

[67] Information available at: https://mydata.org/

[68] Information available at: http://www.selfdata.tech/

[69] Ann Cavoukian, *Privacy by design and the Promise of SmartData*

[70] Ann Cavoukian, *Privacy by design and the Promise of SmartData*

[71] G. Tomko, "SmartData: the Need, the Goal and the Challenge"

5.5.1 Current data processing system

At present, personal data is transferred from data holder to companies without any real control from either part. The authors of the new Regulation strive for a better control of the personal data, by particularly giving it to the data holders. Yet, the data is mostly in the hands of the processing companies, which need to take into account loads of measures in order to respect the regulation.

Companies do for instance have a big responsibility in assuring the protection of the personal data they are processing. To start with, they need to be aware of the fact that they are processing personal data. This is not always an easy task, as the action of "processing", as shown in section 4.1.1, includes basically any action dealing with personal data. They do also need to identify that they are using personal data, which is, as presented in the introduction, any data which can lead to the identification of an individual. Once the data has been categorized as *personal data* and the action has been defined as *processing of personal data*, the company is to coordinate it all. The meticulous organisation of the data has to be respected for two reasons: Firstly, the company is liable for the good use of the data and should thus ensure that it is well used for the right purpose in order to avoid any unlawful use of the data. In case of breach, leak or use of data outside the purposes originally defined, the data holder could call for a violation of the protection of their personal data. As defined previously in this thesis[72], this responsibility is provided in the article 24 of the GDPR, which states that: *"[...] the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."*

Second, the processing company should be well organized in order to enable the data holder to use his rights provided by the GDPR, such as the right of access, the right to data portability or the right to erasure. In order to ensure these rights, the company should be able to quickly access the data subject's data and follow his requests.

However, the "control" now given to the data subject might on the other hand seem very blurry. In a society where technical tools are evolving rapidly and where digital

[72] See section 3.2.2 under "the responsibility incumbent on the controller"

data is being transferred at the speed of light, it requires from the data subject organisational talents to keep control of the personal data concerning him. It appears almost impossible to tell how many companies are processing my personal data right now. A few are of course obvious, others less so. If the data holder does not know where her data is processed, how could she possibly use her rights?

When using the services from different players from public service bodies and organisation, such as hospitals and schools, as well as small and medium enterprises to multinational corporations, access is given to our personal data. That is, because personal data is provided to them by us, the data holders.

All these players process this personal data in the same way, by collecting it and controlling it internally. In line with the GDPR's requirement for the data subject to access her data, the latter is only to get access to this data through the organisation in question. For example, if the data holder wants to have access to her medical file, she needs to contact the hospital which treated her. If the same person needs to manage her theatre-visits, she needs to contact the theatre, and so on. Every single entity having some of her personal data needs to get contacted and dealt with separately.

The current situation presents several disadvantages, starting with the number of players involved. The Cambridge Report[73] on PDS lists five different types of players involved in the process of personal data:

1. "Multinational corporations, some of which derive revenue from data monetisation, and others with more diverse revenue streams (e.g. Google vs. Apple);
2. Small and medium enterprises ('SMEs');
3. Highly-regulated telecommunications companies, private healthcare providers, financial institutions;
4. Public sector regulatory bodies;
5. Public sector organisations such as hospitals, schools, police departments and passport issuing agencies."

It is very likely that an average person has personal data in the database of every player listed above. To manage this data, the data holder should go through all the players she

[73] University of Cambridge Judge Business School, *Personal Data Stores*

is involved with. Not without mentioning that all organisations most likely have different parameters of access, which does not make the bureaucratic achievement easier.

5.5.2 The new approach

The Personal Data Store (PDS) could change the present data management. In fact, the control of personal data, which today is given to organisations and companies, would be shifted to the data holders through PDS providers. From an 'organisation-centric personal data management', it will become a 'human-centric personal data management'. The individuals would get control over their personal data. Finland has been strong in developing the concept of Mydata, and have launched a 'MyData Alliance Finland[74]', an open community aimed at boosting pilot PDS projects.

The Mydata logo illustrates well the idea of centralising the access to personal data, where the data holding individual gets access to her educational, health, social media data…

the MyData logo

A PDS system is by design giving the data holder the choice of the data she wants to disclose and to what organisation she wants to make it available. Through the PDS provider, she can explicitly give her consent to the sharing of the data she wants. The data thus made available is usable by the receiving organisations. The public sector could for instance benefit from the data in better city planning and smoother coordination of public services.

All in all, a PDS system follows the principles held by the GDPR of assuring that the data holders get control over their personal data.

[74] See MyData Alliance Finland at https://mydatafi.wordpress.com/

- Economic benefits

The benefits for the society could be several, starting with generated money in the society. The Boston Consulting Group's calculations[75] assesses that €330 billion annual economic benefit could be generated in Europe by 2020 if the PDS would increase the flow of personal data. Ideally, the PDS ecosystem would enhance trust and users would be more willing to share their personal data to businesses, which in turn would benefit from accurate and profiled datasets.

- Convenience

PDS can answer to the behavioural paradox between control and convenience. As analysed by the Cambridge report, some data holders would like to have a full control over their data and to be the only ones to always decide on the collection of their data. Some data subjects would however prefer and consider more convenient that websites and services "remember" them. By enabling the data holder to set and manage their own personal data store, its processing becomes tailored and individual.

5.5.3 In practice

In practice, the PDS system requires to be hosted. The host could be an independent PDS manager, or the whole system could be self-hosted. As the name implies it, a PDS requires a storage, a place where the personal data can be gathered. Additionally, it requires a platform through which the individual can access and grant access to her personal data. It goes without saying that these technical requirements need to be safely secured.

Tomko describes[76] the security infrastructure of the SmartData initiative as being based on *"stripping a user's personal ID from the body of his/her data. The anonymized data is then segmented, encrypted, and placed in digital "lock-boxes"."* The SmartData is thus relying on anonymization techniques, encryption and safe storage, all methods combined. Although, as shown earlier in this section, anonymization techniques all present risks of reidentification, the protection should logically only get stronger when assimilated to other security measures.

[75] Boston Consulting Group, *The Value of our Digital Identity*, 2012

[76] G. Tomko, "SmartData: The Need, the Goal and the Challenge"

5.5.4 PDS and Föli

As presented in the introduction, Föli is one of the branches of the city of Turku among other public activities such as health care, libraries, schools… If personal data stores were to be implemented in Turku, it would be worth including all the activities carried out by Turku. It would thus enable the Turku-residents to have an overview of all the public activities processing their data or requesting accessing to them. The first steps towards such an approach have already been launched with the "Smart and Wise Turku" project in May 2018.

Data protection is not only a set of legal rules. Technical solutions are required to ensure that the strings of data are securely collected, stored and transferred and for that end, several techniques exist. Anonymisation, encryption and privacy by design are all solutions approved by the GDPR without providing instructions on how to implement them. Personal Data Stores are a novel method in the continuation of the Privacy by Design dynamic which could provide with a complete security for solutions by changing the core control over the personal data.

CONCLUSION

Turku is one of the few cities in Finland to have adopted a city bike service, together with Helsinki and Espoo. This new feature makes the city of Turku attractive, easily discoverable, eco-friendly and smart, or as the Finns say *fiksu kaupunki*[77].

Yet, as smart as the city might become, the administrative steps to take before implementing the system and during its maintenance might not be considered that 'smart' and easy, especially when the new general data protection regulation is enforceable on May 25th, 2018. As a matter of fact, as the date is approaching and the shadow of 20 million euros in penalty is floating in case of non-compliance, companies and organisations are afraid. That is at least the echo media have been giving out in the past few months, as when the French Le Monde writes that '*the GDPR is haunting the French employers*[78]', or when the Swedish Dagens Nyheter title their article[79] "*the abbreviation which might cost companies millions in penalty*" with regard to the GDPR. With such titles, it feels like encouragements to panic. But is it necessary?

Föli is in a rather comfortable seat regarding the city bikes as the whole system is new: this implies that all the processing activities are freshly designed and therefore might be easily adjusted. A new service also implies new contracts with processors, and possibilities to include in these contracts and in the terms and conditions all the necessary information required by the regulation. That is comfortable compared to companies which have been processing personal data in the course of their business and which already have subcontractors: for them, the process of getting in compliance with the GDPR might then be more demanding. All the personal data has to get secured, if that is not the case; new contracts have to be drafted; liability has to be

[77] Finnish for 'Smart city'

[78] See the article in French, « Protection des données : le texte européen qui hante les nuits des patrons de PME français », Le Monde, 8.05.2018, available at : https://www.lemonde.fr/economie/article/2018/05/08/protection-des-donnees-un-casse-tete-pour-les-entreprises_5295916_3234.html?xtmc=rgpd&xtcr=2 . The English title is my own translation.

[79] See the article in Swedish, "Förkortningen som kan kosta företag miljonböter", Dagens Nyheter, 06.02.2018, available at: *https://www.dn.se/arkiv/ekonomi/forkortningen-som-kan-kosta-foretag-miljonboter/* The English title is my own translation.

defined; technical tools might need to get updated; some personal data might even need to cease being collected… In other words, the GDPR comes along with a lot of work!

This thesis is an attempt to identify the necessary work to be done by Föli regarding data protection, both legally and technically. It feels obsolete to consider law on its own, especially when a text like the GDPR comes along and requires technical tools to be implemented and updated. Technology and law have never been that linked than when digitalisation started spreading, and the legal community is well aware of it. As a matter of fact, the GDPR gets enforceable together with the ePrivacy regulation, replacing the previous Directive 2002/58/EC and aiming at regulating personal data in electronic communications. Both texts include digital technology as an important part.

Föli's city bikes are very much depending on digital technologies, especially as their billing system is partly using smartphone as a device, and each bike is equipped with a GPS. Furthermore, all collected personal data is stored in a physical server, and all communications with the users is for the moment made through emails. As required by the GDPR, all personal data has to be secured, and as a consequence it leads to secure the technical tools used for its processing. It is as if personal data was water which needs to be held within a bag, the bag representing technologies. For the water to stay inside the bag, the latter needs to be whole and without holes. The same goes for the whole technical system, which needs to be updated regularly by IT experts as to make sure that personal data cannot leak out.

Technical tools also encompass all the security procedures such as encryption, anonymization and privacy by design. If personal data stores come to get considered as a viable solution, they might come to be considered as embedded technical tools too. Lessig wants us to learn that "*technology is plastic [which] can be remade to do things differently*[80]", and that code, read 'technology', could become a regulator assisting in the protection of personal data. Lessig believes that "*there are both changes in law and changes in technology that could produce a much more private (and secure) digital environment*."

[80] L.Lessig, Code 2.0, in the chapter 'is-ism'

Protected against what? As described in a non-exhaustive list in the second part of this thesis, the threats to personal data are several and could evolve, as new methods of hacking get developed. If personal data is considered as "*the future's fuel*", why wouldn't it be attractive to wrong-doers to find profit in hacking it and selling it? The risk of hacking through vulnerable sensors or unprotected Internet connections is measurable and can be limited, by for example securing all the used technologies and updating them regularly. Security is also achieved through measures such as encryption, safe storages and anonymization techniques. However, these risks also have an effect on psychology, as Schneier argues[81]. According to him, security is both a "*a feeling and a reality*", the reality being measurable, and the feeling being subject to psychological reactions to the calculated risks and the countermeasures put in place. In other words, we might feel truly secure when in fact the risks are terrible, and on the contrary we might feel threatened although everything is safe. Where is the balance? Scientific studies in psychology and behavioural finance have analysed this balance and the reasons for unbalance, and it seems that the GDPR's answer to this is to give the data user *control*.

It will not be stated enough: giving control to the data user is what the GDPR was designed for. This control is made possible through the several rights given to the data holder, namely the right to access, the right to rectification, the right to erasure, right to data portability, the right to restriction of processing and the right to object. The two last ones were not analysed in this thesis as they were not considered applicable in the case of Föli's city bike system. Having those rights, the data subject should be able to have an overview over her data in the processing system.

Guaranteeing these rights do however put quite a lot of pressure on the processing organisations, as they both should secure legally and technically the collected personal data, and have great organisational skills that one may retrieve a specific string of data. Yet again, Föli is in a favourable position as the bike system is new, and the bike user registry is easily organisable from the beginning. They should nonetheless ensure that

[81] Schneier, The Psychology of Security (Part 1), from the Blog Schneier on Security, 2008

all collected personal data has been subject to the data holder's consent and that it is being processed in a transparent way and with a well-defined purpose.

What happens in case of failure, if personal data is breached? Covered by the article 33 and 34 GDPR, the controller shall without undue delay inform the supervisory authority of the breach, and in the case that the breach is "*likely to result in a high risk to the rights and freedoms of natural persons"*, the data holder should be kept informed. The GDPR recital specifies that reprimands might be given by the supervisory authority or fines, and administrative fines might be imposed in case of severe breach. The amount would depend on the circumstances of the breach, for instance on the "*nature, gravity and duration of the infringement and of its consequences and the measures taken […] to prevent or mitigate the consequences of the infringement*." The general conditions for imposing the administrative fines are defined in the article 83 GDPR, and the dissuasive fines of 20 million euros or 4% of the total worldwide annual turnover are charged:

- If the basic principles of processing and of the consent mechanism were not respected,
- If the data subject's rights were not respected,
- If personal data was unduly transferred or,
- If the controller did not comply with an order from the supervisory authority.

However, one paragraph worth reflecting on is article 83(7) which states that *"[…] each member state lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State*." As explained in the introduction, Turku's city bike system is currently operated by the city of Turku but will be shifted completely to Föli in a few years. Meaningless to say that the city of Turku is a public authority, Föli is also a public transport service, subject to national rules regarding administrative fines. It is thus interesting to read the Finnish proposal[82] for a national law, which aims at completing the GDPR in all the

[82] In Finnish Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, available at: http://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80595905

provisions requiring transposition into national law. Its article 25 [83] requires for instance that public authorities and bodies *should not* be subject to administrative fines, as it would be like paying a fine from the State to the State. In other words, Föli would thus not be subject to fines, however does this take away the aspect of liability? Are Föli, as the main controller, still responsible for possible data protection breaches? The answer to this is that public authorities and bodies are subject to other rules and a right processing of personal data belongs to their duty, and severe sanctions could be borne if this duty was violated, as mentioned in the proposal's explanation of the article 25.

However, how does it go with processors, which are all private actors? Init, Nets, Globeon, Western Systems and Nextbike Polska S.A are private organisations and therefore should bear administrative sanctions in case of personal data breaches. These sanctions would however not be charged on Föli, thus a separate penalty mechanism would be put in place appreciating the two different qualities of the actors involved. This new legal situation is likely to be resolved with time, as many other aspects in the data protection field.

[83] Article 25(2) in Finnish: "Seuraamusmaksua ei voida määrätä valtion viranomaisille, valtion liikelaitoksille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille eikä tasavallan presidentin kanslialle."