IoT COMPLIANCE WITH GDPR AND ePRIVACY DIRECTIVE WITH RESPECT TO SMART VEHICLES
Master’s Exam Part I – IT Law Lab

Supervisor
Attorney-at-law and partner in law firm TRINITI Karmen Turk

Tartu
2019
TABLE OF CONTENTS

INTRODUCTION .................................................................................................................. 3

1. General background of the Internet of Things .............................................................. 5
   1.1. Overview of the Internet of Things ........................................................................ 5
   1.2. Examples of the use cases of the Internet of Things .............................................. 6

2. Existing legal framework related to the use of the Internet of Things ......................... 8
   2.1. Rules regulating the electronic communications services and networks .......... 8
   2.2. Horizontal consumer protection rules .................................................................. 10
   2.3. Industry specific rules .......................................................................................... 12

3. Compliance with GDPR and ePrivacy directive for smart vehicles ......................... 12
   3.1. Overview of smart vehicles .................................................................................. 13
   3.2. Processing personal data lawfully ........................................................................ 16
   3.3. Ensuring the purpose limitation, data minimisation and storage limitation ....... 18
   3.4. Providing information in conformity with the transparency principle ................. 22
   3.5. Ensuring the security of processing the personal data ......................................... 25
   3.6. Changes to the business model and legal framework .......................................... 28

SUMMARY .......................................................................................................................... 31

CONTRIBUTION OF GROUP MEMBERS ..................................................................... 33

ABBREVIATIONS ............................................................................................................. 34

REFERENCE LIST ........................................................................................................... 35

Literature .......................................................................................................................... 35

Legal acts .......................................................................................................................... 36

Guidelines and policy documents ................................................................................. 38

Other ................................................................................................................................. 39
INTRODUCTION

The capacity of the computer systems as well as the technical possibilities to process information started to increase already years ago. Furthermore, the lines between the physical and online world have been fading for some time and the era of the Internet of Things (hereinafter IoT) is prevailing being part of the so called Third Industrial Revolution. It is a huge step forward when it comes to intelligent systems and for the last couple of years, the usage of IoT has been increasingly growing in different industrial sectors.

This has been especially clear for vehicles as the automotive industry is having a massive disruption and paradigm change towards increasingly connected and autonomous cars (hereinafter together as smart vehicles). The old automotive business models are changing at a fast pace and new ones are emerging with the technology advancements. Furthermore, in recent years, the rate of smart vehicles has been growing and the end users are continuously more interested in autonomous cars, willing to take a ride in a driverless vehicle.

At this stage, the connected cars have emerged with their impressive decision-making capabilities for assisting the drivers. These connected features that enhance car users experience and/or improve car safety include for example cruise control and parking as well as collision and lane-changing warnings. Millions of connected vehicles are put on the market worldwide every year and the number is expected to increase to 775 million by 2023.

Within the next few years, the features of the connected cars are expected to expand being able to not only communicate with the relevant infrastructure, but also with any other entity that is capable of communicating in that way (e.g. pedestrians, devices, grids etc.). Furthermore, in

---

the next decades the driver might become optional, i.e. the shift will be made also towards semi-autonomous and fully autonomous self-driving vehicles. Already now car manufacturers, system suppliers, road operators and other providers are testing autonomous vehicles in a supervised way (i.e. the driver being on board and able to take control when needed).\(^9\)

On one hand the IoT brings various benefits to the development of modern society as the quality of services is improved by among others the fast spread of wireless devices, sensors and appliances. These services include numerous smart solutions like smart homes, smart cities and smart vehicles\(^10\) that will all help to make the life of people easier and more convenient, making among others the driving experience safer, more enjoyable and more effective.\(^11\) On the other hand it introduces also additional risks\(^12\) as well as worries from the people. Even though privacy issues have been always present in wireless networks, the IoT has new features that require new privacy protection mechanisms.\(^13\) For example, security, trust and privacy problems have been mentioned regarding smart vehicles.\(^14\) More specifically people are worried that their location will be tracked very long and very widely\(^15\) and over 80% of the European drivers were most concerned about the disclosure of private information.\(^16\)

The current paper has been divided into three main chapters. Firstly, the general background of IoT will be provided, including the overview, how it has emerged, and some examples of various use cases. Secondly, an overview of the applicable legal framework of the IoT will be given with the focus on the General Data Protection Regulation (hereinafter GDPR)\(^17\) and the ePrivacy Directive.\(^18\) Lastly, the compliance with the GDPR and the ePrivacy Directive for smart vehicles will be analysed and some changes to the relevant business model and legislation will be suggested.

\(^12\) Ibid
\(^14\) S. Karnouskos, F. Kerschbaum. op cit, p. 160
Keywords: Internet of Things, General Data Protection Regulation, ePrivacy Directive, ePrivacy Regulation, smart vehicle, connected vehicle, autonomous vehicle, driverless vehicle.

1. General background of the Internet of Things

The Internet, even though the term itself was introduced a decade later, was first created in 1960s by the Advanced Research Projects Agency as they had a need for the computers to communicate with each other. Initially the purpose was to interconnect computers and transmit messages. Thereafter, it grew extensively and in 1990s the World Wide Web was introduced, which made it easier to navigate through the Internet. The so called Web 1.0 enabled the linking of documents and basically created a World Wide Web of Information.\(^{19}\)

Furthermore, in the early 2000s, Web 2.0 sprang off as there was a demand for being able to create online content also by those, who did not have the necessary skills. So the Internet became a universal communication technology enabling the carrying of all voice, video, or information content.\(^{20}\) Nowadays, we have moved on to Web 3.0, which is basically represented by the IoT and expected to bring significant benefits to the economy. The number of connected things is estimated to increase to 25 billion in 2020.\(^{21}\)

1.1. Overview of the Internet of Things

The IoT is the next step in the development of the Internet, including the next major economic and innovation wave. It is moving towards a digitisation that enables the interconnection of all objects and people regardless of the type of space – private, public or industrial. These objects and people would be able to interact with each other and report about their statuses as well as the statuses of the surrounding environment. So the IoT can combine the physical and the virtual worlds into one easier, safer as well as more efficient and use-friendly environment.\(^{22}\) In 2014 the Article 29 Data Protection Working Party (hereinafter Article 29 WP)\(^{23}\) mentioned that the

---


\(^{20}\) Ibid, p. 56; Ibid, p. 5.


\(^{22}\) Ibid, p. 362; Ibid, pp. 4-5.

\(^{23}\) Article 29 WP was a Working Party on the Protection of Individuals with regard to the Processing of Personal Data, but it ceased to exist, when GDPR was adopted and the European Data Protection Board (hereinafter the EDPB) established. It was initially created by article 29 of the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of
IoT is merely on the verge of being integrated into our lives. But in 2018 European Union Agency for Fundamental Rights (hereinafter FRA) concluded that the IoT is already a reality.

It is often claimed that Kevin Ashton (Massachusetts Institute of Technology’s Automatic Identification Center in Boston) was the first to use the term in 2009. He mentioned it as a standardized way for computers to capture information from the real world and to understand it. However, it is challenging to define the IoT due to its technical and conceptual complexity and there does not seem to be one agreed definition as different sources have the notion explained slightly differently.

For example, according to the European Research Cluster on the IoT, it is “A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.” Furthermore, Art 29 WP thinks that “The concept of the Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices – “things” as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities”.

1.2. Examples of the use cases of the Internet of Things

The Internet of Things has already been used in a variety of situations and is expected to grow extensively in the upcoming few years. Think for example of a smoke detector that in case of fire will flash your bedroom lights and play an MP3 audio file loudly warning of the fire as well as call the fire department and your neighbours and automatically turn off the flow to the gas appliances. Or a fire extinguisher calling the fire department, when it is being used by you.

---

There are already different devices for monitoring the health of a patient or tracking the daily routine of elderly people and creating alerts in case of serious disruptions in their daily schedule.\textsuperscript{33} Other type of societal challenges have been addressed by Barcelona, when introducing the energy-saving sensors in street lights and mechanisms for detecting when rubbish containers are full\textsuperscript{34}, and by UK that introduced the traffic management control system for reducing traffic congestion.\textsuperscript{35} A broader concept of it is the so called Smart Cities, where the main aim is to increase the efficiency of the city by among others reducing the cost, emissions and energy consumption\textsuperscript{36} (e.g. eToll, smart parking and police assistance).\textsuperscript{37}

Furthermore, there are clear business opportunities in IoT for lead markets. For example, different home automation solutions such as light bulbs, heating systems, smoke alarms, weather stations, washing machines, ovens and security locks of doors that can be controlled remotely over the internet are making homes a “mini IoT environment”. Furthermore, the role of personal wellness and wearables, such as watches and glasses, is also growing as they extend the functionalities and usefulness of the everyday objects. In addition to the devices for generic purposes like measuring daily calorie in-takes or hours of sleep, there are multifunctional ones as well like a medical sensor serving also as a security verification tool.\textsuperscript{38}

Currently, the majority of IoT-based systems include a centralized client-server, cloud servers, strong database and the Internet.\textsuperscript{39} Therefore, in several IoT solutions, the smart object will have an embedded sensor that will send the data generated by it directly to a cloud service. For example, a home device that is used daily like a thermostat,\textsuperscript{40} a camera in a smart TV that sends live feed to be stored in the cloud\textsuperscript{41} and a lifestyle system that monitors with a cloud-based self-learning algorithm the behaviour of the family or alone living elderly generating alerts when something unexpected happens.\textsuperscript{42}

\textsuperscript{39} I. Mistry, S. Tanwar, S. Tyagi, N. Kumar. op cit, p. 2.
\textsuperscript{41} A. Henschke. op cit, p. 7.
All these solutions process enormous amounts of data\textsuperscript{43}, which, as pointed out previously, is in quite many IoT solutions transmitted to a cloud. Furthermore, within the meaning of article 4 point 1 of the GDPR, in case this data relates to an identified or identifiable natural person, it is personal data, which often is the case.\textsuperscript{44} Hence, there are many questions around the vulnerability of IoT devices, including many privacy and security challenges, starting from unauthorised access to the data and finishing with malware.\textsuperscript{45} Therefore, the data in the IoT systems needs to be properly handled, especially when combined from different sources.\textsuperscript{46}

2. Existing legal framework related to the use of the Internet of Things

As regulatory and legal aspects can be considered to be the enabling factors for a successful exploitation of various IoT devices, there is a relatively complex network of regulations and policies regarding the use of IoT. Relevant legal framework can be divided into three broad categories: rules regulating the electronic communications services and networks, horizontal consumer protection rules and industry specific rules.\textsuperscript{47}

2.1. Rules regulating the electronic communications services and networks

Electronic communication is a vital component of IoT, different devices must communicate with each other. Data from the devices is collected and sent to servers, servers share the device data and can send data back to the devices for analysis or to people to use it.\textsuperscript{48} The European Electronic Communications Code\textsuperscript{49}, which consolidated the Access Directive, Authorisation Directive, Framework Directive and Universal Service Directive, as stated in the preamble recitals 1 and 2, modernised the EU telecommunication rules.\textsuperscript{50} Connected Continent Legislative Package set the stage for rising numbers of new business models and more

\textsuperscript{44} Article 29 Data Protection Working Party. Opinion 8/2014 on the on Recent Developments on the Internet of Things. 16.09.2014, pp. 4, 10.
\textsuperscript{45} Ibid, p. 4, 6.
\textsuperscript{48} Body of European Regulators for Electronic Communications (BEREC) report. Internet of Things indicators. p. 5. – BoR (2019) 25, 04.01.2019
innovation, the guarantee for net neutrality, open internet and integrated networks.\textsuperscript{51} Roaming Regulation\textsuperscript{52} creates the possibility to use data internationally without limitations, which is a top priority for many IoT devices.

As one of the focus topics of this work, the ePrivacy Directive will have a more thorough review, as it is the cornerstone regarding the details of confidentiality of electronic communications. “The regulation would adapt the previous directive’s provisions to new technologies and market reality and would build a comprehensive and consistent framework with the GDPR would be \textit{lex specialis} to the GDPR, tailoring it to electronic communications data that constitute personal data.”\textsuperscript{53}

The most relevant articles regarding the ePrivacy Directive are, as follows:

1) Article 4 – security: The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security;

2) Article 5(3) – confidentiality of the communications: storing of information, or the gaining of access to information already stored in a IoT device requires data subject consent, having been provided with clear and comprehensive information, in accordance with data protection directive about the purposes of the processing. In the case where directive 95/46/EC was replaced by GDPR, the requirement for a consent is still relevant;

3) Article 6 (1) – fair collection of traffic data: Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication;

Already in 2006 and referring back to the same statements in 2000, the Article 29 WP mentioned that the notions “electronic communications services”, and “to provide an electronic communications network” are not clear and these should be explained more thoroughly (e.g. is

\begin{footnotes}
\item[	extsuperscript{52}]Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union.- \textit{OJ} L172, pp. 10-35
\end{footnotes}
a cyber café a provider of an electronic communication network). Furthermore, in their view it is regrettable as well, that the provisions of the ePrivacy directive only apply to publicly available networks and not private networks.\textsuperscript{54} Thus, it is not totally clear in which circumstances this provision will be currently applicable in case of IoT devices. However, due to the use of WIFI networks and other type of electronic communications networks, it might be in some cases relevant.

For example, in the latest version\textsuperscript{55} of the Council of the EU for the proposal for the ePrivacy Regulation, particularly recital 12, the clear difference has been made between the transmission and application layer. Namely, it has been mentioned that the transmission services used for the IoT services regularly involve the conveyance of signals via an electronic communications network. However, providers of IoT services operate on top of the electronic communication services and thus they or their customers who use IoT devices are not providers of the electronic communication service.\textsuperscript{56} The European Parliament however has deleted the whole recital and in their explanations they mention that these services were not covered by the ePrivacy Directive, but should be in the new ePrivacy Regulation.\textsuperscript{57}

\textbf{2.2. Horizontal consumer protection rules}

As IoT devices are meant to be used by all people, certain overall rules have to established with EU regulations to protect consumer rights, personal data and the safety of communications. Therefore, The Regulation on the free flow of non-personal data\textsuperscript{58} is useful, as it helps to remove obstacles from the free movement of non-personal data cross Member States and IT systems.

\begin{itemize}
  \item \textsuperscript{58} Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. - OF L 303, pp.59-68
\end{itemize}
Together with the GDPR, this regulation will ensure “a comprehensive and coherent approach to the free movement of all data in the EU”.59

Cybersecurity Act60 and Directive on security of Network and Information Systems61 establish a EU-wide framework for a secure use of digital products and services and to boost overall level of cybersecurity in Europe. In order to protect the consumer rights in the EU, Consumer Rights Directive62, Unfair Commercial Practices Directive63 and Product Liability Directive64 set out the rules to be achieved when products and services are designed, so that the consumers feel that they are fair and safe to use.

The GDPR, which applied to Member States from May 25, 2018, replaced the data protection directive65. The GDPR sets out “EU data protection rules for the processing of personal data that apply to IoT devices.”66 The most relevant provisions from the GDPR the current work will focus on, are:

1) Article 6 – Legal basis to process regular personal data: 1) consent 2) contract 3) legitimate interest;
2) Article 9 – Legal basis to process special categories data: 1) explicit consent;
3) Article 5 – Principles relating to processing of personal data: lawfulness, fairness and transparency (1) a; purpose limitation (1) b; data minimisation (1) c; accuracy (1) d; storage limitation (1) e; integrity and confidentiality (1) f;
4) Article 32 – security of processing: Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,

---

65 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.- OJL 281.pp. 31-50
the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk;

5) Articles regarding rights of data subjects: transparent information, communication and modalities for the exercise of the rights of the data subject (art 12), provide the data subject information, when data is collected (art 13), information to be provided where personal data have not been obtained from the data subject (art 14), right of access (art 15), right to rectification (art 16), right to be forgotten (17), right to restriction of processing (art 18); right to data portability (art 20); right to object (art 21), right not to be subject to a decision based solely on automated processing (art 22).

2.3. Industry specific rules

Many regulations are specific to a particular industry, where IoT devices can be used. IoT devices can be used in every industrial sector, but they are especially relevant for the innovative industrial sector. Digital transformation of industries helps to create different levels of value, for example value for speeding up the production, testing, application. It is very important that different companies in certain industries work together to make the growth of the industry even faster.

For example Intelligent Transport Systems Directive, Type Approval Regulation and eCall Regulation apply to the automotive industry; Common Agricultural Policy to the agriculture sector, Energy Performance of Buildings Directive to the energy sector, EU Basic Regulation for Drones to aviation and Medical Devices Directive to healthcare industry.

3. Compliance with GDPR and ePrivacy directive for smart vehicles

As seen from the previous legal framework overview, the dimension of the IoT relevant legislation is widespread. Furthermore, as mentioned already before, then the vast volume of personal data in the IoT devices also entails risks for privacy and data protection. Therefore, and to be able to narrow down the scope of the current work, the compliance analysis will be based on some of the relevant provisions of ePrivacy Directive and GDPR, which reflect the

---

most important core value principles of the personal data processing in view of the authors of the current work. These provisions will be combined into 4 categories:

1) Lawfulness: article 5(3) of the ePrivacy directive and articles 5(1)(a), 6, 9, 21 and 22 of the GDPR;
2) Limitations: article 6(1) of the ePrivacy directive and articles 5(1)(a),(b), (c) and (e) as well as art 17 of the GDPR;
3) Security: article 4 of the ePrivacy directive and articles 5(1)(f) and 32 of the GDPR;
4) Transparency: articles 5(1)(a) and 12 to 15 of the GDPR.

Throughout the analysis, the authors have chosen as examples the following cars manufacturers, as they have been mentioned in different places as the major or leading companies in the field of smart vehicles: General Motors, Mercedes Benz, Audi, Tesla, Ford and Volkswagen.68

3.1. Overview of smart vehicles

There are many different notions used for vehicles that are somehow related to the IoT. Firstly, the connected vehicles are permanently connected via various communication technologies to the Internet and can interact with the infrastructure and other vehicles. Secondly, hyperconnected vehicles are interacting and exchanging information with any type of entity that is capable of it, e.g. pedestrians, devices, grids etc. Thirdly, in relation to the autonomous vehicles it has been mentioned that the driver may be optional in the next decades.69

It has been found that the notions “autonomous vehicles” and “connected vehicles” are not synonyms. According to the explanations, the driverless or autonomous car does not need to be connected to “outside”, but only to its sensors and cameras and to its own brain. Connection to the IoT is an add-on, allowing cars to connect to other vehicles and to outside information, such as updated road map information, or to connect to services.70


69 S. Karnouskos, F. Kerschbaum. op cit, p. 160.
70 C. Murroni. op cit, p. 10.
However, on the other hand, autonomous driving has been classified into six levels by the international Society of Automotive Engineers,\textsuperscript{71} the first one (level 0) being that the human still drives the car without any supporting system and the fifth one that the vehicles are fully automated without relying on the human input at all.\textsuperscript{72} Furthermore, the American National Highway Traffic Safety Administrations adopted the same levels.\textsuperscript{73} Lastly, the European Commission has mentioned that the connected vehicles (i.e. vehicles connected to other vehicles and/or to the infrastructure) can potentially be semi-autonomous and autonomous. Namely, even though the automated driving is possible without the communication infrastructure (i.e. based only on on-board sensor systems), connectivity is still required to implement it (e.g. for navigation positioning and maps).\textsuperscript{74}

Therefore, it seems that even if these terms (connected and autonomous vehicles) are not synonyms, they are definitely overlapping. Furthermore, all these types of vehicles can be considered as steps of evolution, which have a similar business model and involve risks that are increasing on each step of development (including the combination of different features these vehicles). Therefore, we would combine them in this work under the notion “smart vehicle” and will use the other notions exactly as they have been used in the relevant research papers.

The smart vehicle has been chosen as a use case of this work due to the reasons of relevance and importance more thoroughly explained in the introduction as well as the requirement of the task to choose one example involving cloud computing. Namely, on the EU level it has been suggested that there are three solutions to be used for accessing the in-vehicle data: (i) on-board application platform; (ii) in-vehicle interface; and (iii) data server platform.\textsuperscript{75} The latter may include cloud computing among other as the main architecture in autonomous vehicles,\textsuperscript{76} including the connection of autonomous vehicles to mapping systems,\textsuperscript{77} and/or for analysing and storing big data as well as giving real-time data analytics results.\textsuperscript{78}

\textsuperscript{71} Society of Automotive Engineers. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, J3016, 201806. 2018. - https://www.sae.org/standards/content/j3016_201806/ (09.01.2020)
\textsuperscript{78} S. Sharma, Victor Chang, U.S. Tim, J. Wong, S. Gadia. op cit. p. 83.
Furthermore, there are in the market cloud providers specifically targeted to smart vehicles.\textsuperscript{79} For example, Connected Vehicle Cloud offered by Ericsson\textsuperscript{80} and CloudCar’s white-label platform providing cloud-based infotainment services specifically for the automotive industry.\textsuperscript{81} As cloud computing is easy-to-use and involves low-cost, then many autonomous vehicle data telecommunication companies and government agencies on road safety are beginning to use the cloud for storing the data.\textsuperscript{82}

As an overarching topic the controller-processor relationship raises some accountability and responsibility issues in cloud computing. Namely, the cloud client is a controller, if it determines the purpose and means of the processing of personal data and the cloud provider is a processor in case it processes personal data on behalf of the cloud client. It seems to stem from the opinion of the Article 29 WP that in most situations it is the case, even though it leaves the door open for other type of circumstances with stating “In cases where the cloud provider acts as a controller as well, they have to meet additional requirements”.\textsuperscript{83}

Even though some of the obligations (e.g. the security obligation in article 32, obligation to process the data lawfully) are applicable to controller and processor, then according to article 28 of the GDPR the controller has an additional obligation to use only processors providing sufficient guarantees for complying with GDPR. Therefore, even if the incident happens due to the cloud computing, the cloud client might not be able to exclude itself totally from the responsibility. However, one exemption has been provided from liability for the damage caused by processing which infringes GDPR in article 82(3) in case the cloud client can prove that it is not in any way responsible for the event giving rise to the damage.

Lastly, the autonomous systems have and create an enormous amount of personal data. These systems can identify the driver through psychological characteristics (e.g. fingerprints, heartbeats) and take into account the preference of various people while adjusting the vehicle speed or the music. Sometimes the people might not have consented to it\textsuperscript{84} or might not be even

\textsuperscript{81} CloudCar. Redefining the in-vehicle digital experience. - \url{https://cloudcar.com} (09.01.2020)
aware of it. Therefore, all of it raises quite many questions on the compliance with different privacy regulations.

3.2. Processing personal data lawfully

GDPR art 5(1)(a) states, that data should be processed lawfully. Lawful basis comes from GDPR art 6 and 9. Relevant basis could in the context of IoT are consent, contract and legitimate interest.

It can be said, that establishing a lawful basis is a critical step to take before starting to process data. „If the controller does not have a lawful basis for a given data processing activity (and no exemption or derogation applies) then that activity is unlawful.”85

GDPR mentions several legal basis, one of the most prominent ones being consent. ePrivacy Directive art 5(3) explains, that storing of information, or the gaining of access to information already stored in a IoT device requires data subject consent, having been provided with clear and comprehensive information, in accordance with data protection directive about the purposes of the processing. In the case where directive 95/46/EC was replaced by GDPR, the requirement for a consent is still relevant.

Consent requires a transparent information before a person can give consent to the terms.86 That information can be given in writing in a Privacy Policy, but these documents tend to be long, hard to read and in legalese. Therefore, they are almost never read and to conclude, the consequences are not understood.87 Even more, tech companies can use the second legal basis – contract – so there is no need to ask for a consent to process data. When a connected car is purchased, the sales contract can already state, that all the data will processed in a way and shared in way the car manufacturer wants. These contractual arrangements enable to claim control over personal data.88

Companies can also use legitimate interest legal basis. Article 7 (1)(f) states that personal data may be processed on the basis that the controller has a legitimate interest in processing those data, provided that such legitimate interest is not overridden by the rights or freedoms of the affected data subjects. This legal basis could help the companies „to defend data processing of drivers, passengers and even other traffic participants if the profiles contribute to (i) the efficient performance of contractual promises of adapted driving, (ii) to traffic security, or (iii) to interests of the controller to improve fleet learning and algorithmic precision.“89 In the other hand, it is clear that such processing will hardly be justified by merely the economic interest, which is not overriding the data subject rights regarding health, home, intimacy or location data processing.90

GDPR art 21 and 22 also introduces the right to object to data processing and sets out an automated processing restriction. Automated processing can be profiling as well. Using sensors in connected cars enables to collect sufficient amount of data about a person’s habits. Using analytics can be even more intrusive if more detailed and complete patterns of lives are made.91

People have the right to object that their data contributes to a proprietary or secret intelligence system.92 For example, although Tesla is currently collecting data primarily for the improvement of their own products and services93, Google has shown an interest in similar data collection. Foreseeing the future based on past behaviour and made decisions by individuals would be a valuable for other business sectors as well, for example „advertisement, insurance companies, local and municipal government, and law enforcement for a myriad of reasons“.94 „People’s driving routine and places of interest may permit not only their identification, but also conclusions on sensitive information, such as religious and political associations, sexual orientation, and relationships.“95

Ford mentions in their Connected Cars privacy policy, that they may, where permitted by law, combine and, using automated decision making processes, analyse your Connected Vehicle

89 P. Hacker, Op cit, p. 275.
91 Ibid. p. 8.
Information with other information we hold about you, to assist with the purposes outlined in the Privacy Policy. Even more, the data will be shared to other companies who are providing services on their behalf, for example web-hosting companies and other information technology providers.\footnote{Ford Connected Car Privacy Policy. - https://www.ford.ie/useful-information/terms-and-privacy-policy-hub/connected-car-privacy-policy (11.01.2020)} Therefore automated decision making and data sharing with third parties while using connected cars has become normal business process.

To sum up, it is not clear how exactly personal data is processed using automated means, how companies use profiling and who gets access to the data. Therefore several privacy concerns are raised. Concerns are also raised regarding the lawful basis of processing personal data. Companies may want to continue publishing long, hard to understand privacy policies, which people do not read. Texts should be published in a simple, easily understandable manner and before IoT devices are started to use. As valid contract can be a legal basis as well, while buying an IoT device, IoT manufacturers can get control all of the buyer’s data in a way that is unpredictable and questionable.

### 3.3. Ensuring the purpose limitation, data minimisation and storage limitation

The main reason for the existence of data protection laws is ”the consideration of the data subjects and the recognition that they need dedicated legal protection in the digital age”.\footnote{P. Blume. The Data Subject. European Data Protection Law Review, 1(4). 2015.p. 258} As stated in recital 1, the protection of natural persons in relation to the processing of personal data is a fundamental right. Recital 2 adds, that GDPR is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

To protect data subject rights, GDPR has stated several rights and freedoms. GDPR art 5(1)(b), (c) and (e) set the scene for purpose limitation, data minimisation and storage limitation principles.

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; adequate, relevant and limited
to what is necessary in relation to the purposes for which they are processed and 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.

“The purpose limitation principle implies that data can only be collected for specified, explicit and legitimate purposes. Any further processing that would be incompatible with these original purposes would be illicit under EU law. This principle aims at enabling users to know how and for what purposes their data will being used and decide whether to entrust a data controller with his/her data. These purposes must be defined before the data processing takes place, which excludes sudden changes in the key conditions of the processing. This implies that IoT stakeholders have a good overview of their business case before they start collecting any personal data.”

Regarding the purpose limitation, Tesla for example explains in their privacy policy that related services to connected cars bundle together in a way, which is unclear and/or non-compatible. Examples regarding bundled purposes are „providing requested services, credit and behaviour scoring and operating and expanding business activities”, “data originally collected for maintenance purposes could be used by insurance companies to enrich driver profiles, custom pricing, and offer driving behaviour-based insurance policies or investigate liability in car accidents”.

“Excessive data collection is particularly common in applications powered by machine learning, which use large datasets, often collected over a long period of time, to build their predictive models.”

As it is known, connected cars have several sensors and cameras which are like a nervous system of the connected car. For example, Tesla car has 8 cameras and 12 ultrasonic sensors.

---

101 Ibid.
“It’s estimated that these cars will be generating 4 terabytes of data per car per day”. 104 “But, in a future with billions of mobile devices and trillions of IoT devices moving massive amounts of data, it will also mean evolving the architecture of the cloud away from a centralized model to one where computing applications, data, and services are pushed to the periphery (the “edge”) of a network.”105

Excessive data collection deprives the data subject of control over their data. Data that is unnecessary for that purpose should not be collected and stored for the future “just in case” it may be useful for the future.106

As personal data is uploaded to servers, a threat to national security can occur if purpose limitation is overstepped. Sentry mode107 is a burglary alarm where Tesla cars activate their passenger cabin and parking cameras to film the environment and to call a security service when someone approaches the car. Thus, Tesla car in that mode is a video surveillance unit connected to remote service centres – causing issues when soldiers park inside military facilities. 108

Personal data should not be stored for longer than necessary for their declared purposes, but in case of connected cars, the data retention period can be excessive.109 For example, a person could still have remote control after returning rental car.110 Regarding Tesla cars, their privacy policy about data retentions has no clear indication how long the data will be stored, therefore no clear understanding about it is communicated, which indicates to the possibility that data is more prone to be disclosed or reused unauthorized.111 “In particular, the increasing risks of data breaches coupled with the higher likelihood of enforcement action and litigation may nudge businesses to more proactively securely erase personal data.”112

104 P. Nelson. Just one autonomous car will use 4,000 GB of data/day. - https://www.networkworld.com/article/3147892/one-autonomous-car-will-use-4000-gb-of-data/day.html (11.01.2020)


GDPR art 5 (1)(a) and ePrivacy Directive art 6(1) also mention fairness. It is uncertain what additional limitations the fairness principle bring that go beyond what are mentioned in articles 6–9 in GDPR.\(^{113}\) Fairness in essence means that data should never be collected and processed in a way that the individual is not aware of it. As sensors and cameras can process data non-obtrusive, the companies manufacturing IoT devices must inform the users of the data collection and further processing.

Another principle relating to data subject rights is GDPR art 17 - right to be forgotten. Data subject has the right for erasure of data if the personal data is no longer necessary. “The EU right to be forgotten can be conceptualized as taking three forms: the right to have information deleted after a present period; the right to have a clean slate; and the right to be connected to current information and delinked from outdated information.”\(^{114}\) As a data subject has the right to know what data is collected while using the IoT device, the data subject can ask the device manufacturer to erase all data that it hold. In IoT device, enforcing right to be forgotten can be more complex and vague to deal with, because the data moves from one device to another device and ends up in a server, therefore it is harder to track where the data is stored.\(^{115}\) It cannot be forgotten that a lot can be done by the person itself in order to prevent problems in the future. For example, National Automobile Dealers Association released a guide for consumers what kind of data connected cars most likely process and what types of data to remove before transferring the device to another person, and what subscription services to cancel.\(^{116}\) Volkswagen is a good example how to give instructions how to perform a factory reset to remove information stored in your vehicle.\(^{117}\)

In conclusion, the question how to protect data subject rights is at the centre of debate while using connected cars. Although data subject rights are hard to comprehend while using IoT, a lot can be done by the companies to explain how and what. As trustworthiness in the race to be innovative and develop new solutions is the key for selling IoT devices, a lot can be done by the company itself to give instructions and explanations. In the age of digital revolution it is all about connectedness and how devices can interact to each other. Meanwhile, while data is


\(^{116}\) https://www.researchgate.net/publication/331991225_GDPR_Privacy_Implications_for_the_Internet_of_Things


\(^{119}\) Volkswagen Privacy Policy. - https://www.vw.com/privacy/
uploaded to the cloud server, it is hard for the data controller to protect data subject rights. The more sharing, the more risks and the more device manufacturer has to think how to create innovation but at the same time be ready for data subject access requests to delete all the data the IoT device has collected. Even more, how such data collection can not only be a threat to non-compliance of the GDPR be a threat to national security as well. A lot has been done, for example publishing privacy policies, but the level of detailedness can be improved.

3.4. Providing information in conformity with the transparency principle

Transparency principle foreseen in article 5(1)(a) has been already long ago established in the law of the EU and it is an overarching principle of GDPR. It is closely connected to the fairness principle within the same provision. Even though it has been argued, if it possible to equate these principles, it is clear that they are connected, but fairness goes beyond transparency. Initially, article 5(3) of the ePrivacy directive referred to the obligation to provide comprehensive information foreseen in the data protection directive. However, it has been replaced in 2009 by a different regulation focusing more on the consent as described in chapter 2.1 of this work, while keeping the reference to the obligation to provide information.

The transparency principle mostly relates to the section 2 of the chapter III “Information and access to personal data” of the GDPR. Namely, articles 13 and 14 of this section are stipulating a list of information that needs to be provided to the data subject. Furthermore, according to article 15, the data subject has the right to get additional info about the processing of his or her personal data and copies of such data. Additionally, according to the article 12 of the GDPR, the information shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Providing information to the car users in a concise, transparent, intelligible and easily accessible form, using clear and plain language as required by article 12 of the GDPR, can be quite challenging for the controllers. Namely, connected cars include very complex personal data

processing that have different purposes and involve various parties, possibly automakers, insurers, law enforcement authorities and others. Therefore, the underlying information needs to be correctly identified, especially all the stakeholders like controllers, processors and recipients of the personal data and connect them to relevant processing operations.  

The latter is quite important in the cloud computing, where the data transfer between various parties can be made quite easy. Therefore, it is important to make sure that the data subject is aware of those transfers. Furthermore, the transparency needs to be ensured also in the relationship(s) between cloud client and cloud provider and, where relevant the subcontractor. Furthermore, the controller also needs to check carefully the terms and conditions of the cloud provider (including the locations of all the data centres, where the personal data is being processed) to be able to assess them from the data protection point of view.  

Additionally, the user interface design in the screens available in the connected cars is relevant as well. Namely, one of the more general problem with most of the IoT devices is the loss of screen space, which results in difficulties of displaying the privacy policies. However, this is most probably not the case for cars. For example, Tesla has an eight-inch screen, where it manages to show a 15 pages long privacy policy. Furthermore, Audi has changed in some of their models the style of the infotainment unit that now sits on top of the dashboard, hence giving the possibility to increase the screen size. For instance, Audi Q5 has a seven-inch screen with the possibility to increase it to an eight-inch one. Furthermore, they have developed a huge twelve-inch Virtual Cockpit screen for behind the wheel. Lastly, the screen possibilities have been expanded also by Mercedes Benz as their GLE models have a Widescreen Cockpit with a head-up virtual screen above the wheel.

Even in case of reduced screen space, there are different ways to provide information according to Article 29. For example, it is possible to put it on the object itself, using the wireless

127 Carwow. Audi Q5 interior. - https://www.carwow.co.uk/audi/q5/interior (10.01.2020)  
connectivity to broadcast the information. Furthermore, it is also possible to inform users that are located close to the sensor via location and privacy-preserving proximity testing or print on the IoT devices a QR code or a flashcode from which you can get the necessary information.\textsuperscript{129} The most important element of this obligation is the fact that the data subject should not be actively searching for the information themselves. So the controller is the one, who should actively give this information or actively direct the data subject to the right location.\textsuperscript{130}

The general purpose of the connected devices is to blend in with the environment (be unnoticeable). This is also quite easy in many cases as they take the form of familiar objects that include nowadays networking, sensors and other similar features. When it comes to transparency, then this creates risks as people might not be even aware of the relevant processing. For example, in 2014 there was a survey done of twenty popular IoT devices including Nest Thermostat, the FitBit and home monitoring systems. It was concluded that the IoT manufactures were poorly informing users as among others none of the twenty devices had the privacy-related information in their boxes and did not even refer to the existence of it.\textsuperscript{131}

When it comes to vehicles, then different associations have agreed on the privacy principles. For example the U.S. Alliance of Automobile Manufactures has committed to transparency and to providing their users with clear and meaningful notices about the processing of relevant information.\textsuperscript{132} Furthermore, the European Automobile Manufacturers Association also emphasised as one of the data protection principles that they inform their customers about the processing of personal data (including the necessary information about it).\textsuperscript{133}

However, even if the privacy policies are present, then other issues have been expressed. Namely, a number of studies suggest that privacy notices are almost never read.\textsuperscript{134} Furthermore, it has been found that the language in them is exceedingly ambiguous.\textsuperscript{135} When looking into

\begin{enumerate}
\item P. Hacker. \textit{op cit}, p. 274.
\end{enumerate}
some of the privacy policies published on the websites of the car manufactures, then some are more general as well as do not cover very specifically the connected/smart part of the vehicle (e.g. Audi, Volkswagen) than others (e.g. General Motors and Tesla). For example, Audi and Volkswagen generally mention the use of location data, but General Motors and Tesla have a more specific overview, including General Motors clearly connecting the specific data categories with purposes. Furthermore, General Motors has also referred in their privacy statement to other privacy policies that cover also smart or connected services.\footnote{Audi. Reval Auto Esindused OÜ privaatsuspoliitika [Privacy Policy of Reval Auto Esindused OÜ]. - https://www.audi.ee/ee/web/et.html#layer=ee/web/et/models/layer/privaatsustingimused.html (11.01.2020); General Motors. Privacy Statement. - https://www.gm.com/privacy-statement.html?11.01.2020; Tesla. Legal – Customer Privacy Policy. - https://www.tesla.com/en_GB/about/legal#privacy-statement (11.01.2020); Volkswagen. Privacy statement. - https://www.volkswagen.co.uk/privacy/privacy-statement (11.01.2020)}

To sum up, the stakeholders in the smart vehicle industry seem to make an effort to comply with the transparency principle. Furthermore, even though the privacy policies on the websites were in some cases more general, then it might be that in the process of buying the car you get more relevant information for the specific vehicle and its data processing. However, on the other hand, the general obligation to provide information foreseen in GDPR, is also quite difficult and burdensome to be fulfilled as well as due to people not really reading the privacy policies confirmed by studies, then the added value of this can be questionable.

### 3.5. Ensuring the security of processing the personal data

Security of information can be considered as one of the cornerstones of privacy, because keeping your personal data safe will ensure that you will remain “private”. Furthermore, lack of security can have quite severe consequences regardless if the relevant data will be unlawfully erased or used without your agreement. Therefore, the security obligation of the controllers and processors stipulated in article 32 of the GDPR, is extremely important. It is also closely connected to the integrity and confidentiality principle foreseen in article 5(1)(f) of the GDPR.

On an international level, access control and encryption have been mentioned as typical instruments of security.\footnote{M. Maurer et al. Autonomous driving. Springer. Ladenburg: 2015. p. 511.} Article 32(1) of the GDPR gives a non-exclusive list of technical and organisational measures that shall be implemented, as appropriate, to ensure the necessary level of security. For example, encryption has been explicitly mentioned along with pseudonymisation. Even though access rights are not specifically listed there, then the
organisational rules should definitely cover these as well. However, the necessary level of security will depend on different elements like the risks for the rights and freedoms of natural persons, the availability of relevant security features as well as the costs to implement these.

Furthermore, article 4 of the ePrivacy directive sets a similar obligation to the provider of a publicly available electronic communications service. Even though the article 29WP has seen the need to extend the security requirements in a way that the coverage of IoT devices would be stronger, the initial proposal by the European Commission repealed the security rules to eliminate regulatory duplication (in some cases the reference to the article 32 of the GDPR was made, e.g. article 8(2)(b)). In the latest version of the Council of the EU for this proposal, the reference has been added also to the security obligation of providers of public electronic communication networks stemming from article 40 of the European Electronic Communications Code, which was adopted after the previously mentioned proposal. The European Parliament has followed a similar line.

Following the above (including the chapter 2.1), there is legal uncertainty, what is exactly applicable from the legislation specific to electronic communication. However, as mentioned before as well as confirmed by the European Commission, the rules are similar and even duplicating each other. Therefore, at this stage, without the ePrivacy Regulation replacing the ePrivacy directive, the entities that qualify as controllers or processors of the smart vehicles or providers of the publicly available electronic communications service in relation to those vehicles shall assess the level of security needed and ensure it to the extent necessary.

Security is often seen as an afterthought, even though failure to achieve the relevant level may entail severe safety consequences (e.g. flawed decisions, financial losses, disclosure of personal data, and potential life-endangering actions like road accidents and vehicle immobilisation, financial losses). Namely, the attacker might not merely steal data, but disable the security

---

features of the vehicle and even gain control over it. Therefore, it may lead to endangering road safety for everybody – drivers, passengers and pedestrians.143

Furthermore, it is often quite difficult to secure the IoT devices. Firstly, because of technical reasons like using the wireless communication infrastructure that leads to vulnerabilities regarding physical or proxy attacks and eavesdropping and the non-capability of establishing an encrypted link by most sensors. Secondly, due to business reasons, because building and using an IoT device covers a very complex supply chain.144

Consequently, as the wireless capabilities145 as well as the complexity is increasing, then it gets more challenging to secure the components of the vehicle146 and connected cars are equally vulnerable to security risks.147 Several research publications cover the attacks targeting smart cars and proof-of-concept remote attacks148 on different type of carjacking cases in 2013149 as well as in 2015 and 2016.150 Furthermore, a team of researchers, has analysed 367 publicly reported incidents on the smart mobility ecosystem since 2010, including almost half of them in 2019 (as of 7th of December 2019).151

For example, just last year a man was using an app to remotely hack his ex-girlfriend’s car to see her location and play tricks with the keyless-entry of the Land Rover.152 Furthermore, Tesco parking app exposed 10s of millions of unsecured automatic number plate recognition images, even though luckily the drivers were not visible.153 Additionally, thieves could steal a Tesla just under 30 seconds by hacking the keyless entry access. Lastly, in Netherlands and Belgium some people hacked the trucks’ driving time and speed meters.154

152 C. Chin. op cit.
As mentioned in chapter 3.1, the smart vehicles use cloud computing solutions, which adds to the risks on the security. On the scale of most common attack vectors, servers (including cloud) have been found to be on the second place, representing ca 27% of incidents in 2019. It has been viewed as one of the greatest threats to privacy and tied to numerous data protection risks. For example, without an effective protection, the hackers can use a simple laptop to run from the cloud commands to override the ones operating the vehicle.

On the other hand, there are also some indications that companies are making further steps to increase the security. For example, companies are willing to invest their resources to mitigate the risks by offering monetary awards to hackers and researches for finding security vulnerabilities in their servers and products. Furthermore, the previous attacks have also raised the security awareness of the industry, which has led to several initiatives for the purpose of ensuring more secure vehicles. Lastly, the industry is looking into keeping the flows of data coming from outside of the vehicle separate from the car safety architecture and manage it via a facility that is outside of the vehicle.

To sum up, even though the companies are working on the security matters, it might not be enough or as proactive as needed considering the risks the smart vehicles entail. Furthermore, as we are moving towards more connectivity as well as more autonomy by the vehicles, then the risks are also increasing. Therefore, it is crucial to ensure the compliance with the security obligation to the highest extent.

3.6. Changes to the business model and legal framework

Giving practical value to current work, it is possible to draw conclusions from the aforementioned analysis. As the world is constantly evolving, especially in the digital field and

---

159 C. Marroni. op cit, p. 10.
the number of IoT devices being sold is increasing every year\textsuperscript{161}, new emerging business models need to adapt to the market situation. It is possible to adjust the business model, but at the same business model modifications will not change the legal framework. It is up to the lawmakers at EU level to notice the importance of being connected digitally in order to boost the economy.

In order to process data lawfully and respectfully towards data subjects, user empowerment is essential in the context of IoT. IoT manufacturers should publish privacy policies in a simple and understandable way, using plain language. Where possible, IoT manufacturers should consider making the relevant data protection impact assessments available to the public. New technology should be built in a way that tracking data and deleting it is simple and easily accessible. This enable the user to have a focus on him/her and create a widespread knowledge system in the society. Device manufacturers should inform users about the type of data that are collected by sensors and cameras, how it is further processed, how it will be processed and combined and to whom it is shared with. An application should be available to alert a user that the same device is used by someone else.

As to changing the legal framework, the process is ongoing to revising the ePrivacy directive\textsuperscript{162}. But moreover, the discussions about ethics are the basis of making regulatory decisions. Until there is no real compromise between what is acceptable use of personal data and how to create innovation at the same time, it is very hard to make any changes to the overall legal system. As technology is constantly evolving, for example besides IoT, artificial intelligence is also something new and evolving, then it is quite difficult to propose relevant changes on time that would be also fit-for-purpose. Regulations should be developed within the existing legal framework so it would not stop innovation and would still be applicable to the digital solutions. It should not try to exhaustively solve all emerging problems into details, but create a framework of principles.

Regarding ensuring transparency, there is not a lot one can do in relation to the changes in the business model rather than reducing the complexity of it. However, this would basically entail reducing the connectivity, the added value as well as the main purpose of the IoT devices. Therefore, the only suggestion to be made for the smart vehicle industry is to make sure that


they understand the whole business model themselves enough to be able to inform the data subjects adequately. On the other hand, the GDPR would merit an assessment in relation to the obligation to proactively provide for information to the data subject as stipulated in article 13 and 14, because the list of information is quite long, which results in very long privacy statements that nobody really has time to read.

Therefore, it could be useful to limit the proactively provided information to a bare minimum of the most important information (e.g. that the personal data is being processed and for what purposes). All other information could be accessible by the access request of the data subject. Of course this approach might raise concerns, if the transparency is really succeeded as most of the consumers might not be very active asking for the info that interests them. Therefore, a more balanced approach might be to use the layered solution, whereas at first sight minimal information is given and the data subject may navigate to the second layer of more thorough information. However, this is already possible under the current legislation and would just require a more active implementation from the industries.163

Lastly, the security should be a so called forethought, i.e. the industry should be more proactive in their business model and not only reacting to the threats. Different privacy protections could be used for security like network restrictions, disabling by default non critical functionalities,164, isolating data at different entities and storing the personal data as much as possible under the control of the user.165 Additionally, from the perspective of the legislation, there is more legal clarity needed in respect to the security obligation in the electronic communication regulations due to the overview described in chapter 3.5.

---

SUMMARY

Technical possibilities are increasing in current digital society and different intelligent systems are developed around the world. Innovation can be found in the automotive industry, which took the centre stage of the current work. Smart vehicles are becoming a new normality, but a lot of misconceptions are still surrounding the IoT. Even though there are advantages of these vehicles, they bring up several questions regarding compliance with GDPR and ePrivacy Directive.

The main aim of this work was to analyse a working model of smart vehicles, as one use case of IoT with cloud computing from the point of view of GDPR and ePrivacy Directive and give recommendations to amend the business model or the legal regulations. For a better understanding of the field, a more general background of what does IoT exactly mean was additionally covered, including the meaning of it as well some examples were provided.

Existing legal framework related to the use of the IoT can be divided in 3 categories: rules regulating the electronic communications services and networks, horizontal consumer protection rules and industry specific rules. As the scope of current work was limited, the most relevant provisions from ePrivacy Directive and GDPR were analysed in 4 combination categories: lawfulness, limitations, security and transparency.

Regarding having a lawful basis for processing data of smart vehicle users, it is still unclear how data is processed, combined and shared in mentioned use cases. Ensuring the purpose limitation, data minimisation and storage limitation should also be important to a IoT manufacturer and these principles should be incorporated to a business process. Although data subject rights are hard to comprehend while using IoT, a lot can be done by the companies to explain how and what. As trustworthiness in the race to be innovative and develop new solutions is the key for selling IoT devices, the companies themselves shall commit to give instructions and explanations.

Providing information in conformity with the GDPR is important to stakeholders to create transparency and companies are making an effort to comply with it. However, on the other hand, the general obligation to provide information foreseen in GDPR, is also quite difficult and burdensome to be fulfilled and the added value of it is arguable as the people do not really
read the privacy policies. Security on the other hand is often seen as an afterthought, even though failure to achieve the relevant level may entail severe safety consequences. Furthermore, it is often quite difficult to secure the IoT devices, as the wireless capabilities and the complexity is increasing. Adding cloud computing solutions to IoT increases even more the risks on the security.

There are several things companies themselves can do to improve compliance. Most likely the cheapest solution would be to draft simpler and easily readable, but also more detailed privacy policies. Furthermore the devices should be designed in a way, that it is easy to locate, track and delete data in order to control the lifespan of user data. The smart vehicle industry companies should understand enough the whole business model themselves to be able to inform the data subjects adequately.

The main recommendation to the lawmakers as regards the changes of the legal framework would be to act in a way it foresees the future and emerging new technologies and no extensively detailed regulations are passed. For example, it could be useful to limit the proactively provided information foreseen in GDPR to a bare minimum of the most important information and all other information could be accessible by the access request of the data subject. Additionally, some legal certainty would be necessary regarding the regulations applicable to the field of electronic communication.

It is very important to keep the discussions ongoing in order to find the best solutions for IoT device market. After all, the future of automobiles will be shaped hand in hand by the industry and legislative bodies. IoT and smart vehicles are here to stay and it is very important that the discussions in both levels, industry and legislative level, will continue, especially dialogue between the two, in order to develop the best legislative changes and industry practice for the IoT device users.
CONTRIBUTION OF GROUP MEMBERS

The introduction and first chapter was written by Merili Oja and the second chapter and summary by Krete Paal. The work of the third chapter was divided between both group members. Namely, Merili Oja wrote the first, fourth and fifth subchapter and Krete Paal wrote the second and the third subchapter. The introduction and the sixth subchapter were written in collaboration.
ABBREVIATIONS

Article 29 WP - Article 29 Data Protection Working Party
GDPR - General Data Protection Regulation
IoT - Internet of Things
REFERENCE LIST

Literature

2. A. Henschke. The Internet of Things and Dual Layers of Ethical Concern. Oxford Scholarship Online. 2017
7. D.T. Bourgeois. Information Systems for Business and Beyond. Open Text Book Challenge by The Saylor Academy, 2014

Legal acts


Guidelines and policy documents


Other

52. A. Greenberg. Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video). Forbes: 2013. -


