D.7.1 Legal Requirements for Trust in the IoT

[K.U.Leuven]

FINAL

Authors:
Jos Dumortier (K.U.Leuven)
Niels Vandezande (K.U.Leuven)
Christina Hochleitner (CURE)
Kristin Fuglerud (NR)

Version: 1.0
Date: 25/03/2011
Dissemination level: (PU, PP, RE, CO): PU

Project Co-Funded by the European Commission within the 7th Framework Programme
Abstract

The Internet of Things (IoT) will connect a large number of communication and information systems. These systems will be part of everyday life in the same way mobile phones have become part of our lives. The information security properties of the IoT are often difficult to understand for its users, because they are hidden in pervasive systems and small devices manufactured by a large number of vendors. Trustworthiness, security functions and privacy implications are vast, and must be assessable to users and consumers.

The main focus of the uTRUSTIt project lies in its objective to integrate the user directly in the trust chain, guaranteeing transparency in the underlying security and reliability properties of the IoT. The results of uTRUSTIt enable system manufacturers and system integrators to express the underlying security concepts to users in a comprehensible way, allowing them to make valid judgments on the trustworthiness of such systems. Further, uTRUSTIt’s design guidelines on trust help the industry to implement the trust-feedback toolkit developed by uTRUSTIt in a secure, usable and accessible way.

In this document, the main legal issues regarding trust in the IoT will be analyzed. These issues, data protection and liability, will be further analyzed to ensure compliance by device manufacturers as a prerequisite for trust. Further analysis will address specific problems concerning data protection and liability in relation to the IoT. Based on the issues identified in the analysis of existing data protection legislation and the current legal framework on liability, requirements will be formulated in order to ensure compliance with these specific branches of law related to the IoT.
Table of Contents

1. INTRODUCTION .................................................................................................................. 6
   1.1 Background ................................................................................................................... 6
   1.2 Scope of this Deliverable .............................................................................................. 6

2. LEGAL FRAMEWORK OF TRUST ................................................................................... 7
   2.1 Trust in social sciences ............................................................................................... 7
   2.2 Trust in the information society ................................................................................. 7
   2.3 Trust and the law ......................................................................................................... 8
      2.3.1 Business trust ....................................................................................................... 8
      2.3.2 Investment trust .................................................................................................. 9
      2.3.3 Trust law ............................................................................................................ 9
      2.3.4 Legitimate expectations ...................................................................................... 9
      2.3.5 Trust in evidence .............................................................................................. 10
      2.3.6 Gaps in legal trust .............................................................................................. 11

3. LEGAL RISKS OF THE INTERNET OF THINGS .............................................................. 12
   3.1 European Commission ............................................................................................... 12
   3.2 European Parliament .................................................................................................. 13
   3.3 Article 29 Working Party ........................................................................................... 13
   3.4 Other works ............................................................................................................... 13
   3.5 Conclusion .................................................................................................................. 14

4. PRIVACY POLICY FRAMEWORK AND REQUIREMENTS .............................................. 15
   4.1 General privacy regulation ........................................................................................ 15
      4.1.1 Directive 95/46/EC ............................................................................................ 16
      4.1.2 National privacy legislation .............................................................................. 24
      4.1.3 Review of Directive 95/46/EC ......................................................................... 25
   4.2 Specific privacy concerns relating to the IoT .............................................................. 27
      4.2.1 Controller versus processor ............................................................................ 27
      4.2.2 Limits of the concept of personal data ............................................................. 29
      4.2.3 Application of the household exception ......................................................... 31
      4.2.4 Proportionality and how to implement in the IoT ......................................... 33
      4.2.5 Sensitive data .................................................................................................. 34
      4.2.6 How to obtain the data subject’s consent? ...................................................... 37
      4.2.7 How to inform the data subject? ..................................................................... 39
      4.2.8 Data access rights ......................................................................................... 41
      4.2.9 Radio-frequency identification ....................................................................... 43
   4.3 Conclusion ................................................................................................................... 46

5. LIABILITY ISSUES .............................................................................................................. 49
   5.1 General liability regulation ....................................................................................... 49
   5.2 Specific liability concerns relating to the IoT ............................................................ 52
      5.2.1 Implementation of product liability in the IoT ................................................. 52
      5.2.2 Liability of service providers ........................................................................... 54
      5.2.3 Contractual limitations of liability .................................................................... 57
      5.2.4 Liability under data protection regulations ..................................................... 59
      5.2.5 Cross-border aspects ....................................................................................... 61
      5.2.6 Role definition ............................................................................................... 63
   5.3 Conclusion ................................................................................................................... 65

6. SUMMARY OF LEGAL REQUIREMENTS ...................................................................... 68

7. REFERENCES ...................................................................................................................... 70
7.1 Legislative Sources .................................................................................................................. 70
7.2 Case law .................................................................................................................................. 72
7.3 Legal literature .......................................................................................................................... 73
## List of acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy and data protection Impact Assessment</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-Frequency Identification</td>
</tr>
</tbody>
</table>
1. **Introduction**

1.1 **Background**

Work under work package 7 will establish a set of clear legal privacy policies and legal requirements for trust in the IoT and take into consideration all relevant legislation relating to privacy and the protection of personal data. It comprises the legal evaluation of the developed prototype in order to keep legal compliance. Furthermore, this WP will prove whether uTRUSTit’s activities and in particular its results are in accordance with Europe’s ethical values and standards.

1.2 **Scope of this Deliverable**

This report will present the final results of the research performed in task 7.1 Legal Requirements for realizing Trust in the IoT. It will not only analyze the general legal privacy and liability framework that devices should comply with as a prerequisite for establishing trust in such technology, but also focus on the specific issues of these legal frameworks in relation to the IoT.

This legal task will first look at the issue of compliance with existing data protection legislation as a prerequisite for trust. Further, this task will outline the potential problems and identify the specific legal issues involved in incorporating such trust in the IoT.

The task will furthermore examine the current legal framework on liability. After a general analysis of liability provisions to be found under current EU legislation, this deliverable will address a number of specific issues of liability in relation to the IoT. These analyses will also highlight the benefits and limits of a contractual framework to be agreed on by the device manufacturers of the uTRUSTit platform.

Based on the issues identified in the analysis of existing data protection legislation and the current legal framework on liability, requirements will be formulated in order to ensure compliance with these specific branches of law related to the IoT.

Future work under WP7 will include a final legal evaluation of the application scenarios and architecture by taking into consideration the list of requirements drawn in this WP. Moreover, the requirements formulated within the present deliverable will be applied to the scenarios developed within the framework of D2.2 Definition of User Scenarios. This will lead to the formulation of more practical legal requirements and will result in two deliverables: D7.2 Legal Requirements for the Office and the Home Scenario and D7.3 Legal Requirements for the eVoting Scenario.
2. **Legal framework of trust**

2.1 **Trust in social sciences**

The idea of trust can be found in many disciplines, both in social sciences and exact sciences. In social sciences – sociology, psychology, philosophy and economics – trust is usually perceived as an attribute to relationships between people. In essence, trust is the situation whereby one person believes that another person will act in a certain way. One could go as far as describing this as a situation of reliance, although from a philosophical level one could also argue that trust and reliance are different concepts [McLeod 2006]. It is argued that trust involves the risk of being betrayed, while reliance only involves the risk of being disappointed.

From a psychological point of view, trust is one of the main foundations of psychological development. In Erikson’s stages of psychosocial development [Erikson 1959] trust is the first characteristic learned by a newborn infant. If the infant is exposed to warmth and affection in a secure environment, it will learn to trust its parents. If primary caretakers fail to provide such secure environment, the newborn infant will begin its lifespan with a sense of mistrust against the world. Throughout the individual’s lifespan, trust will remain an important factor in social relationships, with a lack of trust in certain situations even leading to lesser performance on a social, academic and professional level.

The role of trust in social relationships is the main sociological focal point in this subject. Here, trust is perceived as a social construct that serves as a bet for future possibilities. If one person decides to trust another person and thus believes that this person will act as he expects him to, they can engage in activities that would not have been possible without such trust. However, if the trusted person does not act as expected, trust is breached and the person conferring the trust upon the other may be left off worse than he was before this trust relationship. From a sociological point of view, trust therefore inherently constitutes a risk.

The idea of trust as a form of risk-taking can also be found in economical theories. Like in sociology, trust is perceived as enabling new possibilities, leading to new business opportunities and lowering transaction costs [Andreoni]. Trust could therefore lead to economic growth, yet conferring a too high level of trust on transactions with a lower level of trustworthiness could in turn lead to exploitation. The level of trust and trustworthiness should therefore be at the same height. Economics theory also develops games of trust to prove theories such as the Nash equilibrium, the prisoner’s dilemma [Kuhn 2007] being the most well known example. In this theory, the correlation between trust and risk-taking becomes apparent.

2.2 **Trust in the information society**

In more recent years, the concept of trust has broadened its scope from solely inter-human relationships to interactions between the devices of the information society and their users. In the specific field of information security, this is referred to as computational trust. Trusted authorities or

---

1 General sociological work on the concept of trust has been performed [Luhmann 1979].
2 On trust in sociology [Lewis 1985]. See also [Gambetta 2000].
3 A comprehensive study of trust in economics, with focus on e-economy can be found at [Guerra 2003].
4 One example includes Trusted Computing, in which cryptography is used to ensure that a computer will behave consistently in expected ways. On Trusted Computing’s impact on privacy [Hansen 2004]. Also the Article 29 Working Party has adopted a working document on Trusted Computing [Working Party 86].
5 Further research on the more technical aspects of the concept of trust has been performed elsewhere in the uTRUSTit project [utrustin D3.1].
user trust can, for one, be generated through cryptography, the most well known mechanisms being Public Key Infrastructure (PKI) and Kerberos. The rise of the Internet as one of the main media for communication and social interaction and the rise of e-commerce have increased the need to establish a trustworthy relationship between the information system and its human users.\(^6\)

With the coming realization of the IoT, whereby computational connections and networks will become even more pervasive and ubiquitous, the user is ever more required to confide in the devices of the information society. As learned from the economical concept of trust, conferring trust upon a new and uncertain relationship may lead to benefits for both parties, whereas conferring a too high level of trust in an untrustworthy relationship may lead to exploitation. Alternatively, conferring a low level of trust in a relationship may lead to missed opportunities and may thus hinder economic growth. In order for the citizen to fully benefit from the possibilities created by the information society, and in order for him not to fall prone to exploitation, the IoT will have to display trustworthiness of the same level as the trust required from the user.

In order to measure the degree of trust conferred by a user, psychological and sociological scholars have made attempts at developing trust metrics.\(^7\) Such metrics could also be applied to computational sciences and could guide the process of augmenting trustworthiness to correspond to the user’s trust. However, as trust is a complex, subjective and personal matter, one may argue that it could very well be impossible to develop an accurate method of measurement.

The need for trustworthiness of information systems has lead to the growth of trust services. One approach is the creation of a trusted third party. Hereby both parties in a transaction confide in the trustworthiness of the third party thereby securing their own transaction. The third party vouches for the trustworthiness of the parties in the transaction. An example here is the qualified electronic signature, whereby a third party – the Certificate Authority – provides a digital certificate of ownership of a certain public key. In transaction, the opposite party will rely on the trustworthiness of the Certificate Authority to trust the digital certificate and therefore the party owning said certificate.

\subsection{2.3 Trust and the law}

As made obvious by the previous overview, most disciplines have rather distinct views on the precise scope and contents of the concept of trust. However, most disciplines briefly discussed here seem to share certain basic notions on trust. All disciplines seem to agree that trust involves one person taking a risk to confide in another person, herewith hoping he will benefit from this trust relationship. Although conferring trust should lead to a more beneficial position, most disciplines seem to agree that one should not confer a too high degree of trust upon an uncertain relationship, as such could lead to negative outcomes like exploitation. The idea of conferring a degree of trust equal to the degree of trustworthiness of the opposing party, an idea found in economics theory, is currently one of the main issues regarding the IoT, as it currently is uncertain how trustworthiness can be attributed to such ubiquitous networks.

The discipline of law, however, does not follow the path set in other disciplines. Although the concept of trust can be found in various legal systems all over the world, there seem to be highly different incarnations of trust in the law.

\subsubsection{2.3.1 Business trust}

One of the main examples of trust in the law refers to the business trust, an entity formed with the intention to create a monopoly on a certain market. As pointed out in economics theory,

\begin{footnotesize}\begin{itemize}
\item \(^6\) See, for instance, on trust building for consumer transactions [McKnight 2002].
\item \(^7\) The idea of measuring trust and trustworthiness to find the right balance can also be referred to as trust management [Josang 2005].
\end{itemize}\end{footnotesize}
monopolies restrain trade and fix prices, leading to inefficient markets. Therefore, the idea of antitrust was introduced in the law, with early examples being the US Sherman Act\textsuperscript{8} and the US Clayton Act\textsuperscript{9}. These acts have become the basis of what is now known in a broader term as competition law. Despite its name, the business trust has no connection to the concept of trust as found in social sciences or in information security.

2.3.2 Investment trust

Another incarnation of trust in the broader field of business law is the investment trust. This is a company — normally in the form of a public limited liability company — that carries out a collective investment scheme. Investment trusts are closed-end funds, indicating that only a limited number of shares are issued. As an investment company, it is clear that the investment trust entails risks for its shareholders. However, by diversification the investment risk is reduced. Therefore, although there is no direct connection to the concept of trust in social sciences and information security, the investment trust does build upon the idea of a person taking a calculated risk in order to reap benefits from the risk taken.

2.3.3 Trust law

First of all it should be noted that trust law — despite its name — bears no connection to antitrust law. Trust law governs the specific figure of the trust. In this figure, the settlor establishing the trust confides certain property to a trustee of his appointing. The trustee, upon accepting his duties, is bound to manage said property for the benefit of the beneficiary appointed by the settlor. The relationship and division of duties and liabilities between the settlor, trustee and beneficiary is laid down in a deed of trust or through a will. By establishing the trust, the legal ownership of the property is transferred to the trustee, while the beneficiary receives economic ownership.

The establishment of the trust creates a fiduciary relationship between the parties involved. The settlor confides in the fact that the trustee will provide the highest standard of care in his management of the property in benefit of the beneficiary. This concept of conferring trust upon another person in order to gain benefit — in casu not for oneself but for another — is rather similar to the earlier discussed concept of trust in social sciences. The main difference is that the fiduciary relationship is strictly regulated by law — equity in the UK — while other trust relationships may rely more on a non-contractual relationship.

The figure of the trust, finding its origins in the Roman fideicommissum, was mainly developed in the UK. The trust can also be found in other common law States, as well as in civil law States. It should be noted, however, that the precise scope of the concept of trust in these other legal systems can bear significant differences to the British trust.\textsuperscript{10}

2.3.4 Legitimate expectations

While trust law already hints at the scope of the concept of trust found in social sciences and computer security, there are other instances in which one can find a level of trust in the law. One example includes the notion of legitimate expectations. This notion can be found in administrative law as a principle of good governance.\textsuperscript{11} The idea is that if the behavior or acts of a public legal entity raise certain expectations with a citizen, then the citizen may rely on the fact that the public legal entity will continue such behavior or acts in order to meet the citizen’s expectations. Public legal entities are therefore required to display fairness and reasonableness when a citizen has certain expectations following a promise made by said public legal entity or by its long-standing practices.

\textsuperscript{8} Sherman Antitrust Act of 1890 (30 February 1890)
\textsuperscript{9} Clayton Antitrust Act of 1914 (Pub.L. 63-212).
\textsuperscript{10} A comparison between different national implementations of the trust can be found at [Hansmann 1998].
\textsuperscript{11} In Belgium and the Netherlands referred to as “algemene beginselen van behoorlijk bestuur”.

12/04/2011

Page 9 / 75
This theory was further developed in the Wednesbury case. The core of this case – later further developed by the House of Lords – is that if a decision of a public legal entity is so unreasonable that no reasonable authority would have made the same decision, then that decision should be subject to judicial review. The theory of legitimate expectations therefore allows for the citizen to ‘trust’ a public legal entity on its acts and behavior. This is, however, a different concept of trust than the one earlier deduced from economics and sociology. Legitimate expectations do not necessarily require an active form of risk-taking from the citizen, but rather allows an attitude of reliance.

A similar concept can be found in private law. If, during the negotiation phase of a contractual agreement, one of the parties makes certain statements, the opposing party may in, all fairness and reasonableness, rely on these statements. Future retraction of those statements will then be made impossible. The reliance theory states that a party relying on statements made by the opposing party, from which he could reasonably conclude that parties’ intent, may expect these statements to have lead to the conclusion of the agreement.

2.3.5 Trust in evidence

Another incarnation of trust can be found in evidence law. Here it comes in the guise of a fiction of sorts in which evidence is considered as valid, once it satisfies certain formal requirements. This can be illustrated by an example, for instance the case of a written contract between parties. As it is virtually impossible for a court to conduct a full and thorough investigation into the authenticity and integrity of each contract that passes before it, courts will award legal validity if certain requirements are met. Such requirements may include the issuance of one copy for each party to the contract, the presence of a signature of opposing parties on each party’s copy, consecutively numbered pages, etc.

Legal validity of evidence is therefore based on a sort of trust in the ability of the established criteria to filter out evidence that is deemed untrustworthy. The acceptance that a piece of evidence is truly what it purports to be is therefore only established by a reasonable certainty and not by an absolute certainty.

Regarding evidence law and the IoT, it should also be stated that various legal systems around the world are still having difficulties in fully integrating the notion of electronic documents, electronic transactions and the resulting electronic evidence. Although the EU has already made laudable efforts in adopting legal instruments on e-commerce and electronic signatures, with supporting provisions found in the tax directive amongst others, one can still discern a certain lack of trust towards all things “e-” in the field of evidence law. Paper documents are often still attributed a higher legal validity, solely

13 Lord Diplock formulated this as: “[...] a decision which is so outrageous in its defiance of logic or of accepted moral standards that no sensible person who had applied his mind to the question to be decided could have arrived at it.” Council of Civil Service Unions v Minister for the Civil Service, [1985] AC 374, p18.
14 See, for instance on reliance theory in the US [Cohen 1933]. The Dutch Supreme Court ruled on this in: HR 11 December 1959, Eelman/Hin, NJ 1960, 230. For a summary yet critical overview of reliance theory in Belgium (vertrouwensleer), see [Cauffman 2005].
15 In general on Belgian evidence law [Storme 2001]. On formal requirements in Belgian civil law [Van den Eynde 2001].
16 A concise overview of the issues in authentication for e-commerce [Schapper 2006].
on the basis of the use of paper as the medium for displaying the information contained in the document.

2.3.6 Gaps in legal trust

As can be concluded from this overview of a number of different incarnations of trust in legal science, there are fields in which a legal concept of trust shows certain similarities to the concepts of trust found in social sciences and in information security. On the other hand, there are legal concepts designated as a form of trust that display many divergences from the concepts of trust found in other sciences.

In general, one can conclude that the concept of trust has certainly found its way into the legal system, albeit in highly diffuse and divergent forms. In the current legal reality, there is no overarching principle of trust that can be applied to different branches of law, let alone to a matter that is as cross border and embedded in information technology as is the IoT.

In order to propose a more coherent legal concept of trust that could be applied to the IoT, one will first need to examine the specific legal risks associated with the IoT. Such analysis will be conducted in the following sectors.
3. **Legal risks of the Internet of Things**

As indicated in sector 2, there is currently no coherent legal framework on trust in the EU or the Member States. Therefore, one will need to analyze the technicalities of the IoT and the implementation thereof, in order to deduce the legal risks that are of specific importance to the IoT. Once the main legal risks to the IoT have been established, they can be further explored in order to provide for an adequate legal response. Thus a proposal for requirements for a legal framework for trust in the IoT can be established. These requirements will be summarized under section 6.

In the following analysis, policy documents and opinions of advisory bodies and scholars will serve as a means for determining the main legal risks of the IoT.

3.1 **European Commission**

In a 2009 communication, the European Commission outlined an action plan for Europe on the IoT.\(^{20}\) In this action plan, the Commission expects the applications of the IoT to:

> …greatly contribute to addressing today’s societal challenges: health monitoring systems will help meet the challenges of an ageing society; connected trees will help fight deforestation; connected cars will help reduce traffic congestion and improve their recyclability, thus reducing their carbon footprint. This interconnection of physical objects is expected to amplify the profound effects that large-scale networked communications are having on our society, gradually resulting in a genuine paradigm shift.\(^{21}\)

Given the deep societal changes expected from the IoT, the Commission advises to not leave its development to the private sector, but to involve EU policy makers and public authorities. Therefore the Commission identifies the following 14 action points:

1. Governance
2. Continuous monitoring of the privacy and the protection of personal data questions
3. The ‘silence of the chips’
4. Identification of emerging risks
5. IoT as a vital resource to economy and society
6. Standards mandate
7. Research and development
8. Public-private partnership
9. Innovation and pilot projects
10. Institutional awareness
11. International dialogue
12. RFID in recycling lines
13. Measuring the uptake
14. Assessment of evolution

In summary, one can conclude that action points 1, 2 and 3 relate to issues concerning privacy and data protection. Action points 1 and 5 raise questions on liability issues. Also regarding security


\(^{21}\) [Ibid.], 2.
issues – whereby action points 4 and 5 indicate that technologies such as RFID will be used – raise questions of privacy and data protection. Data protection and liability can therefore be indicated as two domains in which a more coherent legal framework applicable to the IoT would be needed.

The Commission has already adopted a recommendation with regards to RFID. In this recommendation the Commission stresses the need for a full assessment of the impact of RFID on privacy and data protection.

3.2 European Parliament

Also the European Parliament has conducted research on the IoT. In this report the European parliament moves a motion for a resolution on the IoT. Also here, the focus lies on an adequate privacy policy framework, governance and liability, as well as on the use of RFID as the main identification technology for connection to the IoT. This resolution was adopted on 15 June 2010.

3.3 Article 29 Working Party

The Article 29 Working Party has not yet adopted a working paper on the subject of the IoT. However, previous work of the Working Party corresponds to a number of the issues that were indicated in, amongst others, the European Commission Communication of 18 June 2009.

Work of the Article 29 Working Party of use for the present subjects includes opinions and consultations on RFID, on accountability, on the interpretation of the principles of Directive 95/45/EC and on future reviews of that directive [Working Party 169].

These works will be used in further legal assessments throughout this document.

3.4 Other works

Much has been written on the IoT since the term was first coined in the late 1990’s, including works from other governmental entities, regulatory bodies and scholars.

The International Telecommunication Union (ITU), for one, warns that privacy concerns regarding the IoT may eventually hinder its full implementation [ITU 2005]. This sentiment is not shared by the US National Intelligence Council (NIC); they only refer to regulatory concerns and make no mention of privacy-related issues [NIC 2008]. These works of governmental entities and regulatory bodies, however, tend to focus on the actual implementation of and expected economic benefits from the IoT.
The challenges posed by the IoT to privacy data protection, as well as regarding liability issues, are mainly addressed in the scholarly community.\textsuperscript{30} As RFID is one of the main technologies that will be used to implement the IoT, it has even been suggested to not treat RFID and the IoT as separate matters, but to refer to these concepts as equivalents [Buttarelli 2010].

As is the case for Article 29 Working Party opinions, other governmental, regulatory and scholarly works on privacy and data protection – including the use of RFID – as well as on liability issues, can be used as suitable source material for further analysis of the specific legal issues regarding the implementation of the IoT.

\textbf{3.5 Conclusion}

From the previous policy documents and papers it becomes apparent that a number of legal issues concerning the IoT require a more coherent legal framework that is properly adapted to the specific challenges posed by the IoT.

In general, one can conclude that the main challenges indicated here can be categorized under the headers of data protection and liability. Specific issues on data protection and liability will therefore be further explored in the following sectors in order to establish the requirements for a legal framework for trust in the IoT.

\textsuperscript{30} See for instance on privacy and security challenges [Weber 2010]. See also [Atzori 2010]. Also on privacy, but including data accountability [Mayer 2009]. On RFID [Dobson 2006].
4. Privacy policy framework and requirements

As explained in sector 3, one of the main legal risks associated with the IoT is how to comply with current and future privacy regulations. As privacy is becoming more of a genuine concern to the citizen and as threats to the citizen’s privacy are becoming more pervasive, it becomes clear that providing a satisfactory level of privacy protection will be one of the most pressing issues to be resolved before expecting the citizen to put his trust into the IoT. Therefore, this sector aims to provide a more coherent view of the current legal framework regarding privacy protection, with specific attention to the main privacy concerns relating to the IoT.

First, an overview will be provided of the current legal framework regarding privacy protection in the EU. More in detail, the main focus of this sector will lie on the EU framework regarding data protection found in Directive 95/46/EC. Given the nature of a directive and its need for national implementation by the EU Member States, a concise overview will be provided on the major differences in the national implementations of this directive by the Member States and the consequences of this divergence for a pan-European implementation of the IoT. As Directive 95/46/EC is currently impending review, this sector will also look forward to the expected changes that may have an influence on the IoT.

Second, this sector will take a closer look at some of the more specific privacy concerns relating to the IoT. Some of these issues – such as the line between the notions of controller and processor, the limits of the concept of personal data, the application of the household exception, the implementation of the principle of proportionality and the scope of the concept of sensitive data – focus on the limitations of the definitions currently employed in the EU legal framework on data protection, while other issues focus more on the interaction with the data subject – such as how to obtain the data subject’s consent and how to inform this person, as well as his data access rights. Under this sector, the use of radio-frequency identification (RFID) will also be analyzed. While RFID is not directly mentioned in Directive 95/46/EC, this technology can be used to process personal data. In section 3.1, European Commission, it was indicated that the use of RFID can be considered as one of the main building blocks of the IoT. This, combined with the potential privacy implications of RFID, justify the analysis of this technology in consort with the analysis of specific issues regarding the processing of personal data in relation to the IoT.

4.1 General privacy regulation

From the following overview of legal instruments regarding this matter it becomes apparent that privacy regulations have only become widespread and commonly accepted since the second half of the 20th century. The right to privacy therefore is a relatively young notion, although one may argue that the need for privacy even predates humanity. Even in several animal species one can discern a territorial behavior, whereby an animal marks clear boundaries from its fellows. Privacy relates to that specific need of an individual to distance itself – or information relating to itself – from its society. Yet, regardless of this idea of privacy as a type of basic instinct, legal protection of the right to privacy only started to emerge at the end of the 18th century. Following the American and French revolutions, the idea of protected personal communication and the inviolability of the personal home became accepted. Only a century later was the actual term privacy coined as “the right to be let alone” by Warren and Brandeis [Warren 1890]. In the course of the 20th century, this right would be included in major human rights instruments in the framework of the United Nations and the Council of Europe.

Within Europe, the right to privacy can mainly be found in article 8 of the European Convention on Human Rights (ECHR). This article concerns the private and family life, home and correspondence of the citizen. Although this article is still one of the foundations of European privacy protection, its value in the field of data privacy has since been surpassed by the more enforceable instruments of the EU. Apart from Directive 95/46/EC, the EU has also provided for privacy protection in the field of telecommunication (Directive 2002/58/EC) and in the field of data retention (Directive 2006/24/EC). Furthermore, the EU has included the right to privacy in the Charter of Fundamental Rights of the European Union, anchoring the value of human rights protection in the Treaty on the European Union.

4.1.1 Directive 95/46/EC

The idea of data privacy gained foothold in Europe after the Organization for Economic Co-operation and Development (OECD) published guidelines on the protection of privacy and transborder data flows. These guidelines served as the inspiration for the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Given the lack of support for this convention, yet realizing the need for adequate data protection across Member States, the EU started work on a directive on the matter in the early 1990’s using the basic principles laid out in the aforementioned Council of Europe Convention.

Finally, on the 24 October 1995, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data was accepted. Implementation into national legislation by the Member States was expected by late 1998.

In this sector, the basic principles of Directive 95/46/EC will be explicated. Note that Directive 95/46/EC aims to protect only the fundamental rights and freedoms of natural persons. As the goal of the uTRUSTit project is to enhance trust in the IoT, this overview of the general principles of EU data protection legislation will aid in understanding how personal data can be processed lawfully. A clear understanding of the consequences regarding the processing of his personal data, can contribute to the enhancement of the citizen's trust in the IoT.

4.1.1.1 Definitions and scope

Article 2 of Directive 95/46/EC states a number of definitions, delineating the precise scope of the directive. More specifically, the directive provides definitions for the notions of personal data,
processing of personal data, personal data filing system, controller, processor, third party, recipient and the data subject’s consent.

The core of Directive 95/46/EC is the notion of personal data. This is defined as:

...any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Note that the directive does not distinguish between written, oral, visual or any other type of information. Furthermore, the information needs to identify a natural person or make this person identifiable. A person can be considered as being identified when his identity can directly be established. This is the case in using national single identification number of general application. As such identification number is uniquely assigned to one single citizen, this citizen can directly be identified using this identification number. Other examples include name, address, date of birth, etc. While these last examples are not necessarily unique for one single citizen, they carry a high probability of direct identification of the person involved. If the person involved cannot be identified directly, he may still be identified indirectly by combining different elements or by deducing other identifiers from available information. In such case, the person is identifiable. This definition leads to a very broad spectrum of information that could potentially serve as personal data. Under sector 4.2.2, a number of cases will be presented in which the limits of this definition are explored.

Second, the personal data needs to be the subject of processing of personal data. Processing is defined as:

...any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Also in this case, Directive 95/46/EC gives a very broad definition of this notion. Virtually every act in which personal data is used can be considered as a form of processing. Note that both automatic and non-automatic processing can fall under the scope of this directive.

A personal data filing system is:

...any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

Note that unstructured data is excluded from this definition. Furthermore, the data needs to be accessible according to certain criteria. According to recital 27 the structure needs to relate to such criteria.

The entity responsible for the processing is the controller. This is:

...the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or

---

40 A national single identification number of general application is an identification number attributed by States to their citizens in order to uniquely identify them. Such identification numbers are used in, for instance, Belgium, Sweden and Spain.

41 Recital 27 Directive 95/46/EC; [Dumortier 2010].
regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

The main criterion in this definition is the authority to determine the purposes and means of the processing.\footnote{In the case of split tasks, the person determining the purposes of the processing is the controller. [De Bot 2001]} Note that, while the directive is only aimed at protecting the fundamental rights and freedoms of natural persons, the controller can be both a natural person and a (public) legal person. Joint responsibility in case of multiple entities collaborating is also an option.

As the person responsible for the execution of the processing and the person conducting the actual processing are not necessarily the same, the directive foresees the possibility of a processor. This is:

...a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Note that the processor has to be a person external to the controller. If, for instance, the controller is a company and it designates one of its employees to perform the processing, this employee is an internal designate and no external processor. The processor therefore performs the processing on behalf – but not under direct authority – of the controller.

It should be noted that the distinction between processor and controller is not always very clear. Therefore, specific research into the precise scope of both definitions will be performed under section 4.2.1.

A third party is:

...any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

This definition is by default negatively formulated: any entity that is no controller, processor or data subject is by definition a third party.

A recipient is a:

...natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

This is any person to whom the personal data is disclosed. Such disclosure can be interpreted very broad, as making the personal data available – for instance through a website – can also constitute a potential disclosure. Note that in principle every entity can be a recipient, which includes controller, processor and third party. Employees of the legal person/controller receiving access to the personal data are internal recipients.

Finally, the article provides a definition for the data subject’s consent. This is:

...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

This consent can be given both explicitly as implicitly [De Bot 2001]. Although the directive does not specify that consent needs to be granted in writing, a written and signed consent form is obviously preferred from an evidential point of view. The fact that the consent needs to be given freely indicates that it cannot be given as a result of external pressure, for instance emanating from the controller. Furthermore, consent can only be given for a specific processing. Therefore, no consent can be given for
all future processing of personal data. The consent also needs to be informed, meaning that the data subject needs to be well aware of the means and purposes of the processing for which he grants his consent. The data subject can at any time revoke his consent ex nunc, therefore disabling the use of his data for future processing. The revocation of consent for a past processing is not possible. Under section 4.2.6, a more detailed explanation will be given on how to obtain the data subject’s consent.

Regarding the precise scope of the directive, article 3 states that the directive is not applicable to processing:
- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
- by a natural person in the course of a purely personal or household activity.

The second exception – often referred to as the household exception – is not clearly defined in the directive and will therefore be further explicated under sector 4.2.3.

Article 9 provides an exception for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. More exemptions for public authorities are provided under article 13.

4.1.1.2 Basic principles of processing

Three principles form the basis of every fair and lawful processing: Legality/transparency, finality and proportionality.\(^{44}\)

**Legality/transparency**

The principle of legality means that the data subject needs to reasonably know which of his personal data is processed, why and by whom. If a public legal entity processes personal data, it needs to provide a clear legal norm as basis for the processing. For private persons – natural and legal – this means that sufficient transparency on the purposes and means of the processing needs to be provided. Specifically, the directive states that data can only be processed if:

(a) the data subject has unambiguously given his consent; or
(b) 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; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom

\(^{43}\) Obligations and rights may be restricted for safeguarding: “(a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others.”

\(^{44}\) Articles 5, 6 and 7 Directive 95/46/EC.
the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1) [of the Directive].

**Finality**

No fair and lawful processing can be performed without clearly delineating specified, explicit and legitimate purposes. The purposes need to be disclosed to the data subject and need to be adequately formulated in order for him to give his informed consent. Data can also not be further processed in a way incompatible with those purposes.\(^{45}\)

**Proportionality**

Data need to be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed. They may not be stored longer than is necessary for the purposes for which the data were collected or for which they are further processed.\(^{46}\) Data needs to be accurate and, where necessary, kept up to date. Inaccurate or incomplete data needs to be erased or rectified. Under sector 4.2.4 more research will be performed on how to comply with the principle of proportionality in the IoT.

### 4.1.1.3 Data subject’s rights

**Right to information**

The controller needs to provide certain information to the data subject.\(^{47}\) A distinction is made between the situation where the controller receives the data from the data subject personally or from another source.

If the information has been obtained from the data subject, in so far as such further information is necessary:

- (a) the identity of the controller and of his representative, if any;
- (b) the purposes of the processing for which the data are intended;
- (c) any further information such as:
  - the recipients or categories of recipients of the data,
  - whether replies to the questions are obligatory or voluntary,
  - as well as the possible consequences of failure to reply,
  - the existence of the right of access to and the right to rectify the data concerning him.

If the information has been obtained from another source, in so far as such further information is necessary, and with the exception of processing for statistical purposes or for the purposes of historical or scientific research, or if the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law:

- (a) the identity of the controller and of his representative, if any;
- (b) the purposes of the processing;
- (c) any further information such as
  - the categories of data concerned,
  - the recipients or categories of recipients,
  - the existence of the right of access to and the right to rectify the data concerning him.

---

\(^{45}\) Note that further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible.

\(^{46}\) This corresponds to the idea of data minimization.

\(^{47}\) Articles 10 and 11 Directive 95/46/EC.
Right of access
The data subject has the right to exercise a certain degree of control over his personal data. First of all, he may ask for confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed. He may also ask communication to him in an intelligible form of the data undergoing processing and of any available information as to their source and knowledge of the logic involved in any automatic processing of data concerning him at least in the case of automated decisions. This information needs to be supplied to him without constraint at reasonable intervals and without excessive delay or expense.

Right to correction
The data subject may also ask – where appropriate – the rectification, erasure or blocking of data of which the processing does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data. This includes notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with the data subject’s request for correction, unless this proves impossible or involves a disproportionate effort.

Right to object
On compelling legitimate grounds relating to his particular situation, the data subject has the right to object to certain types of processing. The directive lists “processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority and processing necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed” as cases in which the right to objection needs to be granted. Furthermore, he can object to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

4.1.1.4 Special categories of data
As mentioned under sector 4.1.1.2, Basic principles of processing, the processing of personal data is in principle allowed if the processing complies with the principles of fair and lawful processing. Article 8 of the directive, however, defines special categories of data of which the processing is prohibited. Specifically, this concerns “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.” Summarized, article 8 prohibits the processing of sensitive data, medical data and judicial data.

There are, however, a number of exceptions that do allow for the processing of these special categories of data:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject’s giving his consent; or
(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

---

48 Article 12 Directive 95/46/EC.
49 Article 12 Directive 95/46/EC.
50 Article 14 Directive 95/46/EC.
processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

d processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

e the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.\textsuperscript{51}

Article 8 (3) provides an exception for processing required for preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Article 8 (5) provides an exception for processing of data relating to offences, criminal convictions or security measures. These may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

4.1.1.5 Confidentiality and security

The directive also provides for the confidentiality and security of the processed personal data.\textsuperscript{52} These are technical and organizational measures that need to lead to more secure processing and storage of personal data. Even in an otherwise strictly fair and lawful processing, data leakage could cause an infraction to the principle of data minimization.

Article 16 concerns the persons acting under the authority of the controller and the processor. They may not process the personal data except on instructions from the controller, unless he is required to do so by law. This ensures confidentiality.

Article 17 deals with the security of the processing. Member States need to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. For implementing measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, the state of the art and the cost of their implementation will be taken into account.

The controller needs to ensure that the processor can provide sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out. The controller must also ensure compliance with those measures. The duties of the processor need to be governed by a contract or legal act binding the processor to the controller and stipulating that the processor shall act only on instructions from the controller, and that the controller’s obligations shall

\textsuperscript{51} Article 8 (2) Directive 95/46/EC.

\textsuperscript{52} Articles 16 and 17 Directive 95/46/EC.
also be incumbent on the processor. For evidential matters, such contract or legal act needs to be concluded in writing.

### 4.1.1.6 Notification

In order to assess whether a certain processing complies with the principles set forth by the directive, a duty of notification has been included in article 18 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. Member States can, however, simplify the notification or provide exemptions for a number of reasons listed under article 18 (2). Most notably, this includes the appointment of a personal data protection official.

Regarding the content of the notification, article 19 states that this includes:

- (a) the name and address of the controller and of his representative, if any;
- (b) the purpose or purposes of the processing;
- (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
- (d) the recipients or categories of recipient to whom the data might be disclosed;
- (e) proposed transfers of data to third countries;
- (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

The Member States must also determine which type of processing can bear specific risks for the personal rights and freedoms and must ensure that these types of processing are examined prior to their start. The national supervisory authority will perform such examination.

Finally, the Member States need to adopt measures to guarantee the publicity of the processing operations. National supervisory authorities will keep a public register of duly notified processing operations. Also processing operations exempt from the duty of notification need to supply the information included in article 19.

### 4.1.1.7 Data transfers

In principle, processed personal data can only be transferred to a third State if such State can guarantee an adequate level of data protection.\(^{53}\) This adequacy is assessed in the light of all the circumstances surrounding a data transfer operation, in particular “the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.” The Commission performs such assessment. Article 26 provides a number of exceptions to this rule of data transfer. These exceptions are formulated in the same line as the exceptions to the principal prohibition of processing special categories of data.

### 4.1.1.8 Supervisory authority

Within each Member State, one or more independent public legal entities will monitor the implementation and the national application of the principles set forth in the directive. Next to an advisory function, these supervisory authorities are granted powers of investigation, the power to

\(^{53}\) Article 25 Directive 95/46/EC.
intervene and the power to engage in legal proceedings.\textsuperscript{54} Given the nature of their tasks, the members of the supervisory authorities are sworn to secrecy.

Representatives of the national supervisory authorities are united in the so-called Article 29 Working Party. This Working Party acts as a pan-European advisor and strives for a more harmonized and coherent application of the principles of the directive throughout the EU Member States. Its precise tasks are listed under article 30.

4.1.1.9 Requirements

From the previous analysis, one can deduce the following requirements (nr. 1A):

- It is required that IoT actors identified as data controllers are aware of the precise definitions of national data protection legislation applicable to the processing under their control.
- The data subject’s free, informed and unambiguous consent is required for legitimate processing of personal data.
- Legality or transparency is required for fair and lawful processing of personal data.
- The purposes of the processing of personal data are required to be clearly indicated in advance.
- The processing of personal data is required to only include relevant and non-excessive data, in relation to the specified purposes.
- The data controller is required to ensure sufficient information of the data subject.
- The data controller is furthermore required to ensure that the data subject can fully enjoy his right of access, his right to correction and his right to object.
- Special notice is required to the special categories of personal data.
- The data controller is required to ensure confidentiality and security of the processing of personal data under his control.
- Due notification to the competent national Data Protection Authority (or Authorities), in compliance with national legislation, is required.
- Data transfers to third States are required to comply with applicable legislation.

4.1.2 National privacy legislation

Being a directive, the principles of Directive 95/46/EC discussed here first need to be transposed into the national legal system of the EU Member States. Unlike a regulation, directives are not self-executing and are thus not immediately enforceable as law in the Member States. As directives only provide a certain goal that needs to be met and usually leave it to the Member States to decide upon the means they wish to adopt to achieve said goals, it is of no surprise that the national implementation of directives can lead to very divergent results.

\textsuperscript{54} Article 28 Directive 95/46/EC.
A directive is therefore by nature not the most ideal legal instrument if one aims to create a pan-European harmonized framework on a certain topic. This has become very apparent in the case of the EU legal framework on data protection, as found by Directive 95/46/EC. The initial purpose of the Directive was not so much to block the processing of personal data, but to facilitate data transfers between the EU Member States. Such data transfers were at that time severely restricted due to the highly divergent national privacy policies of the Member States. The directive was therefore aimed at supporting the further expansion of the common market and introducing a harmonized level of data protection throughout the whole EU. Harmonizing elements can, for instance, be found in article 1 (2) that states that Member States “shall neither restrict nor prohibit the free flow of personal data between Member States” for reasons connected with the protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data [De Bot 2001].

Although one could argue that the directive has attempted to provide harmonization on this topic, the clear divergence in Member States’ policies shows that the effect of the directive has remained limited to the establishment of a minimal degree of protection. Certain parts of the directive – such as article 5, article 8 (7) and recital 9 – allow for a degree of national differentiation that goes beyond what could be expected from a true attempt at harmonization. If harmonization was the true goal of the principles of Directive 95/46/EC, this goal may have been missed by utilizing a directive and by allowing for such a high degree of national differentiation.

The divergence of national policies on data protection could also hinder the goal of facilitating data transfers between the EU Member States. As, for instance, the national supervisory authority in one Member State holds up higher demands for notifications than the national supervisory authority in another Member State, the transfer of data between these Member States may be hindered. The Article 29 Working Party has taken note of these divergences and has issued opinions and recommendations for a more coherent interpretation across the EU. Examples of this include Opinion 1/2010 on the concepts of "controller" and "processor" and Opinion 4/2007 on the concept of personal data.

Specifically for the IoT, this being a worldwide self-configuring network of objects, this could very well mean that it may become difficult to establish the specific role of certain parties and their corresponding duties, especially in the case of cross border data transfers. A certain processing may be subject to notification in one Member State, while being exempt from notification in another and a certain party involved in the processing may be regarded as a controller in one Member State and as a processor in another Member State. This ultimately requires a thorough reading of the privacy regulations of each Member State involved in a certain processing, a task rendered even more difficult when discussions of territoriality arise.

As different EU Member States may have divergent national provisions regarding data protection, IoT actors are required (nr. 1B) to establish the precise geographical scope of their potential processing of personal data in order to establish which national data protection legislation(s) will be applicable to their processing of personal data.

4.1.3 Review of Directive 95/46/EC

Even though the data protection directive was adopted in 1995, the grand majority of the principles therein are directly taken from the Council of Europe’s 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. With thirty years of use and remaining virtually unchanged, one could therefore wonder whether the main principles that, to this day, form the basis of the legal framework of EU data protection should be replaced by newer principles.
that better reflect the drastically changing nature of data communication and data protection. Current issues – IoT, the Internet, social media, etc. – were not around at the time that these principles were conceived and their authors could not possibly have foreseen the drastic changes to the information society in the past decade.

At this moment, outdated principles are applied to situations they were never intended to be applied to; this leads one to wonder when the limits of the flexibility of these principles will finally be reached. The need for a thorough review of Directive 95/46/EC can therefore no longer be ignored. Even the opinions of the Article 29 Working Party may have reached their limits as their legal value may be contested, as they may push interpretations of existing principles too far and as they may not always provide more coherence in such interpretations [Van Eecke 2009]. A new approach therefore seems imperative to render the current legal framework on EU data protection more future proof.

A number of issues to be discussed during the review of Directive 95/46/EC include the basic definitions found in article 2. Growing discussion on the scope and interpretation of notions such as controller, processor, personal data and sensitive data have demonstrated the need for reform. With regards to the right to information, criticism has risen on standardized privacy policies often found on websites. Although such generic privacy policies may comply with the requirements set forth by the directive, they do not necessarily provide the data subject with the information he really needs, therefore not meeting the purpose of the right to information. These and other issues under discussion will be further examined under sector 4.2, Specific privacy concerns relating to the IoT.

Apart from reviewing existing principles, a number of new principles may be added to the next iteration of the EU data protection framework. For one, it is clear that in the information society it has become very difficult to permanently erase data. Many websites provide links to content found on other websites, while others even copy certain content to their own servers. Because of the large scale on which this linking and copying takes place, it is virtually impossible to compile an exhaustive list of which web servers offer a certain piece of information. If said piece of information concerns the personal data of a data subject, he may face an insurmountable challenge in having this information deleted from the internet permanently. To counter what can be referred to as the perpetual memory of the internet, one could think of a right to be forgotten\(^{55}\) as complement to the right to privacy, traditionally referred to as the “right to be let alone”\(^ {56}\). Such would enable the data subject to personally determine that their data is no longer processed and deleted when they are no longer needed for legitimate purposes.

Another means for enhancing the data subject’s control over his own personal data is the notion of data portability\(^ {57}\). Such would allow the data subject to fully withdraw his personal data from an application or service so that the withdrawn data can be transferred into another application or service, as far as technically feasible, without hindrance from the data controllers.

---

\(^{55}\) The Commission has addressed this principle as such: Communication of 4 November 2010 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, “A comprehensive approach on personal data protection in the European Union”, COM(2010) 609, 7-8.

\(^{56}\) A proposal for a law providing a “right to be forgotten” has already been introduced in the French Senate: “Au total, il convient de noter que plusieurs mesures de la présente proposition de loi permettent de donner une plus grande éffectivité au droit à l’oubli numérique”; Sénat France, Proposition de Loi visant à mieux garantir le droit à la vie privée à l’heure du numérique, www.senat.fr, 2009-2010, nr. 93.

Another idea coined by the Commission is to establish a right to silence of the chips. This would give the data subject the right to disconnect from their networked environment at any time. Within the IoT, such would mean that the data subject would be able to opt-out of the constant flow of interconnected devices.

The possibility of review was discussed in July 2010 during a meeting of the Article 29 Working Party. It was discussed that national supervisory authorities should receive a more important role in supervising the application of the EU data protection framework. Regarding the review of the principles of the directive, the French Commission Nationale de l’Informatique et des Libertés (CNIL) warned that such review could entail a lengthy procedure [Out-Law 2010].

4.2 Specific privacy concerns relating to the IoT

4.2.1 Controller versus processor

As discussed earlier, the main actors performing the processing of personal data are the controller and the processor. Although the classification as one of these actors is highly important to determine the precise scope of the responsibilities and liabilities of a certain party to the processing, the distinction between these two notions is not always very clear and well defined. For data protection – in general as well as relating to the IoT – it will therefore be essential to establish a clear distinction between these two actors and their respective roles.

As defined under the general introduction to the key principles of Directive 95/46/EC, the controller is the natural or legal person who holds the authority to determine the purposes and the means of the processing of personal data. In case of a legal person, the employees of this legal person concerned with handling the data that is to be processed – or even performing the actual processing – are considered as internal designates. If the controller, however, assigns the task of processing the personal data to an external entity, to execute the processing on the controller’s behalf, then said external entity is considered to be a processor.

From these definitions, one can understand that the main characteristic of the controller is to ‘determine the means and purposes’ of the processing, while the processor executes ‘on behalf of the controller’. The mere application of these definitions can already lead to discussion, as the attribution of the authority to determine means and purposes or of the ability to act on behalf of another party may to a certain extent lie in the eye of the beholder. Therefore, the attribution of control or of delegation to one or another party may be subject to the person or entity performing such attribution.

Recent technological and societal developments – such as the IoT – have also influenced these two concepts and their applicability. At the time of the drafting of Directive 95/46/EC, the EU envisioned very specific models of data processing that allowed for a more clear-cut application of the concepts of controller and processor [Van Alsenoy 2009]. The rise of the Internet, with new communication models and means for service providing, has lead to the creation of new data processing models that allow for a less static attribution of the concepts of control and delegation, therefore making it difficult to establish the roles of controller and processor. This may even lead to the appointment of co-controllers, leading to joint liability [Van Alsenoy 2009]. Joint control may in turn

---

60 Note for instance article 6 (2) of Directive 95/46/EC indicating that it is the responsibility – and thus the liability – of the controller to ensure that the general principles of fair and lawful data processing are observed.
61 Although the legal term ‘delegation’ can be understood broader than is intended here, the term is used in order to follow the precise wordings of the Article 29 Working Party.
lead to even greater confusion regarding the precise division of liabilities between these joint controllers and even applicable law. As service providers are ever more convergent, one entity may in one aspect of its tasks be a controller, while being a processor in other aspects of his tasks.

The Article 29 Working Party has taken notice of the changing times and the consequences thereof for the application of the concepts of controller and processor. In an opinion, the Working Party aims to give an overview of the current situation, as well as an attempt to allocate responsibility to ensure compliance [Working Party 169]. The Working Party sees it as “the crucial challenge […] to provide sufficient clarity to allow and ensure effective application and compliance in practice” [Working Party 169]. On the other hand, continued effectiveness needs to be ensured and undue consequences under changing circumstances need to be avoided by balancing the need for present acceptable consequences with future needs for adjustment.

Regarding the issue of control, the Working Party determines that this is a factual issue that can be assessed pragmatically with a view to ensure predictability [Working Party 169]. The Working Party distinguishes three situations from which control can stem [Working Party 169]: from explicit legal competence, from implicit competence and from factual influence.

Regarding the means and purposes of the processing of personal data, the Article 29 Working Party states that, in short, this refers to the why and how of the processing [Working Party 169]. In assessing who determines purposes and means, it will be important to maintain a pragmatic approach, looking into the level of influence a certain party exercises. After all, a processor will, up to a certain extent, determine the means for the processing, as he performs the actual processing. The mere fact that he has some level of determination on the means for the processing does, however, not automatically qualify him as a controller. The level of discretion is therefore the key component in assessing the ability of determination, and therefore in attributing the role of controller.

On the issue of joint control, the Article 29 Working Party wants to ensure that the ever more complicating data processing models of today do not hinder an easy and efficient allocation of roles and responsibilities. Full compliance to data protection principles should be ensured at all times, even in the case of a controller whose limited role prohibits from fulfilling his full duties as a controller.

The Article 29 Working Party therefore aims to allocate responsibility where the actual control is exercised, making the concept of controller more of a functional concept, than a mere static one. Although this opinion is a laudable attempt at providing more clarity on the applicability of the concepts of controller and processor to a highly different environment than which they were originally intended for, the opinion still leaves a number of underlying issues untouched. For one, regarding the issue of co-control, the Working party stresses the need for a clear allocation of roles. In this respect it should be noted that (co-)controller contracts could provide a clear division of tasks and responsibilities and could therefore provide for an effective role allocation. Such contracts are, however, still not legally recognized. Introducing the requirement for controllers to draft such contracts in order to ensure

62 Article 4 (1) (a) of Directive 95/46/EC states that the law of the territory in which the controller has its main establishment is applicable to the processing.

63 I.e. when the controller or the specific criteria for his nomination are designated by national or Community law.

64 I.e. when the capacity to control has not been explicitly laid down by law, but can be derived from common legal provisions or established legal practice pertaining to different areas.

65 I.e. by analysis of contractual relations between parties involved.

66 Note that the Article 29 Working Party has a broad view on the concept of means. This not only includes deciding upon the actual technical measures of processing the data, but also certain organizational measures such as deciding upon which data is to be processed, which third parties can gain access to the data, which data is to be deleted, etc. As the determination of the means is to a certain extent the task of the processor, this broad definition sensitively enlarges the scope of the processor’s work package. Determination of purpose, however, is reserved to the controller.
compliance in the EU legal framework on data protection could therefore already lead to a much clearer role division, thereby providing a solution to the main issues regarding role and responsibility attribution.

Regardless of the Article 29 Working Party opinion, the application of the concepts of controller and processor to new data processing models still leaves room for legal uncertainty. One can therefore look forward to the upcoming review of Directive 95/46/EC to see how these concepts and their application will evolve.

Prior determination of the specific tasks and responsibilities of each party is required (nr. 2) to fully assess the roles of each party. This will enable to determine which party is controller and which party is processor, as well as to assess the scope of their roles.

4.2.2 Limits of the concept of personal data

The concepts of controller and processor are not the only fundamental concepts of Directive 95/46/EC, whose applicability to changed data processing models has come under discussion. Even the foundation of the directive, the very concept of personal data itself has met its limits and shortcomings. As the definition of this concept in the directive has a very broad scope, the precise interpretation of the concept of personal data appears to differ amongst Member States.

Aiming to provide a more coherent interpretation across the EU, the Article 29 Working Party has adopted an opinion on the concept of personal data [Working Party 136]. As this concept forms the very basis of the EU legal framework on data protection, a coherent and homogenous interpretation by all Member States is of utmost importance. Although it could be argued that the definition of the concept of personal data has deliberately been formulated in a broad manner in order to embed flexibility in the application of the concept to various circumstances, it should also be noted that the scope of the concept should not be overstretched [Working Party 136]. Here, the Working Party clearly states that it would be undesirable to stretch the existing concept for application to situations not intended to be covered by the legislator, which is an appropriate reaction as the idea of overstretching the applicability of existing concepts is one of the core issues that augmented the demand for review of the directive. However, the Working Party also warns for a too narrow application of the directive. When the application of the concept of personal data may at first sight seem to be overstretched, one should first look at the scope of the directive, in particular of article 3. Next, one should look at exemptions or simplifications in the directive or in national implementations thereof. The Working Party addresses the national Data Protection Supervisory Authorities (DPA) to monitor the application and interpreting of the directive and to endorse a broad definition of concepts for application of the directive to societal and technological evolutions.

The Working Party continues its opinions by analyzing the constitutive elements of the concept of personal data. First, the element of information is analyzed [Working Party 136]. Here, it is indicated that nature and content of the information are of no importance as all information is included under the scope of the directive, regardless of nature or content. From this, one can deduce\(^7\) that the directive is not limited to the protection of information regarding the strict sphere of home and family, but also touches subjects beyond this sphere such as labour law\(^68\), court records\(^69\) and direct marketing\(^70\). Also the format or medium used in presenting the data is of no importance.

---

\(^{67}\) As noted by the Working Party, the broad scope of the Directive is endorsed by the European Court of Justice: ECJ C-101/2001 Bodil Lindqvist, 2003, §24.

\(^{68}\) Article 8 (2) (b) Directive 95/46/EC.

\(^{69}\) Article 8 (5) Directive 95/46/EC.

\(^{70}\) Article 14 (b) Directive 95/46/EC.
Second, the information needs to relate to an individual [Working Party 136]. This can be a direct relation, where information about a person is given.\(^{71}\) Also possible is an indirect relation, whereby information is provided on an object that relates to the individual.\(^{72}\) In short, the Working Party considers data to relate to an individual if “it refers to the identity, characteristics or behavior of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated” [Working Party 105]. According to the Working party, information can relate to an individual if there is a content element\(^{73}\), a purpose element\(^{74}\) or a result element\(^{75}\).

Third, regarding the element of identified or identifiable individuals [Working Party 136], the Working Party notes that this means that the individual should be distinguished from the other members of the group, or that it should be possible to do so. Directly or indirectly refers to the degree of precision by which a certain identifier can indicate a single individual.\(^{76}\) For indirect identification, one will have to combine several elements of information together before a unique identification can be made. For defining the notion of identifiable, the Working Party refer to recital 26 of the Directive where identifiable is defined as all the means likely reasonably to be used to identify an individual. By determining what is likely reasonably to be used one, has to keep in mind several factors – such as the cost of identification – and reality has to be applied. Hypothetical possibilities for identification are not likely reasonably to be used and are therefore not to be considered as personal data. The Working Party also makes note of the use of pseudonymization of data to disguise identities and of anonymization to make identification impossible.

The last element analyzed by the Working Party is that of the natural person [Working Party 136]. As explained earlier, the directive protects the rights and freedoms of natural persons. In this opinion, the Working Party elaborates on the fact that this data is generally regarded to relate to living natural persons. Therefore, two particular cases could come to mind: the dead and the unborn.

In general, the dead are no longer regarded as being part of the concept of natural persons and are therefore excluded from data protection rights. Exceptions to this rule may, however, apply. For one, if the controller is not certain of a person’s death, he will process data relating to that person as if he were living. Data relating to the dead may also provide information on the living, for instance hereditary medical conditions, and is therefore to be processed according to the applicable provisions in the directive. Regarding medical data it should also noted that confidentiality duties continue even in death.

Although most, if not all, States have reached consensus on the end of life, there are still differences in national legal systems on the beginning of life, complicating the case of personal data relating to the unborn. One will have to look into the national provisions on rights relating to the unborn in order to establish whether a particular State grants data protection rights to this case.

Note that, if certain data appears not to be personal data under the scope of the directive, one might have to look at national implementation thereof as these may have enlarged the scope of the directive. The pending review of the directive may also have implications to the precise scope of the concept of personal data.

---

\(^{71}\) The Working Party lists medical and personnel records as examples of files in which data relating to an individual can be found.

\(^{72}\) The value of a house can, for instance, give information on the assets and wealth of its owner.

\(^{73}\) If information on an individual is given, regardless of any specific purpose.

\(^{74}\) When data is provided for a specific use.

\(^{75}\) When the data provided can have an impact on an individual’s rights and interests.

\(^{76}\) This is obviously a contextual matter. The notion “man in business suit” may not provide much help for identifying a particular individual on Wall Street, while it may be useful to single out someone in a more rural crowd.
With these analyses of the core notions of the concept of personal data, the Article 29 Working Party hopes to have cleared the precise scope of this foundation of the EU legal framework on data protection. With regards to the IoT it will be important to clearly define the precise types of data that may be subject to processing in order to analyze whether these types can be considered as personal data under the scope of the directive or not.

IoT actors are required (nr. 3A) to ensure that they are aware of the scope of the notion of personal data under the national legislation applicable to the processing of personal data under their control. Follow-up on the review of Directive 95/46/EC is required to ensure ongoing compliance with changing data protection principles.

4.2.3 Application of the household exception

Although the rules established in Directive 95/46/EC may at times seem rather strict, the directive also provides for many exceptions. One of the main exceptions can be found under article 3 (2) of the directive. This exception states that the directive does not apply to the processing of personal data “by a natural person in the context of a purely personal or household activity.” This exception is commonly referred to as the ‘household exception’ and allows for natural persons to perform what can be regarded as a processing of personal data, as long as such processing serves strictly personal intent.

The classic example of such processing for personal use is the electronic contacts file or application\(^77\). In such file or application – found for instance on smartphones or in e-mail software – the individual can store phone numbers, e-mail addresses and other identifiers of his friends, family and colleagues. A strict application of the principles of the directive would consider this as a processing of personal data under the scope of the directive, therefore requiring the individual keeping an electronic contacts file to comply with these provisions. As such would cause unreasonable and undesirable results, the directive has exempted this type of personal use. It should be noted that the exemption only applies to the strictly personal use. If the individual keeping a personal contacts file, for instance, decides to use this data with a commercial intent, the household exemption will not apply to such use.

As discussed before under sector 4.2.1, controller versus processor, the directive was at the time of its drafting focused on specific models of data processing, in which the precise scope of the processing and the roles of its actors were clearly delineated. Changing models of data processing due to more integrated and ubiquitous information systems – such as the IoT – blur these previously clear lines and instigate discussions on the precise scope of the roles of the parties involved in the data processing. With the rise of Web 2.0, social networks and user-generated content, more and more content on the Internet is generated by users acting in a private, non-professional and non-commercial capacity. If personal data is processed in such user-generated content, can the household exception still apply? In order to assess the use of the household exception in this changed data processing landscape, one will have to look deeper into the notion of personal or household use.

Apart from the expanding interconnection between objects found in the IoT, also humanity seems to have found a new method for connecting with each other. Social networks – mainly Facebook\(^78\) and Twitter\(^79\) – are frequented by an ever-growing number of users and have become a staple in daily communication.

An important characteristic of these social networks is that the user decides which personal information he wishes to share with the network. In such regard, the user could be considered as a data controller [Van Alsenoy 2009]. However, the fact that these social networks can be accessed anywhere where an active cellular or Wi-Fi reception is available – be it at home, at work or on the road – makes it

\(^{77}\) The directive addresses this as “records of addresses” in recital 12.

\(^{78}\) www.facebook.com.

\(^{79}\) www.twitter.com.
difficult to assess the precise capacity in which users post their content. Work-related information can be posted at home and not all information shared by users during the office hours qualifies as work-related information. As explained earlier, the household exception will only apply to the processing of personal data in a personal or household context, stressing the importance of establishing the right capacity in which the user is acting. The rise of social networks has, however, blurred the lines between the different capacities in which a user may act. The question raised here therefore becomes twofold: How do we distinguish the different capacities, in which a user may act and can the household exception still apply to personal data processed in online user-generated content if such content was produced in a personal capacity?

The Article 29 Working Party has addressed the issue in an opinion [Working Party 163]. First, it is noticed that the household exception can indeed apply to user-generated content in which personal data is processed, as long as such processing was conducted in the personal or household sphere of the user [Working Party 163]. Regarding the capacity of the user, an important line of thought followed by the Working Party is that this can be deduced from the publicity of his social network profile [Working Party 163]. If the profile is only visible to a select group of friends, the user may be considered as acting in a personal capacity. A user who keeps his profile visible to all users within that social network, or even indexable by search engines, can be regarded as going beyond the personal or household sphere. Also, personal websites or non-social network posts that are fully visible to the general Internet public can be regarded as not being uploaded in the personal capacity of the user. Therefore, the household exception cannot apply and the user becomes a data controller and needs to comply with the provisions of the directive.

This reasoning is mainly deduced from case-law. In the Lindqvist-case, the European Court of Justice ruled that the household exception must be interpreted as “relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.”

This was later further elaborated in the Satamedia-case, where the Court ruled that the household exception “must be interpreted as relating only to activities which are carried out in the course of private or family life of individuals (see Lindqvist, paragraph 47). That clearly does not apply to the activities of Markkinapörssi and Satamedia, the purpose of which is to make the data collected accessible to an unrestricted number of people.”

Although the reasoning behind this decision can certainly be understood, it fails to address a number of underlying issues. First, it is not assessed what constitutes the threshold of public dissemination [Van Alsenoy 2009]. When does a profile become too public to be considered as part of the user’s private sphere? Second, one could question the all-or-nothing approach of the exception. According to the reasoning of the European Court of Justice and the Article 29 Working Party summarized here, the qualification of the user of a social network as data controller or his exemption from any duties in this regard depends mostly if not solely on the publicity of his profile and the size of his network of online friends. One could therefore argue in favor of a middle way, that leaves room for certain differentiation.

It should also be noted that the European Court of Justice referred to the notion of “private or family life” rather than the notion of “purely personal or household activity” found in the directive. The

---

80 This opinion has been further explored by: [Korff 2009]; [Van Alsenoy 2009].
82 ECJ C-73/07 Tietosuojaavaltuutettu v Satakunnan Markkinapörssi Oy & Satamedia Oy, 2008, §44.
83 See also: [Korff 2009].
84 Though the exemption clears the user from the data controller duties imposed by the directive, general civil and criminal law provisions still apply to the user’s content.
notion used by the Court can be found in the European Convention of Human Rights.\textsuperscript{85} One could argue that the notion of “private or family life” has a more broad scope of application than the rigid concept of “purely personal or household activity” [Van Alsenoy 2009]. From this, it could be deduced that the household exception should apply to bona fide users of social networks, unless their profile has been made fully public [Van Alsenoy 2009]. Also the mere distinction between a public visible-to-all profile and a private friends-only profile seems to have lost its \textit{raison d’être} in the current society. The concept of friend on social networks refers not so much to the idea of a small group of people known personally by the user, but rather indicates a person who has visited the user’s profile and found it necessary to befriend that user. As certain social network users have even made a sport of collecting the largest mass of friends, it is clear that even a private profile only visible to friends can be highly public.

In summary, the household exception can apply to users processing personal data as part of their content generated on, for instance, social networks, insofar as such processing was conducted within their personal sphere. Currently, the personal sphere of the online user is determined by the publicity of his profile and his number of online friends. This criterion can, however, not suffice in the current evolutions of the information society. One could therefore propose a more updated definition of the concept of personal sphere, with possible room for differentiation in the household exception in order to avoid the current all-or-nothing approach.

\textbf{IoT actors are required (nr. 3B) to ensure that they are aware of the scope of the notion of the household exception under the national legislation applicable to the processing of personal data under their control. Follow-up on the review of Directive 95/46/EC is required to ensure ongoing compliance with changing data protection principles.}

4.2.4 Proportionality and how to implement in the IoT

Although the principle of proportionality is not directly mentioned in Directive 95/46/EC and can only be vaguely deduced from article 6 of the directive, it is one of the cornerstones for fair and lawful processing of personal data. The principle of proportionality is even considered a cornerstone for EU community law and is included in the Treaty on the European Union.\textsuperscript{86} In summary, this principle entails a two-tiered assessment [Kuner 2008].\textsuperscript{87} First, one needs to establish whether the proposed means are adequate to achieve the envisioned purpose. Second, one needs to assess whether the proposed means will lead to negative consequences on interests protected by law and whether such negative consequences can be justified in the light of the envisioned purpose. The goal of such assessment is to ensure whether there is no other means available that would lead to the same result, but would lead to less negative consequences.

The principle of proportionality could therefore be regarded as a principle of minimization. In choosing the means for the processing of personal data, the principle of proportionality requires one to choose the ‘lesser of two evils’. As the data collected may also not be excessive “in relation to the purposes for which they are collected and/or further processed”\textsuperscript{88}, the principle of proportionality could also be regarded as referring to the concept of data minimization. Processing excessive amounts of data would therefore be considered as a violation of the principle of proportionality.

\textsuperscript{85} Article 8 Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome, 4 November 1950.
\textsuperscript{86} Article 5 (4) Consolidated version of the Treaty on European Union, OJ. C 83 of 30 March 2010, 18. For further reading on the importance of the principle of proportionality in EU community law and in realm of the Council of Europe: [Kuner 2008].
\textsuperscript{87} Other authors describe a trie-tiered process: suitability (Are the means suited to reach the purposes?), necessity (Are the means necessary to meet the purposes?) and non-excessiveness (Do the means not go further than what is strictly necessary to attain the purposes?). [Bygrave 2009]
\textsuperscript{88} Article 6 (1) (c) Directive 95/46/EC.
The principle of proportionality, as a general principle of basic EU community law and as one of the main principles of the EU legal framework on data protection, will therefore have to be complied with in all processing of personal data. As already established, the implementation of the IoT in daily reality will lead to increased data flows between all kinds of devices. Naturally, personal data will be processed here as well, as can be deduced from the scenarios developed within the framework of this project. Therefore, in order for the IoT to be compliant to current data protection legislation, one will have to ensure that the principle of proportionality is respected.

As can be deduced already from this summary overview of the core components of the principle of proportionality and their implications, this will require a certain degree of planning up front [Kuner 2008]. For instance, if the principle of proportionality dictates that the means used in the envisioned processing of personal data may not be excessive to the purposes of said processing, then one will obviously have to decide on the proportionality of the means at the moment those means are decided upon. Any post factum assessment of the proportionality of the means used will be too late, as the potential violation of the proportionality principle will have already occurred.

Therefore, if a certain processing of personal data is planned, one will have to decide on a number of issues at the very moment of determining the means that will be used to execute the envisioned processing. As established earlier under section 4.2.1, controller versus processor, the means will often – at least to a certain degree – be decided upon by the processor, rather than the controller. In this regard, one could think of reaching an agreement between controller and processor regarding the means to be used for the processing. Such agreement will be of high importance, as a controller will want to avoid allowing his processor to decide upon the means he will use to execute the processing and subsequently deciding upon means that are excessive to the purposes set forth by the controller. It is, after all, the responsibility of the controller to ensure that all data processing is carried out fair and lawful, which includes complying with the principle of proportionality.

Second, the personal data that is to be processed in the envisioned data processing needs to be exhaustively determined on beforehand in order to ensure that no more data is collected than is absolutely necessary to meet the purposes set forth by the controller.

Regarding those purposes it should be noted that these might not be exceeded, as stated in article 6 (1) (c) of Directive 95/46/EC.

Data controllers planning to process personal data in the context of the IoT should therefore ensure to start planning the precise purposes of the processing early. This, together with an early determination of the data to be processed and the means to be used – together with the processor – will ensure compliance with the principle of proportionality.

The prior determination of the precise purposes and means of the processing is required (nr. 4) to ensure compliance with the principle of proportionality.

4.2.5 Sensitive data

As explained earlier in the analysis of the general principles of Directive 95/46/EC, under sector 4.1.1, the EU has decided to establish special categories of personal data of which the processing is in principle prohibited, unless such processing would fall under the scope of one of the exceptions listed
under article 8 of the directive. However, as with many other principles found in the directive, it is not always very clear what the precise scope of this sensitive data is.  

One could view sensitive data in a very strict or in a very broad sense. Medical data, for instance, in a strict sense would be the medical records found at a general practitioner’s office or in the hospital, or certain data regarding social security held by public and private health insurers. Here, one can also think of data concerning the data subject’s medical cabinet or the prescriptions written to him by his attending physician.

For medical data in a broad sense, one could even look at a picture of the data subject. As the directive does not make any distinction in the format in which personal data is presented, a picture may very well be considered as personal data if it can identify or can indirectly lead to the identification of the data subject. As a picture of a person wearing glasses, holding a walking cane or even displaying hair loss can provide information regarding the medical state of the person pictured, such picture can be considered as providing medical data.  

In an even broader approach to the concept of medical data, one may even look at the contents of one’s refrigerator or food cabinet, as the diet observed by a person may provide information on his medical state.

As it is the goal of the IoT to interconnect more devices and objects, one can understand that the data processing resulting from this interconnection may include data that could be considered as sensitive data in the broad sense or even in the strict sense. In the present project this was evidenced in the discussion on the scenarios that will be developed. Therefore, it will be important to clearly demarcate the scope of the concept of sensitive data and its components, in order to assess in which case the personal data processed in the IoT will be regarded as regular personal data that needs to comply with the general principles found in article 6 of the directive, or as a special category of personal data needing to comply with the stricter provisions of article 8 of the directive.

As a reminder, article 8 lists specific cases in which the processing of personal data could be allowed. Member States may expand this list.  

As general on sensitive data: [Van Alsenoy 2007].

90 In general on sensitive data: [Van Alsenoy 2007].

91 Note that pictures can also reveal ethnicity, another type of sensitive data.

92 Food may also provide information on the data subject’s religious beliefs, for instance kosher food.

93 During work on scenarios for the uTRUSTit project, it was decided that the case of a medical cabinet would be included. Therefore, during this implementation of the IoT, medical data on the individual will be processed. See for instance: [utrustit D2.9]

94 Article 8, (4) to (6) of Directive 95/46/EC.

95 Article 8 (2) (a) of Directive 95/46/EC.

96 For instance, both Google and Facebook have endured criticism on their approach to automatically enable certain changes to their services that could have an impact on the user’s privacy. Although the user was offered the option to opt-out, many users preferred the default situation to be to opt-in instead. See for instance on Facebook privacy settings. [Emigh 2010] In a rather ironic response, Facebook did deploy opt-in as a default setting, yet only for its new security settings. Privacy-infringements must be opted-out from while privacy-enhancements must be opted-in to. [Wisniewski 2011] Google CEO Eric Schmidt does seem to have understood the need for consent, as his 2011 Mobile World Conference keynote was littered with references hereto. [Miller 2011]

97 Article 8 (3) of Directive 95/46/EC.
national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.”

Then what is the precise scope of the concept of sensitive data? Unfortunately, the directive itself does not provide much information that could be used in determining this scope. Also the Article 29 Working Party does not shed more light on the scope of the concept of sensitive data. However, regarding medical data in electronic health records [Working Party 131], the Working Party does seem to support a rather broad definition of the concept, stating that all data found in medical files can be considered as medical—and thus sensitive—data [Working Party 131]. As the working document at hand is specifically aimed at electronic health records it cannot be used for deducing general conclusions regarding all sensitive data.

One noticeable peculiarity is how certain Member States have transposed this provision into national law. Most Member States have in this topic used more or less the same wordings as the directive in their national privacy legislation.98 Other Member States, notably Belgium, have spun off the concept of medical data from the concept of sensitive data.99 This enlarges the special categories of personal data to the strict concept of sensitive data—formulated as in article 8 (1) of Directive 95/46/EC minus the medical data—medical data and judicial data.100 Even though the Belgian Privacy Act does not provide a definition on the concept of medical data, doctrine has explained this as “all personal data concerning the previous, current or future physical or psychological state of health of the data subject.”102 Other Member States that have provided a separate definition for the concept of medical data seem to cover the same scope [Junion 2010]. Although this definition certainly leaves room for discussion, it does seem to support a broad definition of the concept of medical data. This is, however, a definition found in the national implementation of certain Member States and only relates specifically to medical data. One can therefore not deduce general conclusions from this, although both this definition and the previously mentioned working document of the Article 29 Working Party seem to favor a broader definition.

Another interesting notion can be found in Belgian law. The preparatory works of the Belgian Privacy Act address the issue of the scope of the concept of sensitive data.103 In order to establish whether personal data can be regarded as sensitive, one needs to assess whether the personal data at hand relates directly to one of the types of sensitive data enumerated in the Belgian Privacy Act or whether the sensitivity becomes apparent from the personal data itself.104 The Belgian legislator wanted to keep the scope of the concept of sensitive data within reason and therefore requires that the sensitivity of certain personal data can be established with certainty or at least with probability bordering to certainty.105 For instance, the mere fact that a person bought a copy of the Qur'an is not enough to establish with certainty that this person is a Muslim and can therefore not be considered as sensitive personal data.

From this, one can conclude that the Belgian legislator supports a rather broad interpretation of the concept of personal data, yet does not support the broadest interpretation of this concept as such interpretation would lead to unreasonable results. A mere national implementation and interpretation of the directive can in principle not be applied on a pan-European level, but could be defended in this.

---

98 See for instance [Junion 2010].
99 Article 7, §1 Act of 8 December 1992 on the protection of the personal sphere regarding the processing of personal data (Belgian Privacy Act), Belgian State Gazette 18 March 1993.
100 Article 6, §1 Belgian Privacy Act.
101 Article 8, §1 Belgian Privacy Act.
102 Translated from Dutch. Original text: “alle persoonsgegevens die de vroegere, huidige of toekomstige fysieke of psychische gezondheidsstoestand van de betrokkene betreffen”, [De Bot 2001]
103 Memorandum by the Belgian Chamber of Representatives 1997-1998, doc. 1566/1, 33-34.
104 See also [De Bot 2001].
105 Memorandum by the Belgian Chamber of Representatives 1997-1998, doc. 1566/1, 33-34.
From previous analyses, one can deduce that the European legislator and the Article 29 Working Party support the notion of reasonability in applying and interpreting the directive. Although Directive 95/46/EC is aimed at providing the European citizen with a broad scope of data protection, it is clear that the scope of the provisions found in the directive can never be applied or interpreted in such manner that it would lead to unreasonable or undesirable results.

Regarding the interpretation of the concept of sensitive data and its application to the IoT, one must therefore defend the test of reasonability. The concept of personal data can be interpreted in a broad manner, but cannot be stretched to the broadest possible scope.

IoT actors are required (nr. 3C) to ensure that they are aware of the scope of the notion of sensitive data under the national legislation applicable to the processing of personal data under their control. Follow-up on the review of Directive 95/46/EC is required to ensure ongoing compliance with changing data protection principles.

4.2.6 How to obtain the data subject’s consent?

As can already be concluded from the analysis of the European legal framework for data protection so far, the data subject’s consent is an important notion in the processing of personal data.\textsuperscript{106} Also for the processing of sensitive personal data, the data subject’s consent is one of the few cases in which such processing can be performed.\textsuperscript{107} It should be noted though, that consent is certainly not the only way for conducting a legitimate processing of personal data, even sensitive personal data. As Member States can enlarge the cases in which personal data can legitimately be processed or the exceptions in which sensitive personal data can be processed, it becomes clear that the data subject’s consent will not be required for a fair degree of processing. However, the vast majority of the cases will still require the data subject’s consent as the cases of article 7 and the exceptions of article 8 of Directive 95/46/EC are still rather narrow and allow for relatively little application, even when enlarged in national implementation by the Member States.

As explained earlier, the consent can be given both explicitly and implicitly [De Bot 2001]. Important is that the consent is given freely, without external influence, aimed at a specific processing. Furthermore, the consent needs to be informed\textsuperscript{108}, meaning that the data subject needs to be well aware of the means and purposes of the processing for which he grants his consent. Although the directive itself does not state that consent needs to be provided in writing, it is clear that from an evidential point of view written consent will always be preferred. In certain cases, written consent will be mandatory, for instance in certain national implementations of the provisions of the directive.\textsuperscript{109} As national implementations of the Directive – and thus of the concept of consent – may differ, certain Member States may impose more thorough requirements on how the data subject’s consent can be provided.

Although it may not seem an easy task to ask each data subject involved in a certain processing of personal data for his consent, it does serve a dual purpose. While the consent enables the data controller to perform his envisioned data processing in a legitimate manner, the fact that he needs to inform the data subject before this party can make his informed decision, could also serve as compliance to the duty to inform the data subject\textsuperscript{110}.

\textsuperscript{106} Article 7 (a) Directive 95/46/EC.
\textsuperscript{107} Article 8 (2) (a) Directive 95/46/EC.
\textsuperscript{108} Further on informed consent [Van Alsenoy 2007].
\textsuperscript{109} For instance in processing sensitive and medical personal data in Belgium, written consent is mandatory: Articles 6 and 8 Belgian Privacy Act.
\textsuperscript{110} Article 10 Directive 95/46/EC.
The most common way of receiving consent is using a consent form. Such form provides the data subject with all the information he needs to know before making his free, specific and informed decision on granting his consent to the processing of his personal data. The idea is that the data subject carefully reads the consent form before signing it and handing it back to the data controller. In practice, however, the use of consent forms could lead to certain issues.

One issue with using consent forms is that they are more often than not based on standard forms that are barely edited to fit the specific cause they serve.\(^\text{111}\) If a consent form provides only a general repetition of the data subject’s rights, which could be copied directly from Directive 95/46/EC, the data subject will still not be well informed to provide his consent to the processing at hand. One can therefore recommend that consent forms need to be drafted with care to ensure that the data subject becomes fully aware of the processing for which his consent is sought, its actors, its means and purposes and which personal data is required for such processing. Only in such case, a signed form can indicate compliance to the duty to inform the data subject, as well as the clear and written consent of the data subject to the processing of his personal data.

It is, however, no easy task to draft a clear and informative consent form. To make the data subject fully aware of the precise nuances involved in the processing at hand, the actors and their precise roles and the exact means and purposes of the processing, requires precise drafting that will more often than not result in a long and tedious text unintelligible to all people but lawyers. One will therefore have to find a compromise between the need for the consent form to be precise and complete and the request for user friendliness.

An unintelligible text may read to the refusal of the data subject to sign the form as he does not comprehend what is laid out before him, but it may also go by unnoticed. Although consent is an important principle in the field of data protection – after all it provides the data subject with the power to personally determine which of his personal data can be processed in which processing – it seems to have lost some of its original strength. In the current society, data subjects need to provide their consent on a daily basis for a plethora of services.\(^\text{112}\) As a result, a majority of data subjects has become conditioned to signing consent forms and currently does so without bothering to look what the contents of the form are.\(^\text{113}\) The threshold for providing consent to a specific processing of his personal data has become so low that the very use of such consent forms may certainly be questioned.

It is therefore recommended to draft clear consent forms that invite the data subject to actually read them instead of blindly signing them and to monitor whether the data subject has really understood what is conveyed to him in the consent form.\(^\text{114}\) This is especially of importance to the IoT, as a rise in devices and objects that become interconnected and could possible process personal data would lead to an increase in consent forms that would need approval from the data subject.

As the implementation of the IoT could lead to an increase of consent forms, that would need to be signed by the data subject and send back to different parties, one could propose a more integrated approach [Verhenneman 2008]. In an integrated approach, one could group related cases of personal data processing together in a general consent form that would cover all aspects of these cases of data processing. This would lower the amount of consent forms submitted to the data subject, but would

---

\(^\text{111}\) Many standard templates for consent forms or even consent form generators can be found on the Internet.

\(^\text{112}\) Installing software, creating an account on a website, etc. The number of examples in which personal data is processed is countless and virtually all of these examples require the data subject’s consent.

\(^\text{113}\) Especially on the Internet, the simple ‘click to accept’-button has lowered the threshold to providing consent even further.

\(^\text{114}\) The need for stronger and clearer rules on informed consent was also addressed by the Commission: Communication of 4 November 2010 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, “A comprehensive approach on personal data protection in the European Union”, COM(2010) 609, 8-9.
also enlarge the contents of that general consent form. Careful drafting and grouping is therefore of utmost importance in such integrated approach. The ethics guidelines, drafted in the framework of deliverable 7.4 of the uTRUSTit project, will include examples of compliant consent forms. This ethical analysis will also demonstrate how certain States may impose stricter requirements on the provision on the data subject’s consent.

Carefully drafted consent forms – for instance in a multi-layered format – are required (nr. 5A) to ensure compliance to the requirement of consent and the right to information. Note that such privacy policies and consent forms need to be compliant with national data protection legislation.

4.2.7 How to inform the data subject?

The objective of Directive 95/46/EC is to protect the rights and freedoms of the natural person regarding the processing of his personal data. Apart from regulating the processing of personal data by listing requirements that all cases of processing of personal data need to comply to, the directive also creates a number of rights aimed at further empowering the user against any unwanted or unclear processing of his personal data. One of those rights, as explained earlier under sector 4.1.1.3, Data subject’s rights, is the right to information.

The data subject has the right to be informed on a number of topics, such as the identity of the controller, the purposes of the processing, the identity of the recipients, whether replying to the questions is obligatory and on the existence of access rights and a right to rectification. Such information should enhance the transparency of the processing of the data subject’s personal data and should result in a better informed data subject, which – as discussed previously – is necessary in order for the data subject to provide a duly informed consent.

However, as indicated in the assessment of the data subject’s consent in relation to the IoT – sector 4.2.6 – there are certain concerns regarding the degree to which this provision can reach its intended effect. Just like consent forms, the information that data controllers need to provide to the data subject is more often than not included in standard privacy policies [Van Eecke 2009]. Like consent forms, such privacy policies are often either very concise and therefore do not provide the data subject with the information he would really need in order to provide his informed consent, or they are very detailed and therefore virtually unintelligible to the average citizen without a degree in law. While such privacy policies may technically comply with the requirements set forth in the Directive, they do, in effect, not attain their intended goal, namely the enhancement of the transparency of the processing of the data subject’s personal data.

The European Commission and the Article 29 Working Party have taken note of this inadequacy of the right to information under the current provisions of Directive 95/46/EC. Already in the first report on the implementation of the directive by the Member States in 2003, the European Commission noticed that the Member States had adopted rather divergent national legislation on this topic.116 Regarding the implementation of the right to information, the Commission made the following remark:

The implementation of Articles 10 and 11 of the Directive showed a number of divergences. To some extent this is the result of incorrect implementation, for instance when a law stipulates that additional information must always be provided to the data subject, irrespective of the necessity test the Directive foresees, but also stems from

115 Articles 10 and 11 Directive 95/46/EC.
divergent interpretation and practice by supervisory authorities. Submissions stressed the difficulties for multinational companies operating on a pan-European level that arise from these divergences.\footnote{Ibid., 17-18.}

The Article 29 Working Party therefore called for more harmonized information provisions.\footnote{Ibid., 24.} The Commission followed up on this report in 2007.\footnote{Communication from the Commission to the European Parliament and the Council of 7 March 2007 on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87, 11p.} In this communication, it is stated that guidelines for controllers and models for multi-layered privacy notices have been provided.\footnote{Ibid., 4.} For further harmonization efforts, the Commission refers to the works of the Article 29 Working Party.\footnote{Ibid., 9-10.}

One of such works of the Article 29 Working Party is a 2001 recommendation on online personal data collection [Working Party 43]. In this document, the Working Party aims to set a number of minimum obligations for controllers [Working Party 43]. Regarding the right to information, the Working Party lists what information should be provided to the data subject at which time and how [Working Party 43]. The Working Party lists both the basic information required by the directive as well as additional information necessary\footnote{Note that articles 10 and 11 of the directive list the basic mandatory information that needs to be provided. Additional information can be supplied, but only where necessary. This necessity test is aimed at avoiding long and tedious privacy policies as they provide information the data subject may not need to know and due to their unintelligibility fail to enlighten the data subject with the information he does need to know.} to provide the data subject with a fully clear and transparent overview of the processing at hand.

The Article 29 Working Party builds forth on this issue in a 2004 opinion [Working Party 100]. In this opinion, the Working Party aimed to establish pragmatic solutions towards developing more harmonized information provisions. Four reasons were given for such approach [Working Party 100]:

- The need to ensure more compliance with current information requirements,
- The need to raise citizen’s awareness on data protection rights,
- The need to present information with meaningful and appropriate content to the data collection situation, and
- The need to improve the quality of data protection from the individuals’ perspective.

One of the main findings of the Working Party is the concept of the multi-layered notice, where each layer provides the data subject with information he truly needs in order to provide his duly informed consent and where all layers together comply with relevant legislation [Working Party 100]. Such multi-layered notice could provide the data subject with a clear and summarized version of relevant information on one layer. The full version of the notice – necessary for compliance to national legislation – is moved to another layer. Therefore, the notice is both compliant, because all required information is there, and easily accessible to the data subject.

The Working Party endorses a three-layer notice [Working Party 100]. The first layer would provide the core information as required by the directive, as well as additional information necessary to be provided on beforehand to ensure fair and lawful processing. The second layer would provide a condensed notice, which would repeat the information provided on the first layer in a more expanded
version, including contact information. The third layer would provide the full notice, necessary for compliance to national data protection legislation.

Although the three-layered privacy notice proposed here could be an interesting item in enhancing the transparency of the processing and the information provided to the citizen, it seems that this proposal has not been taken up by many data controllers. A 2010 communication from the Commission remarks that recent reporting evidences that online privacy notices are still “unclear, difficult to access, non-transparent and not always in full compliance with existing rules.” The Commission therefore considers:

- introducing a general principle of transparent processing of personal data in the legal framework;
- introducing specific obligations for data controllers on the type of information to be provided and on the modalities for providing it, including in relation to children;
- drawing up one or more EU standard forms (‘privacy information notices’) to be used by data controllers.

In order to ensure transparency of the processing and to provide adequate information to the data subject in the context of the IoT, one could therefore recommend the use of the three-layered notice or similar techniques. Multiple layers could provide the data subject with clear and concise information that will assist him in making a duly informed decision on providing his consent. National privacy legislation requiring long and obsolete information to be provided can still be complied with by pushing such obsolete information back to the deeper layers of the notice. The efforts of the Commission on EU standard forms will need to be followed up.

Carefully drafted privacy policies – for instance in a multi-layered format – are required (nr. 5B) to ensure compliance to the requirement of consent and the right to information. Note that such privacy policies and consent forms need to be compliant with national data protection legislation.

4.2.8 Data access rights

As discussed earlier under sector 4.1.1.3, the data subject has a right of access to the data concerning the processing of his personal data. Note that the directive has formulated this provision in a broad sense, so that the right to correction – often discussed separately from the right of access – is included under this provision. The goal of the right of access is to provide the data subject with a certain degree of control over his personal data that is being processed. Therefore, the data subject may ask for information regarding whether or not data relating to him are being processed, as well as for information on the purposes of that processing, involved categories of data and recipients. Such information needs to be provided to him in an intelligible form and without constraint and excessive delay or expense. The right of access is an active right of the data subject, requiring him to actively solicit access to the data concerning the processing of his personal data. The right to information, by contrast, allows for a more passive stance from the data subject as he is being informed. Note that the scope of the right to access as well as the procedural requirements to gain such access can differ according to national legislation.

124 Ibid., 6.
125 Article 12 Directive 95/46/EC.
However, as evidenced in previous subsectors, a number of rights aimed at protecting the data subject’s rights and freedoms concerning the processing of his personal data have appeared to fail to meet their goals. One therefore needs to look how the data subject can attain a higher level of control over his personal data. The European Commission has addressed this issue in a communication.\textsuperscript{126} The Commission identifies two conditions that need to be met in order to ensure a high level of data protection to the data subject’s personal data.\textsuperscript{127} On the one hand, the processing of personal data by the data controller needs to be limited in relation to its purposes. This means that the data controller can process no more data than absolutely necessary to attain the envisioned purposes of the processing, a principle earlier addressed under sector 4.2.4, proportionality and how to implement in the IoT, as the principle of data minimization. On the other hand, the Commission finds that data subjects need to be provided with effective control over their own data.

The Commission refers to the Charter of Fundamental Right of the European Union.\textsuperscript{128} Article 8 of this Charter concerns the protection of personal data and stresses the principles of fair processing, legality and consent. This article also addresses the right of access to data and the right to correction.\textsuperscript{129} The Commission has hereby stressed the importance of the right of access and the need to ensure that this right is duly observed. However, given the many differences in national implementations of Directive 95/46/EC by the EU Member States, there is no harmonized approach in the exercise of this right. In this respect, the Commission also references the online environment, in which data retention is more prevalent and often occurs without the data subject’s knowledge of it or consenting to it. The Commission refers to the particular case of online social networks, where data retention is one of the cores of the business model of the providers of such services. If an individual is unable to retrieve his personal data from such social network, then the exercise of his right of access and his right to correction and deletion are impeded.\textsuperscript{130}

The Commission therefore proposes a number of measures to ensure a higher degree of data protection to the data subject’s personal data.\textsuperscript{131} Firstly, the principle of data minimization needs to be strengthened. Second, the modalities for the actual exercise of the right of access, correction and deletion need to be improved. This would be done by subjecting the data controllers to deadlines and requirements for allowing the data subject to exercise his right of access in an easier and effective manner. Third, the Commission proposes a right to be forgotten, enabling the data subject to effectively delete his personal data when no longer needed for the data controller’s processing. Lastly, this is complemented by the principle of data portability. This would enable the citizen to withdraw all of his personal data from one service or application in order to transfer this data to another service or application.

The Commission’s concern on the exercise of the right of access on the Internet can be transposed to the IoT. As interconnections between devices and objects are becoming ever more pervasive and ubiquitous, the data subject may very well lose track of which of his personal data is retained by which data controller. Once more, an adequate execution of the data subject’s right to information will lead to the data subject granting his duly informed consent. The data controller will


\textsuperscript{127} \textit{Ibid.}, 7.


\textsuperscript{129} Article 8 (2) Charter of Fundamental Rights of the European Union.


\textsuperscript{131} \textit{Ibid.}, 8 and as already discussed under the subchapter on the review of Directive 95/46/EC (sector 4.1.3 of the present deliverable).
therefore need to address the data subject’s right of access and the modalities to exercise this right in his privacy policy.

Access to personal data is also a concern for the data controller himself. Under article 17 of Directive 95/46/EC, the data controller is required to implement appropriate technical and organizational measures in order to prevent unauthorized access to the personal data in his possession. In the Article 29 Working Party opinion on online social networking, for instance, the issue of access to profile information is addressed [Working Party 163]. The Working Party recommends, for instance, that default settings need to restrict access to personal data on profiles [Working Party 163]. Note also the case of the user of a social network who decides to make his profile fully public, thus dropping all access restrictions, and thereby becomes subject to controller duties as his processing of personal data has gone beyond the coverage of the household exception.133

Also in the IoT, access rights will be an important issue to observe. The growing scope of the interconnection of devices and objects could lead to increased security concerns. An adequate system for access rights management will therefore need to be included. Data controllers will therefore need to clearly define the roles of the authorized users and their respective access rights.

More transparency and data minimization is required (nr. 6) to ensure compliance to the right of access.

4.2.9 Radio-frequency identification

As indicated earlier under section 3.1, European Commission, RFID has been identified as one of the main technologies that will be crucial to the large-scale implementation of the IoT. The European Commission, for one, explicitly refers to the use of RFID as an integral part of its strategy relating to the IoT. Also the Assistant European Data Protection Supervisor, Giovanni Buttarelli, explicitly refers to RFID as one of the main building blocks of the IoT [Buttarelli 2010].

The use of RFID is, however, not without controversy. As an RFID tag can consist of a very small integrated circuit and antenna, it becomes possible to insert RFID tags in virtually any household item without the owner of said item even knowing of its presence. As RFID tags are commonly used for identification and tracking, this may pose substantial privacy concerns to the data subject. If, for instance, one purchases a coat with an RFID tag embedded in the lining, this person could in theory be tracked virtually anywhere a RFID-reader could be placed. As the price of an RFID tag has been reduced to just a few cents, one can expect the number of tags surrounding the data subject in his home only to increase.

Therefore, it is important that the use of such RFID tags is subject to certain regulation. Such regulation should make it clear to the data subject where he can expect to find RFID tags and what he can expect them to do. Only if the use of RFID becomes sufficiently transparent, the data subject will confer trust upon this technology. Given the importance of RFID to the IoT, trust in RFID will lead to more trust in the IoT. Regardless of the importance of an adequate legal framework for the use of RFID, there is currently no legal framework in place that covers all aspects of RFID and the IoT [Weber 2010].

---

132 This is a reaction against Facebook’s default use of opening up new potentially privacy-infringing features, requiring users to opt-out if necessary, instead of having them opt-in to such features.

133 Discussed earlier under sector 4.2.3, application of the household exception.

134 For access management for privacy in a medical context and general security policy recommendations in the medical sector [Verhenneman 2008].

Legislators and scholars worldwide have understood the advantages and the risks of RFID and have voiced opinions on this subject. The European Commission, for one, already communicated on the need for a policy framework on RFID in 2007. In this communication, the Commission stresses the beneficial factors of RFID – especially in the sectors of transport, food and health – and the current concerns on this technology resulting from the lack of an adequate legal framework. With regards to the current legal framework, the Commission remarks that RFID is currently mainly regulated by the Data Protection Directive – Directive 95/46/EC – and not so much by the e-Privacy Directive – Directive 2002/58/EC. While it is true that the e-Privacy Directive is aimed specifically at electronic communications, it contains provisions applicable to a more advanced level of technology than what the Data Protection Directive currently has to offer. As the main issue with the Data Protection Directive is its lack of adaptation to modern technologies, it would therefore be interesting to see such more technologically advanced provisions included in this directive after the pending review.

The Commission further addresses the Member States to adopt adequate national measures. Given the diversity of RFID tags and the ongoing technological progress in this field, Member States will have to continuously monitor the implementation of RFID in their territory. Such monitoring will have to focus, inter alia, on the fields of radio spectrum, standards and health and environmental concerns. Finally, the Commission pledged further actions on RFID, as well as the development of a research agenda on this matter.

The Commission’s 2007 communication was the subject of a 2008 opinion by the European Data Protection Supervisor (EDPS). In this opinion, the EDSP mainly stresses that the provisions of Directive 95/46/EC are still valid and that no amendments would be necessary to mitigate the risks set by the use of RFID. Given the nature and the impact of RFID, the EDPS does seem to endorse the adoption of a specific framework for RFID-usage. Although the option of self-regulation does appeal to both legislators and scholars, the main conclusion is that certain involvement of the legislator will be necessary to ensure that all parties involved take up the proposed measures [Weber 2010]. The EDPS also mentions the need for a privacy-by-design approach, whereby techniques and standards are used to ensure data protection compliance by envisioned RFID products and services before their launch.

In the Commission’s 2007 communication, the Commission also addressed the Article 29 Working Party as the entity that should monitor how Member States regulate RFID in order to maintain a certain common approach. For the Working Party, RFID is no new and upcoming issue as it already addressed

---

140 Ibid., 9-11.
142 Ibid., 6.
this topic in 2005 [Working Party 105]. After a more general overview of RFID, its benefits and drawbacks, the Working Party finds that, in the cases where personal data is processed, the use of RFID could fall under the Scope of Directive 95/46/EC [Working Party 105]. The use of RFID would therefore need to comply with the principles of the directive. Given the multitude of different RFID tags, the Working Party calls for more standardization and interoperability [Working Party 105]. The Working Party brings two issues to the forefront: awareness and deactivation [Working Party 105]. The data subject needs to be made aware of the presence of RFID tags around him. As discussed earlier, RFID tags can make use of very small hardware, making it easy to hide such tags on places the data subject would never expect to find them. If the location of the tag would be made clear to the data subject, he may approach this technology with more confidence. Second, certain tags only serve a limited purpose – for instance security tags used in stores as anti-theft measure – and should therefore not remain active longer than necessary to attain their purpose. In the case of the security tag, the tag on an item should be disabled after its purchase. The Working Party later that year commented on the results of the public consultation on RFID [Working Party 111]. It found that most participants to the consultation agreed to the main lines of thought formulated in the previous opinion.

The Commission resumed work on RFID in a 2009 recommendation.143 In this recommendation the Commission largely repeats the highlights of its 2007 communication. Again, the Member States are called upon to monitor the implementation of RFID in their territory and the compliance thereof to the fundamental rights and freedoms of the data subject with regards to the processing of his personal data.144 Again the Commission addressed the Article 20 Working Party to keep a general overview on the actions proposed by the Member States. The Commission also introduces the idea of a Privacy and data protection Impact Assessment (PIA).145

This recommendation was followed by an opinion of the Article 29 Working Party [Working Party 175]. The Working Party also references the Privacy and data protection Impact Assessment (PIA) that according to the Commission’s recommendation should be made by RFID operators. Industry representatives and other stakeholders have drafted a PIA framework, which is what the Working Party comments on in its opinion. As such assessment needs to be made before deploying a certain product or service, the manufacturer or service provider – in the case of personal data processing also acting as data controller – will need to address privacy considerations before launching his product or service, leading to an implementation of the notion of privacy-by-design [Working Party 175]. Therefore a PIA could be beneficial for both data controller and data subject. The proposed PIA framework distinguishes four types of RFID tags based on degree of personal data processing and control by the data subject. It does, however, not contain a clear risk assessment model [Working Party 175]. Because of this and other shortcomings, the Working Party does not endorse the proposed PIA framework.

The proposed PIA framework was revised in January 2011 [Enisa 2010] and discussed by the Working Party in February 2011 [Working Party 180]. The new proposed PIA framework includes a pre-assessment phase as well as a risk assessment phase. This proposal therefore incorporates the recommendations previously made by the Working Party. The proposal is therefore endorsed by the Working Party and will be implemented. A Commission report on the implementation of its 2009 recommendation will further evaluate the uptake of the PIA framework. This report was originally planned for May 2012, but will likely be postponed.

In summary, one can endorse the decision to rely on a more privacy-by-design approach by adopting a PIA framework. This leads to a broader scope of control ex ante, therefore ensuring that new RFID-related products and services comply with the requirements set forth by the Data Protection

---

144 Ibid., mainly on p3 and p6-7.
145 Ibid., mainly on p3 and p6-7.
Directive and the e-Privacy Directive. This will lead to a higher trustworthiness of RFID technology, which is necessary for the data subject to confer a higher degree of trust into such technology. As RFID is one of the key technologies in the IoT, a higher degree of trust in RFID will lead to a higher degree in the IoT.

The need for transparency is also required (nr. 7) for the use of RFID. The citizen needs to be made aware of the presence of RFID tags surrounding him and should – ideally – be enabled to control these tags.

4.3 Conclusion

Section 4, privacy policy framework, focused on the application of the current EU legal framework on data protection to the IoT. As indicated under section 3, legal risks of the IoT, privacy and data protection relate to a number of action points, set by the European Commission as vital to the implementation of the IoT. One can therefore conclude that compliance to data protection legislation will be important to enhance user trust in the IoT.

From the general overview of the principles of Directive 95/46/EC, one can remember that the interconnections set by the IoT will likely also be used to transport personal data. If the actors controlling certain products and services of the IoT are therefore processing personal data, they need to be regarded as data controllers in the sense of Directive 95/46/EC. The principles of the directive will apply and need to be complied with.

As the directive only gives the main principles for transposition into national legislation by the EU Member States, one will have to establish which national data protection legislation is applicable to the processing of personal data at hand. As the Member States have adopted legislation that is, at points, highly divergent from one another, it will be imperative to comply with the specific provisions adopted by the competent legislator. Cross border processing may, in certain cases, even be subject to multiple national privacy legislation.

Note that Directive 95/46/EC is currently under review. As the main principles of this directive can be traced back to the early 1980’s, it is no surprise that such principles cannot be stretched indefinitely for application to the ever-changing information society. A thorough review will be necessary to ensure that the EU legal framework on data protection becomes more future proof. Such review may also add new principles, such as the right to be forgotten, data portability and the right to silence of the chips.

Next, a number of more specific privacy concerns relating to the IoT were addressed.

One concern is that the changes in society have lead to changed data processing models. As the notions of controller and processor were developed for more static data processing models, it has become very difficult to determine the precise role of the actors involved in the data processing. However, as the controller and the processor have very different responsibilities and liabilities, it is of utmost importance to clearly establish who can be attributed which role. Here, one can refer to the opinion of the Article 29 Working Party that helps in establishing the role-division. For future use, specific attention should go out to (co-)controller contracts that can further delineate the precise tasks and responsibilities of each party. A clear delineation of the responsibilities of controller and processor will be important to the IoT, as the web of interconnections realized by the IoT may make it difficult to discern the precise scope of the tasks of all actors involved.

The main concept of the directive itself, personal data, has also become subject of concerns. As is the case for a number of provisions in the directive, the concept of personal data can be defined in a
very narrow sense or in a very broad sense. The Article 29 Working Party seems to endorse a broad
definition, yet also warns for overstretching the concept. For application to the IoT, one will have to
analyze the types of data that may be subject to processing for further assessment of whether these
types of data constitute personal data or not. This is important to establish whether the principles of EU
data protection will be applicable to a particular actor in the IoT. As these principles will only apply
when personal data is processed, it is evident that a clear understanding of the scope of that notion is
needed.

Also the exceptions to the principles of the directive seem to be subject to the same concerns
regarding their precise scope. One of the main exceptions is the household exception, exempting
personal data processing for personal or household use. Here, it is important to establish what
constitutes personal use. Given the fact that more and more data is user-generated and published on
the Internet, one can wonder whether such publicity can still count as personal use, even if the data
was published in a purely personal capacity. Here, the reasoning of the European Court of justice’s
Lindqvist decision can be followed. If the data is posted to a social network profile that has been made
visible to all users, or even indexable by search engines, then the household exception cannot apply as
this does not constitute personal use. Data on a profile that is only visible to a selected number of
friends, however, does constitute personal use. Although this reasoning has been upheld in subsequent
cases, it fails to address the issue of threshold for such publicity and leads to an invariable all-or-nothing
approach. For application to the IoT, this is important as actors identified as controllers of the
processing of personal data will want to know whether they can benefit from an exception to the
general rules of EU data protection.

The principle of proportionality is one of the cornerstones for fair and lawful data processing and
even of EU community law in general. Its importance is therefore not to be underestimated, yet the
precise scope of its implication remains rather vague. In summary, one will first need to determine
whether the proposed means are adequate to attain the envisioned purposes. Second, one needs to
assess whether such means are necessary to attain the envisioned purposes and whether they do not
go further than what is necessary for attaining these purposes. Complying with the principle of
proportionality in data protection legislation will therefore require an ex ante analysis of the data
controller to ensure that he employs the correct methods of data processing and that no more data is
processed than necessary. Given the influence of the processor on the means, clear agreements
between controller and processor on this subject are imperative. Also this principle will be of capital
importance to the IoT. If a provider of IoT services is identified as a controller of the processing of
personal data under the EU legal framework on data protection, he will need to ensure that
proportionality is sufficiently implemented in the processing under his control.

Apart from providing the general principles for the processing of personal data, the directive also
defines special categories of personal data of which the processing is in principle forbidden. Under the
directive, this includes judicial data and so-called sensitive data. Note that while the directive
understands medical data as part of sensitive data, certain Member States have adopted medical data
as a separate category. Once more, the precise scope of this notion leaves room for very broad or very
narrow interpretations. From the rather limited literature on this aspect, one can conclude that the
interpretation of the concept of sensitive data should be approached with reason. In order to
determine whether a certain fact can be considered as sensitive data, it will have to be established with
reasonable certainty that this fact indeed actually reveals sensitive data on the subject. As the
processing of sensitive data is subject to harsher restrictions than the processing of regular personal
data, IoT actors will need to have a clear understanding of the concept of sensitive data in the
jurisdictions in which they process personal data.

One of the most important requirements for personal data processing is the data subject’s
informed consent. The data subject needs to be adequately informed before he can freely give his
informed consent, thus necessitating adequate information. Such is usually performed through the use
of consent forms. Such consent forms, however, are often highly general and do not provide the clear and adequate information needed to provide informed consent. One will therefore have to carefully draft a consent form that will provide the data subject with the precise information he needs, yet without falling into the use of unintelligible legal jargon. One will have to monitor whether the data subject has fully read and understood the form before signing it. One should also consult national data protection legislation, as different Member States may impose divergent criteria on how to obtain the data subject’s consent. IoT service providers qualified as controllers under the EU data protection framework will need to ensure that they understand the requirements on how to obtain the data subject’s consent, found in the national data protection legislation of the Member States in which they process personal data.

As already became apparent in the discussion on consent, the data subject needs to be adequately informed on the processing of his personal data. Just as is the case with consent forms, the data subject’s right to information is often complied with by the data controller by providing a standardized privacy policy that often does not inform the data subject on the information he truly needs. One can therefore propose a different approach, found in the multi-layered model envisioned by the Article 29 Working Party. Such model could provide concise, yet relevant, information in a first layer, so that the data subject is immediately made aware of it. This information can be further explored and more detailed in other layers. The final layer could provide the data subject with the information required by national data protection legislation, which is more often than not a copy-paste of certain principles and therefore not effectively informative to the data subject. Also here, a clear understanding of how to draft compliant and effective privacy policies will be necessary for IoT actors to comply with national data protection legislation applicable to their processing of personal data.

Another right of the data subject that has fallen subject to concerns is the right of access. This right aims to provide the data subject with a certain degree of control over his personal data. Such control seems to have gotten lost in the online environment, where data retention without the data subject’s knowledge is highly prevalent and may even be the core of the business model of the service – as is the case in social network services. As a reaction to this, the principle of data minimization needs to be strengthened, the modalities for effective exercise of the right of access – including the right to correction and deletion – needs to be improved and the right to be forgotten – linked to data portability – needs to be implemented. As was the case for the right to information, IoT actors qualified as controllers of the processing of personal data will need to ensure compliance of their processing to national data protection legislation applicable to their processing.

Lastly, this sector addressed the use of RFID, which has been defined as one of the key technologies in the implementation of the IoT. Given the lack of a clear and encompassing legal framework on this topic, policymakers and scholars have looked at how to bring more legal certainty to the use of RFID, eventually leading to more trust in the IoT. Although self-regulation was met with positive notes, the general consensus is that a certain degree of governmental control is still necessary. Two points were indicated as imperative: awareness and control. It is required that the data subject is made aware of the presence and the competences of the RFID tags around him and he must be able to exercise a certain degree of control over them. Hereto, the Member States were addressed to adopt adequate legal measures and to have the Article 29 Working Party monitor them. The Article 29 Working Party also monitored the development of a Privacy Impact Assessment framework by industry partners and other stakeholders. An ex ante approach to data protection compliance will lead to more privacy-by-design and will eventually increase the trust in RFID – and IoT – solutions.

From this analysis, a number of legal requirements for the processing of personal data in relation to the IoT were deduced. These legal requirements will be summarized, together with the legal requirements on liability issues relating to the IoT, under sector 6, summary of legal requirements.
5. **Liability issues**

As indicated under sector 3, legal risks of the IoT, it has been established that more concrete legal provisions on liability issues relating specifically to the IoT will have to be adopted in order to provide for a coherent legal framework for trust in the IoT. This is, for instance, evidenced by the European Commission that has adopted actions points relating to the IoT from which liability issues can be deduced.\(^{146}\)

Therefore, the currently existing pan-European regulations on liability issues will be analyzed in the present sector. After a more introductory assessment of the general liability principles, a number of liability regulations with specific importance to the IoT will be analyzed.

### 5.1 General liability regulation

As indicated under sector 4, legal provisions on privacy can be found in a variety of legal instruments, often covering a different aspect of the general EU framework on the protection of privacy and data protection. The same can be said about liability as the precise scope of this notion differs greatly amongst different legal instruments.

One notion of liability, for instance, can be found in company law in the guise of the well-known limited liability company (LLC). In general, this concept can be understood as a form of company in which the shareholders are not directly liable for debts of the company other than their share in said company. If one, for instance, invests €50,000 in a limited liability company and said company files for bankruptcy, one can expect to lose a maximum of €50,000.

Liability issues can also be found within the EU legal framework on data protection, specifically regarding the responsibilities of the data controller and processor. Also the EU Directive on e-commerce contains specific provisions on liability.\(^ {147}\) Another directive relates specifically to product liability.\(^ {148}\)

From these different provisions on liability issues, one can deduct several types of liability. In the present subsector, these different types of liability will first be analyzed. Next, in subsector 5.2, specific liability concerns relating to the IoT, an overview of the general principles of the most important legal instruments on liability will be provided, with specific attention to their applicability and issues thereof to the IoT.

#### Civil versus criminal liability

A first distinction must be made between liability under civil law\(^ {149}\) and liability under criminal law. Criminal liability is triggered when a provision of criminal law was violated. For such liability, two key components\(^ {150}\) need to be present: *actus reus* and *mens rea*. *Actus reus* refers to the physical element of a crime being committed, either by acting whereby such act was prohibited or by failing to

---

\(^{146}\) Specifically note action points 1 and 5 of Communication of 18 June 2009 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, “Internet of Things – an action plan for Europe”, COM(2009) 278, 4-5 and 6-7


\(^{149}\) Note that the notion ‘civil law’ in this respect refers to the domain of private law, which generally includes family law, property law, contract law and tort law, as opposed to the domain of public law, which generally includes administrative law, international law and criminal law.

\(^{150}\) As classically found in Belgian law, yet universally applied [Haus 1869].
act when such act was mandatory due to a duty of care. The act or failure to act must correspond to all physical and material elements that constitute the criminal act required by law. Mens rea refers to the moral element of the crime, namely that the actor must have had the intention to commit the crime, regardless of his motives. The intentional element is, however, not always required. Under strict liability, the actor who performed the prohibited act or failed to perform the obligatory act can still be held liable, even if it was not his intention to commit a crime due to his acting or failure to act, regardless of his degree of culpability. Liability under civil law will be covered in the following paragraphs.

**Culpa in contrahendo**

Even though liability under civil law is mostly covered by contractual liabilities, there are a few exceptions in which liability can be triggered even without a directly applicable contractual clause. One of these examples includes the *culpa in contrahendo*, which means as much as ‘fault in the conclusion of a contract’. As negotiations leading up to the conclusion of a contract can often drag on for a long period of time and could require expensive research – especially in large business transactions – it may very well occur that a certain party commits mistakes that could lead to the premature end of said negotiations. If one negotiating party has lost considerable amounts of time and resources on these negotiations and now sees them falling through due to a mistake by another party, he may very well want to seek compensation for the damages he suffered. However, without a formal contract between these parties, general contract law will not be of any use in seeking such compensation. Therefore, the *culpa in contrahendo* provides a remedy to the negotiating party that suffered damages during such contractual negotiations due to a mistake committed by another negotiating party. Even if the negotiations were successful and resulted in a formal contract between the negotiating parties, the *culpa in contrahendo* can still be triggered if later problems arise due to a mistake committed by one of the parties during the negotiation phase.

Given the theory of consent, all parties are free to start and end negotiations with each other [Geens 2003]. They cannot be bound to enter a contractual bond solely based on their negotiations. This contractual freedom, however, does entail a number of obligations. For one, parties are bound to negotiate with care and to not cause damages to another party during or due to the negotiations. If one party suffers damages that are a direct result of another party’s lack of care, then the damaged party can seek compensation [Geens 2003].

Note that this principle is not accepted in all legal systems. Certain legal systems rely on the principle of good faith obligations [Geens 2003] or estoppels [Kessler 1964] as this is the point where contract law and tort law meet.

**Contractual liability**

The main type of liability under civil law is a direct result of contractual obligations between parties. This liability will be triggered when a party does not live up to how he was supposed to act – or refrain from acting – under the contractual provisions he agreed to. Contractual liability can be avoided by calling *force majeure* or through hardship or exclusion clauses.

Force majeure refers to a situation beyond the parties’ control that prevents one or more parties from performing their contractual obligations. Where force majeure is commonly used in situations where the performance of one’s contractual obligations has become impossible, hardship provides a means for the situation in which the performance of one’s contractual obligations has become unreasonable. Hardship is therefore applied when a certain unforeseen and uncontrollable situation

151 For one, this entails a duty to duly inform the other party [Dumortier 2010].

152 Note that in the article referred to here, the author analyzes several legal concepts in order to assess which would fit the *culpa in contrahendo* best. The author concludes that the Aquilian liability – which will be discussed later – is a best fit.
has rendered the performance of the obligations of one of the parties excessively burdensome. While such party will not want to perform his obligations as stated in the contract, he will still want to perform under alternative conditions. While the goal of force majeure is non-performance, the goal of hardship is therefore performance under different conditions. Parties can further limit their liabilities through mutually agreed exclusion clauses. As the precise scope of such exclusion is a specific topic of concern, the subject of contractual limitations of liability will be further elaborated on under subsector 5.2.3, contractual limitations of liability.

**Aquillian liability or negligence**

The Roman *lex Aquilia* was designed to provide compensation for unlawfully inflicted damages.\(^{153}\) Although the *lex Aquilia* was originally only intended for use in limited cases, its scope was gradually expanded. Due to its continued use and expansion, the principles of the *lex Aquilia* were preserved in later legal systems based on Roman law, eventually ending up in the Napoleonic Civil Code. Therefore, in this Code – as still in use in France and Belgium – one can now find provisions aimed at providing compensation for specific types of unlawfully inflicted damages outside the scope of a contract.\(^{154}\) Note that three elements need to be present for the Aquilian liability to be applicable: faulty act imputable to its actor, damages, or causation [Dumortier 2010].

However, not all legal systems have inherited the Aquilian – also called delictual – liability. In common law systems, this type of liability for unlawful damages outside the scope of a contract can be found under the tort of negligence. In general, negligence consists out of four elements. First, a duty of care must be established. This concept has been established mainly in case law, with the most famous case being Donoghue v Stevenson.\(^{155}\) Later, a three-tier test was devised to establish a duty of care. First, harm must be reasonably foreseeable. Second, the person harmed and the person inflicting the harm must share certain proximity. Lastly, imposing liability must be 'fair, just and reasonable'.\(^{156}\)

Second, it has to be established that this duty of care was breached. In order to breach his duty of care, the person inflicting the harm must have failed to meet the standards that, given the circumstances of the case, could be expected from an average reasonable man. Professionals, for instance, have to observe a higher standard in their duty of care as one can expect them to act in a more skillful way.

Third, damages must be proven. This can be direct material damages, economic losses, and reputational or emotional damages.

Finally, causation needs to be established. It must be assessed whether the damages sustained are a direct result of the breach of one’s duty of care. As essential element in the duty of care itself, proximity is therefore also imperative in the assessment of causation.

**Risk liability**

In previous types of liability, one could always distinguish an element of fault. Whether within the framework of contractual obligations or outside of any contractual obligation, one can always find a remedy for damages suffered by unlawful acts or lack of acting. Another type of liability, however, dismisses the element of faulty behavior and attributes liability solely on the basis of risk. The most well-known implementation hereof is product liability, whereby the manufacturer can be held liable for a defective product, without it having to be proven that he acted faulty. Given the importance of the

---

\(^{153}\) This is referred to as “*damnum iniuria datum*” as found in book 9, chapter 2 of the Digesta in the Corpus Iuris Civilis.

\(^{154}\) See Chapter II, Title IV of Book III of the Belgian Civil Code. Article 1382 generally refers to damages caused by faulty acts by another person. Article 1383 refers to damages caused by neglect or imprudence. Article 1384 concerns damages caused by a person under one’s responsibility or items under his custody. The scope of this article has been gradually expanded over the years. Finally, articles 1385 and 1386 refer to damages caused by animals or defective buildings.

\(^{155}\) Donoghue v Stevenson, [1932] UKHL 100.

\(^{156}\) Caparo Industries plc v Dickman, [1990] 2 AC 605.
legal framework on product liability, this type of liability will be discussed separately under subsector 5.2.1, implementation of product liability in the IoT.

5.2 Specific liability concerns relating to the IoT

5.2.1 Implementation of product liability in the IoT

As briefly discussed earlier, one particular type of liability does not require the element of fault present in other types of liability. In this case, liability is triggered solely on the basis of risk. This particular type of liability has mostly been developed in the sphere of product liability.

The notion of product liability was first developed in the US, where already in the early 20th century a car manufacturer was held liable for damages caused by his products, regardless of the lack of a direct contractual bond between the manufacturer and the person who sustained the damages. 157 While in this case the focal point was still the negligent behavior of the manufacturer, further development of this theory would make the product itself the main focal point, therefore no longer necessitating any degree of negligence. In 1963, the doctrine of strict liability was developed.158 It is argued that even without the presence of negligence, it is a matter of public policy to ensure that harm caused to a person due to a defective product is restituted. Regardless of any fault, the manufacturer is responsible for bringing such product to the market and should therefore be held liable for damages sustained due to its product.

The doctrine of strict liability was first introduced in the EU through a 1977 Council of Europe Convention.159 This Convention introduced the idea of holding producers liable to pay compensation for death or personal injuries caused by a defect in his product.160 Despite its interesting provisions, the Convention was only signed by four parties, none of which have lead to ratification. The Council of Europe’s 1977 Convention has therefore never entered into force. The European Union, already having performed preliminary work on product liability in the framework of consumer protection161, adopted the notion of strict liability in further iterations of its resolutions.162 In 1985, this lead to the adoption of a directive that would lay down general rules on product liability for transposition into national law by all EU Member States.163

The directive was specifically drafted to cover a very wide scope of application and therefore provides rather broad interpretations of the notions of product and producer.164 While the directive originally excluded primary agricultural products and game from its scope, this exclusion was dropped in 1999 at the height of the BSE crisis. Damages caused by nuclear accidents are, however, still excluded.165 Also electricity is considered as a product under the scope of the directive. The directive

---

160 Article 3 (1) European Convention nr. 91 on Products Liability in regard to Personal Injury and Death.
161 Preliminary programme of the European Economic Community for a consumer protection and information policy, OJ C 92, 25 April 1975, 2-16.
164 Articles 2 and 3 Directive 85/374/EEC.
165 Article 14 Directive 85/374/EEC.
also provides for liability of suppliers if it would be impossible to determine the producer. Joint liability is also provided for in the directive.

In order to be rewarded compensation, the person sustaining the damage needs to prove the damage, the defect and the causal relationship between defect and damage. The directive considers a product to be defective “when it does not provide the safety which a person is entitled to expect, taking all circumstances into account”. Examples of such circumstances given in the directive are: “(a) the presentation of the product; (b) the use to which it could reasonably be expected that the product would be put and (c) the time when the product was put into circulation”. The launch of a better product, however, is no reason to consider a product defective. Whereas earlier texts on this subject mostly referred only to damage caused by death or by personal injuries, the directive also includes damages to, or the destruction of, any item of property other than the defective product itself. Limitations to this definition are that the damaged item must have a value of lower than 500 ECU and that it must be intended for private use or consumption and thus mainly used by the injured person for his own private use or consumption. Compensation must also be claimed within three years of discovering the damage and defect and within ten years of the product launch.

The directive also provides for exoneration of liability. The producer will not be held liable if he proves that:

(a) that he did not put the product into circulation; or
(b) that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards; or
(c) that the product was neither manufactured by him for sale or any form of distribution for economic purpose nor manufactured or distributed by him in the course of his business; or
(d) that the defect is due to compliance of the product with mandatory regulations issued by the public authorities; or
(e) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered; or
(f) in the case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product.

While the directive also allows Member States to limit the height of a producer’s total liability, the directive also provides that exclusion clauses limiting the liability of the producer are not allowed.

---

166 Article 3 (3) Directive 85/374/EEC.
167 Article 5 Directive 85/374/EEC. When damage is caused jointly by a defective product and the act or omission of a third party will, however, not reduce the liability of the producer. Liability may be reduced if it is the person sustaining damages who was responsible jointly with a defective product. Article 8 Directive 85/374/EEC.
168 Article 4 Directive 85/374/EEC.
169 Article 6 (1) Directive 85/374/EEC.
170 Article 6 (2) Directive 85/374/EEC.
171 Article 9 Directive 85/374/EEC.
172 Article 10 and 11 Directive 85/374/EEC.
173 Article 7 Directive 85/374/EEC.
174 Article 16 Directive 85/374/EEC.
175 Article 12 Directive 85/374/EEC.
as well as allowing the Member States to adopt derogations to the so-called development risks defense.  

Since its adoption, the directive has been subject to three Commission reviews. The second review, conducted in 2000, followed a Green Paper that would consider a revision of existing provisions on product safety and product liability. This report considers the functioning and the practical impact of the directive and assesses a number of recommendations for further development. Following this review, a Council resolution was adopted, calling for an amendment of the directive in order to include liability of suppliers. The third review, conducted in 2006, builds forth upon previous reviews and the 2002 Council resolution. The report refers to a number of studies from which the Commission concludes that application of the principles of the directive in practice has risen and that these provisions are fairly uniformly implemented and interpreted in the Member States. The Commission therefore proposes further analysis in order to achieve further harmonization.

With the growing number of interconnected devices and objects resulting from the IoT, it is clear that the producers of such devices and objects will at some point face liability for a faulty product. The principles of the EU directive on product liability are, as indicated by the Commission, fairly uniformly implemented and interpreted across EU Member States and can therefore be considered as the general framework on EU product liability. In general, there are only fairly limited exceptions to the producer’s liability. Member States can, however, put certain limitations on this liability. Regarding the liability of producers of products specifically aimed at the IoT, one can therefore refer to the general EU framework on product liability, with specific attention to certain national deviations on the exceptions to this liability.

Given the rather strict application of product liability, producers are therefore required (nr. 8) to be made aware of the precise scope of these provisions.

5.2.2 Liability of service providers

As stated in the general introduction to sector 5.1, general liability regulation, EU provisions on liability can be found in a plethora of different legal instruments. One of such instruments is the Directive on e-commerce, which contains specific provisions dealing with the liability of service providers.

Specifically, this directive refers to the liability of intermediary service providers. The main idea behind these provisions can be found in a basic problem created by the Internet. As the Internet can be used as a means to circulate harmful or illegal information it is important to assess who can be held liable for such information. In many cases, however, it will not be an easy task to identify the user that uploaded the information. As a result, such cases are often redirected towards the service provider that

---

176 Article 15 (1) (b) Directive 85/374/EEC.
181 Articles 12 to 15 Directive 2000/31/EC.
hosted the website on which the information was posted or the internet service provider that provides
the internet access to the user suspected of uploading the harmful or illegal information. As it may lead
to undesirable effects to hold service providers liable for all acts committed by the users of their
services, the EU has created a specific framework that governs the liability of these intermediary service
providers.

The provisions in the directive on liability cover three specific situations and provide a final
general provision. First, the directive addresses the situation of mere conduit.\(^{182}\) This means that, when
a service provider only transmits the information provided by a recipient of the service, or only provides
access to a communication network, this service provider will not be held liable for that transmission.
Such is, however, subject to the conditions that the service provider
(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the
transmission.\(^{183}\)

Even if such information transmission or access provision would include automatic, intermediate
and transient storage, such storage would still be regarded as mere conduit if it is conducted for the
sole purpose of transmitting information and if the information is not stored for a longer period than
necessary for the transmission.\(^{184}\) Although service providers can under the scope of this provision not
be held liable for the nature of the information transmitted, they can be asked to terminate or to
prevent an infringement.\(^{185}\)

A second situation addressed by the directive is that of caching.\(^{186}\) In the same vein as the
provision on mere conduit, service providers are not held liable for the automatic, intermediate and
temporary storage of information, if such storage is performed for the sole purpose of making the
further transmission of said information to other requesting users more efficient. Also here, this is
subject to certain conditions, namely that the service provider
(a) does not modify the information;
(b) complies with conditions on access to the information;
(c) complies with rules regarding the updating of the information,
specified in a manner widely recognized and used by industry;
(d) does not interfere with the lawful use of technology, widely
recognized and used by industry, to obtain data on the use of the
information; and
(e) acts expeditiously to remove or to disable access to the information
it has stored upon obtaining actual knowledge of the fact that the
information at the initial source of the transmission has been
removed from the network, or access to it has been disabled, or
that a court or an administrative authority has ordered such
removal or disablement.\(^{187}\)

As under the previous article, while not held liable, service providers can be asked to terminate or to
prevent an infringement.\(^{188}\)

---

182 Article 12 Directive 2000/31/EC.
183 Article 12 (1) Directive 2000/31/EC.
184 Article 12 (2) Directive 2000/31/EC.
185 Article 12 (3) Directive 2000/31/EC.
186 Article 13 Directive 2000/31/EC.
187 Article 13 (1) Directive 2000/31/EC.
188 Article 13 (2) Directive 2000/31/EC.
The third specific situation addressed by the directive is hosting.\textsuperscript{189} If a service provider delivers the service of storing information provided by the recipient of the service, the service provider will not be held liable for the contents of such information. This is, however, subject to the conditions that the service provider

(a) does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.\textsuperscript{190}

Furthermore, the service provider may not control or exercise authority over the recipient of the service and he may still be required to remove the information or block access thereto.\textsuperscript{191}

Lastly, the directive provides that one cannot ask the service providers to monitor all information transmitted or stored by them or to actively locate illegalities therein.\textsuperscript{192} If service providers are made aware of alleged illegalities concerning the information they transmit or store, they will need to inform the appropriate authorities.\textsuperscript{193}

The EU saw such provisions necessary to ensure that no unreasonable burden was put on the intermediary service providers as they play an important role in the development of the Internet and e-commerce, particularly in cross-border transactions. The provisions of the directive relating to these liability issues were therefore almost literally transposed into national law by the Member States.\textsuperscript{194} Although the directive only addressed the three situations discussed earlier, certain Member States have even further expanded this waiver of liability to hyperlinks and search engines.\textsuperscript{195}

The issue of the liability of service providers can also be of importance to the IoT. As more devices and items become interconnected, the continuous flow of data will only increase. The growing demand for interconnection also leads to a growth in the tasks of classic intermediary service providers. As service providers of all kinds are more and more leaving their traditional field of work and expanding the scope of their services towards newer technologies, it has become difficult to assess what precisely constitutes an intermediary service provider. It will therefore be important for a service provider to establish the precise scope of its activities and to determine whether it can benefit from the specific liability exemptions offered to intermediary service providers.

An example to illustrate this is the Belgian case against Yahoo! In this case, Yahoo! was convicted for failing to comply with a provision in the Code of Criminal Procedure that requires electronic communication network operators and electronic communication service providers to disclose identification data relating to their users if so requested in the course of a criminal investigation.\textsuperscript{196}

Yahoo! argued that this provision is aimed at the operators of a physical network and the ‘classical’ providers of access to the Internet and not at tertiary service providers whose services only make use of the existing network that is operated by other parties. As Yahoo! does not operate a

\textsuperscript{189} Article 14 Directive 2000/31/EC.
\textsuperscript{190} Article 14 (1) Directive 2000/31/EC.
\textsuperscript{191} Article 14 (2) and (3) Directive 2000/31/EC.
\textsuperscript{192} Article 15 (1) Directive 2000/31/EC.
\textsuperscript{193} Article 15 (2) Directive 2000/31/EC.
\textsuperscript{195} Ibid., 13.
\textsuperscript{196} Article 46bis Belgian Code of Criminal Procedure (Wetboek van Strafordering).
physical public network infrastructure and as it does not offer its users access to the Internet – on the contrary, its users must already be able to access the Internet before they can benefit of the services offered by Yahoo! – it cannot be considered as a network operator or service provider in the sense of the Belgian Code of Criminal Procedure.

The Belgian Supreme Court, however, refuted this reasoning and states that the services offered by Yahoo! – in this case it concerned specifically the webmail service – are to be considered as services offered by service providers in the Sense of the Belgian Code of Criminal Procedure. 197 Although this case did not directly concern the liability of intermediary service providers for the contents of the information they transmit or store, such reasoning shows that the sometimes highly divergent definitions of the concept of service provider found in different legislation could have implications regarding the provisions on their liability. As IoT services are likely to often have a cross-border dimension, one will have to take in account the specific scope of the notion of service provider under legislation from various states.

Precise delineation of the tasks of a service provider is required (nr. 9) to assess which legislation can be applied to the particular situation of such service provider.

5.2.3 Contractual limitations of liability

As discussed under sector 5.1, general liability regulation, parties can avoid their contractual liabilities by calling force majeure or through hardship or exclusion clauses. As force majeure and hardship rely on circumstances beyond the parties’ control, exclusion clauses are the only means available to parties to mutually agree on limiting their liabilities in the contract itself.

One can distinguish three different types of exclusion clauses. An exclusion clause sensu strictu is designed to exonerate a party for a certain breach of contract that may occur during the course of the parties’ contractual bond. Alternatively, a party may not aim to fully exonerate himself from any liability for his potential breaches of contract, but to place a limit on his maximum liability, regardless of the actual value of damages caused by his breach. Such clause can also be referred to as a limitation clause [Taylor 2007]. Third, one can also limit the period of time in which a party can call on the adverse party’s liability.

One can also distinguish exclusion clauses by how they have been incorporated into the contract. The most obvious way to incorporate an exclusion clause in a contract is by including it in the draft terms of the contract that is later signed by all parties involved [Taylor 2007]. This relies on the basic notion that all terms included in the contract are fully read and understood before a party makes such legal commitment by signing the contract. Therefore, one can expect an exclusion clause included in the terms of a signed contract to be fully known to and understood by all signing parties.

Second, an exclusion clause can be incorporated by notice [Taylor 2007]. As not every document will be signed, the incorporation by notice allows an exclusion clause to be valid without signature if it has been reasonably brought to the attention of the parties involved. Due notice, however, is a notion that can be subject to wide interpretations. For one, an exclusion clause may be included in terms printed on the back of a receipt. If the receipt on its front refers to the fact that the conditions can be found at the back of the same receipt, one could argue that this is a reasonable notice. 198 From case law, one can deduct that it does not matter whether the adverse party is truly aware of the exclusion clause. The main component here is that the party that wishes to rely on the clause has made reasonable efforts to notify the other parties [Taylor 2007]. In judging the reasonability of the efforts of notification made, judges will rely on accompanying factors such as the timing of notice, the type of document on

197 Cass. 18 januari 2011, Nr. P.10.1347.N. Note that the case has been referred back to the Court of Appeals, which may still come to a different conclusion.
198 As argued in Parker v South Eastern Railway, [1877] 2 CPD 416.
which notice was made and whether notice of the existence of an exclusion clause was made or of its actual contents. One should also remark that the higher the degree of exoneration found in the exclusion clause, the higher the degree of reasonable notice that will have to be observed [Taylor 2007].

Last, exclusion clauses can be incorporated into a contract by means of custom set by previous courses of dealing. If certain parties have a history of dealing with each other, and if certain exclusion clauses were always incorporated in previous contracts between them, one can consider such clauses to also be incorporated in future contracts. Important here is that all parties must have a long and consistent course of dealing with each other. Similarly, certain trades may share particular customs such as incorporating certain exclusion clauses in their contracts. If in a particular contract an exclusion clause is not incorporated by signature or notice, but if the incorporation of such clause is a known custom in that particular trade, one can still consider the clause to be duly incorporated [Taylor 2007].

The possibility of the exclusion clause results from the concept of freedom of contract and consent. If parties are free to choose whether they enter a contractual bond with each other, they are also free to choose how they wish to organize the rights and responsibilities of such bond. As long as both parties consent to the contractual terms – thus if mutual consent has been established – there should be no reason to consider such contract as invalid.

The freedom of contract, however, is not an absolute freedom and can be limited in court or by State laws. This is a result of the freedom of contract being abused, for instance in labour conditions. As a result, the scope of exclusion clauses is limited as well, as an unlimited freedom of liability exclusion would lead to unbalanced situations whereby the more powerful party would exonerate itself from all liability.

Therefore, case law on this subject sees judges looking for a reasonable interpretation of exclusion clauses brought before them. If a literal interpretation of the words used in the clause would lead to unreasonable results, judges would either reject the clause or limit its application to achieve reasonable results. Similarly, exclusion clauses are traditionally interpreted contra proferentem. Other grounds of exclusion that are usually treated with particular care by judges include negligence and fraud. Although negligence could be accepted as a potential exclusion ground if the clause is properly formulated, it should be noted that there are no strict and formal rules on this. Acceptance of negligence as exclusion ground will therefore have to be judged on a case-by-case basis. This leads one to understand that fraud will not easily be accepted as a potential exclusion ground [Taylor 2007].

Also legislation may limit the scope of exclusion clauses. For one, as criminal law is part of public law, one cannot exclude its liability from criminal offenses [Dumortier 2010]. Other legislation that may limit exclusion clauses is aimed at consumer protection. As such legislation originates from the idea that consumers are often in a lesser negotiation position and therefore may be forced – often unknowingly – into accepting unbeficial contract terms, consumer protection legislation is aimed at correcting the position of the consumer in the negotiation phase and in the contractual terms.

The British Act on unfair contract terms, for instance, is aimed at limiting the use of certain terms that might compromise the legal protection of the consumer. With regards to exclusion clauses, the Act renders certain terms ineffective and subjects other terms to reasonableness [Taylor 2007]. Furthermore, the national implementation of an EU directive has lead to the adoption of a specific

199 In the early 20th century, unfavorable labour conditions violating State law were upheld if such conditions were agreed upon by contract. U.S. Supreme Court, Lochner v New York (1905), 198 U.S. 45-76.
201 This means that the clause will be construed against the party that wishes to rely on the clause. [Taylor 2007]
202 See: Canada SS Lines Ltd v The King, [1952] AC 192.
203 Unfair Contract Terms Act 1977 (c 50).
regulation on unfair terms in consumer contracts.\textsuperscript{204} \textsuperscript{205} This instrument amongst others codifies the contra proferentem rule [Taylor 2007]. As it concerns the implementation of an EU directive, all EU Member States have adopted similar legislation on the protection of consumer contracts.

As the IoT will lead to a web of interconnections of divergent devices, produced by different manufacturers, and will include divergent services, delivered by different service providers, one can imagine the need for the actors of the IoT to conclude contracts between them, in order to ensure that their relationship is covered by a legally sound document. Just like in any other field of business, one can imagine IoT actors to want to limit their contractual liabilities. In the light of the analysis performed here, one can conclude that contractual limitations of liability through exclusion clauses will need to be carefully drafted. As clear negotiations leading up to a written and signed contract will not always be possible in the ever-growing digitalization of society, providers of services relating to the IoT wishing to limit their liabilities will have to ensure that such exclusions are incorporated by notice. Here, it will be important to ensure that these notifications display sufficient reasonableness. Such reasonableness will also need to be displayed in the contents of the exclusion clause. If an exclusion clause leads to a too broad limitation of liability, it will result in an unfair and unbalanced position for one of the parties. As such unfairness would fail the test of reasonableness, judges will not uphold such clauses. Unfair contract terms may even violate legislation aimed at the protection of consumer contracts.

\textbf{Therefore, while contractual liability can be limited by exclusion clauses, they require (nr. 10) careful drafting as excessive clauses may be deemed unreasonable.}

\begin{section}{5.2.4 Liability under data protection regulations}

As was extensively discussed under sector 4, privacy policy framework, parties involved in the processing of personal data may face liability under the EU legal framework on privacy and data protection. In particular, this concerns the data controller and data processor. As these two main actors in the topic of personal data processing have divergent responsibilities, it is essential to clearly demarcate the precise roles of these two actors.

To reiterate what was discussed under sector 4.2.1, controller versus processor, the controller is the actor who ‘determines the means and purposes’ of the processing, while the processor executes ‘on behalf of the controller’. As the processor executes the processing of the personal data, he will up to certain extent be able to determine how such processing will be performed. That is, the processor can also in part determine the means. It is therefore the determination of the purposes that is exclusively reserved for the data controller.

The main provisions regarding the processing of personal data – as discussed under sector 4.1.1.2, basic principles of processing – found under article 6 of Directive 95/46/EC must be complied with in each processing of personal data. The same article states that it is the responsibility of the data controller to ensure such compliance.\textsuperscript{206} Likewise, it is the responsibility of the data controller to ensure that the rights of the data subject are respected and that they can be effectively exercised.\textsuperscript{207} Further responsibilities of the data controller include the confidentiality and security of the processing and notification to the appropriate DPA(s).

Given the importance of the role of the data controller in the processing of personal data, the EU has decided to include provisions on remedies, liability and sanctions in the directive. Regarding

\textsuperscript{205} The Unfair Terms in Consumer Contracts Regulations 1999 (SI 1999/2083).
\textsuperscript{206} Article 6 (2) Directive 95/46/EC.
\textsuperscript{207} Articles 10 to 12 and 14 Directive 95/46/EC.
remedies, the directive refers to the possibility of administrative remedies before inter alia the national DPA.\footnote{Article 22 Directive 95/46/EC.} Such national DPA could, for instance, provide the data subject with assistance in the exercise of his rights in the processing of his personal data for purposes of national security or defense.\footnote{Article 28 Directive 95/46/EC.} The national DPA could also intervene in legal proceedings against a processing that does not comply with existing legislation. Apart from intervening in legal proceedings launched by others – mainly data subjects whose rights were violated – national DPAs could also independently engage in legal proceedings when the principles of the national legal framework on data protection have been violated. The directive also provides that Member States must ensure that access to the national judicial authority is cleared for any breach of the rights guaranteed to him by national legislation applicable to the processing.

With regards to liability, the directive provides that “any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.”\footnote{Article 23 Directive 95/46/EC.}

Once more, this provision clearly points to the controller as the person liable for all damages resulting from incompliant processing. The controller may be exempted – partially or wholly – if he can provide evidence that he was not responsible for the event that gave rise to the damage. This provision bears resemblance to the general Aquilian liability and the tort of negligence.\footnote{Note that the article illustrates that three elements similar to those found in the Aquilian liability are present: “damage resulting from an unlawful processing operation” indicates the elements of damage, causality and a certain degree of fault, as the processing must be unlawful. It is, however, not the person suffering the damage that will have to prove the data controller’s wrongdoings. Contrarily, it is the data controller himself that needs to provide proof of his not being responsible for the damages suffered. This lends a certain degree of objectivity to the provision in the directive.}

Lastly, the directive provides that Member States must “lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive”.\footnote{Article 24 Directive 95/46/EC.}

Such sanctions could be rather steep. The Belgian Privacy Act, for instance, includes fines up to €100,000 and up to two years of prison sentence for repeated offences against the provisions included in the Act.\footnote{Articles 37 to 43 Belgian Privacy Act.}

As can be concluded from this overview, the data controller faces strict liabilities under the EU legal framework on privacy and data protection. When processing personal data, it will therefore be of capital importance to ensure that all principles of the applicable national data protection legislation(s) are duly complied with. For IoT actors qualified as controllers of the processing of personal data, this means that they can face the liabilities discussed here. It will therefore be of utmost importance for them to establish a clear delineation between the responsibilities of the controller and the processor of the processing under their control. They will also need to ensure compliance to the applicable national data protection legislation(s), lest they face the liabilities for incompliant or illegal processing of personal data.

\textbf{IoT actors identified as controllers of the processing of personal data under the scope of Directive 95/46/EC are therefore required (nr. 11) to precisely delineate of the tasks and responsibilities of controller and processor is required to clearly define their liabilities.}
5.2.5 Cross-border aspects

What can be deduced from this analysis of the legal framework on liability in the EU this far is that no common conception of the notion of liability can be found. The precise scope of the liability is fully dependent on the particular situation between the parties and their respective role in their legal relationship. Moreover, as legal provisions in this field at an EU level are limited to particular cases such as e-commerce, product liability and data protection, one can distinguish significant differences in the national legal frameworks on liability of the Member States.

This can lead to issues when a cross-border situation would present itself. Think for instance of an American and a Chinese company entering a contractual relationship to provide services in Belgium and in the execution of their services there cause damages to a German citizen, with whom they do not share a contractual bond. As the US, China, Belgium and Germany may have very divergent legal instruments on liability, one will have to decide which national legislation will have to be applied to this particular case. One will also have to decide which judge will be competent to rule on this case. Note that, for instance, Belgian judges can in certain cases apply the national law of a different State. Therefore, the mere application of, for instance, German law to a case does not automatically necessitate the competence of only German courts. Lastly, after a court decision has been rendered, the question of execution remains. If, for instance, a Belgian judge renders a decision that will have effect on German territory, one will have to wonder whether German judges will execute this foreign decision.\textsuperscript{214} The three problems identified here – applicable law, competent judge and execution of foreign decisions – form the scope of private international law.\textsuperscript{215}

Given the notion of freedom of contract, parties are in principle free to decide on these issues themselves. A forum selection clause and a choice of law clause could then be included in a contract with a cross-border nature to establish which law will be applied and which judge will be competent, if a dispute should arise between the parties. Such clauses could of course be abused to appoint less strict legal systems and more lenient judges. As is the case with the previously discussed exclusion clauses, forum selection clauses and choice of law clauses will have to be analyzed to prevent abuse of the freedom of contract, to preserve the position of all parties – especially consumers – and to prevent forum shopping.

When no forum or applicable law was selected by the parties, one will have to fall back on procedural directions offered by different legal instruments. In order to establish which judge has competence over a certain case, EU Member States can rely on the so-called Brussels I Regulation.\textsuperscript{216} This Regulation applies to civil and commercial matters – with exceptions listed under article 1 (2) – and establishes general rules on the competence of judges. Note that – being a regulation – these provisions apply directly to all EU Member States and do not necessitate implementation in national legal instruments. As a general rule, a citizen of an EU Member State is sued in that Member State.\textsuperscript{217} There are, however, several exceptions to this rule. If the dispute between parties concerns a contract between them, for instance, the citizen may be sued before the courts of the Member State where obligation in question is performed.\textsuperscript{218} In the case of tort, the citizen may be sued “in the place where

\textsuperscript{214} This problem occurred, for instance, in a case where American judges did recognize a French judicial decision, but did not execute it as the American court found that the decision would violate US constitutional rights. The decision was later appealed and has sparked further discussion. See for instance [Graux 2009].

\textsuperscript{215} In common law States also referred to as ‘conflict of laws’.


\textsuperscript{217} Article 2 Regulation 44/2001.

\textsuperscript{218} Namely, “in the case of the sale of goods, the place in a Member State where, under the contract, the goods were delivered or should have been delivered and in the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided.” Article 5 (1) Regulation 44/2001.
the harmful event occurred or may occur”. Specific exceptions also apply to consumer contracts and employment contracts.

The same Brussels I Regulation also provides rules on the recognition of judgments rendered in other EU Member States. Such judgments shall be recognized and enforced in all Member States.

To establish which law will be applicable to a certain situation, one will first have to assess the specific nature of the case. As can be determined from its nature, liability issues regarding the IoT will mostly concern contractual issues or the Aquilian or tortuous non-contractual liability.

For contractual matters, the Rome I Regulation specifies which legal system will apply. This regulation applies to disputes regarding civil and commercial contracts, with a few limitations. The regulation recognizes the freedom of choice, but stresses that this freedom is only relative and can be subject to limitations. For one, the regulation recognizes overriding mandatory provisions, the application of which shall not be overridden. In absence of a choice by the parties, a contract for the sale of goods shall be governed by the law of the country where the seller has his habitual residence. For a contract for the provision of services, the applicable law shall be the law of the country where the service provider has his habitual residence. The regulation further provides specific rules for contracts of carriage, consumer contracts, insurance contracts, individual employment contracts. Furthermore, the regulation provides procedural guidelines for, amongst others, the assessment of the validity of the contract and the consent thereto, subrogation and the burden of proof.

For non-contractual matters, the Rome II Regulation specifies which legal system will apply. As evidenced in recital 11 to this regulation, the EU legislator has understood that the Member States share highly divergent opinions on non-contractual obligations and liabilities and therefore decides that the concept of non-contractual obligations should – within the scope of the regulation – be understood as an autonomous concept. Consequently, damages covered by the regulation include tort and delict, unjust enrichment, negotiorum gestio and culpa in contrahendo. The regulation applies to purely civil and commercial non-contractual relationships, with a number of exclusions. Generally, the regulation refers to “the law of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occur.” However, if both the person injured and the person causing the injury live in the same Member State, the law of that

---

220 Articles 15 to 17 Regulation 44/2001.
221 Articles 18 to 21 Regulation 44/2001.
223 Articles 33 and 38 Regulation 44/2001.
225 Article 1 Regulation 593/2008.
226 Article 3 Regulation 593/2008.
227 Article 9 Regulation 593/2008.
228 Article 4 (a) Regulation 593/2008. Article 19 defines ‘habitual residence’ as the principal place of business of a natural person or the place of central administration of a legal person at the time of the conclusion of the contract.
229 Article 4 (b) Regulation 593/2008.
230 Articles 5 to 8 Regulation 593/2008.
231 Articles 10 to 18 Regulation 593/2008.
233 Recital 11 to Regulation 864/2007.
A manifest connection to a certain Member State may also indicate the law of that Member State to be applicable. Specific rules apply to product liability, unfair competition, environmental damage, infringement of intellectual property rights and industrial action. Further provisions are present for unjust enrichment, *negotiorum gestio* and *culpa in contrahendo*. As under the Rome I Regulation, the Rome II Regulation recognizes the relative freedom of choice and provides rules on the scope of applicability, mandatory overriding provisions, validity and burden of proof.

The framework set by the Brussels I, Rome I and Rome II Regulations therefore sets a coherent and harmonized pan-European legal framework for the determination of applicable law and competent judge and for the execution of foreign judgments. Its scope is, however, limited to EU Member States. For rules of international private law applicable to non-EU Member States, one could look at the work of the Hague Conference on Private International Law. This includes a convention related to the international sale of goods. Also a convention adopted within UNCITRAL provides “internationally accepted substantive rules on which contracting parties, courts, and arbitrators may rely”.

As the interconnection between the devices and objects of the IoT will certainly not be limited to a particular State, one should prepare for cross-border consequences. Be it within the framework of a contractual agreement or on a purely non-contractual basis, the rules found in private international law will provide guidance on the determination of the applicable law and competent judge, as well as with regards to the execution of a foreign court judgment. However, as even the coherent framework set by the Brussels I, Rome I and Rome II Regulations demonstrates, this may still lead to lengthy disputes. One could therefore recommend incorporating a forum selection clause and a choice of law clause in a contract, to avoid such proceedings at least within a contractual framework. As with exclusion clauses, moderation and reasonableness are imperative in the drafting of a forum selection and choice of law.

While international private law may provide guidance in cross-border disputes, producers may benefit from using forum selection and choice of law clauses. These clauses do require (nr. 12) careful drafting.

### 5.2.6 Role definition

For the precise determination of the liability of persons involved, as already explained earlier, it is of capital importance to assess what their particular role in the relationship is. As evidenced in the discussion on the notions of data controller and processor – see sector 4.2.1, controller versus processor – the precise scope of the liability is highly dependent on the role definition.

Such role definition, however, is not always clear-cut. Certain legislation may, for instance, not fully delineate the scope of its terms, leaving room for interpretation. Other legislation may contain clearly defined terms, yet may be unable to uphold these definitions as the societal background of that legislation changes drastically. A notable example of this is the EU legal framework on data protection, found in Directive 95/46/EC. Even though the concepts of this directive were clearly demarcated at the time of their conception in the early 1980’s, their application to the current digital society has become questionable.

---

239 Articles 5 to 9 Regulation 864/2007.
240 Articles 10 to 13 Regulation 864/2007.
241 Articles 14 to 22 Regulation 864/2007.
242 Convention of 15 June 1955 on the law applicable to international sales of goods.
The blurring of a clear distinction between different roles has lead to the fact that one may discern several different cases of processing of personal data within one application. This leads to the fact that several actors may be considered as the data controller, but with regards to different processing operations present in this application.

If one were to consider processing of personal data in a medical setting, one may think of a general practitioner as a data controller as he will determine the purposes of the processing he performs [Verhenneman 2008]. He can therefore be held fully liable, as he is the entity responsible for the processing. If this general practitioner would operate from within a hospital, for instance, other issues arise. Certain doctors are full employees of the hospital, while others may work on the basis of self-employment. Given the specific tasks and responsibilities of different staff members and the need for internal division thereof, it would be advised to appoint the hospital as main actor responsible. In certain cases, the hospital and medical staff members may be held liable as (joint) controllers as they both exercise a degree of authority over the determination of the purposes and means for the processing of their data.

Even though the hospital and medical staff are the main actors responsible for the processing of personal data, other actors involved may also be considered as controllers on some accounts. External security staff, for instance, that manages access to and surveillance of the premises may also process personal data when they require additional information within the context of establishing a system for access rights management [Verhenneman 2008]. External entities working for the hospital could have their role restricted to that of a processor, thus avoiding the highest degree of liability. By doing so, the external entity will, however, no longer be able to determine the purposes of the processing as such is reserved for the controller. He will still have certain authority over the determination of the means – as he executes the processing – and could thus present his services as means only [Verhenneman 2008].

The possibility of such role definition, however, will fully depend on the precise nature of the business relationship between the parties involved. If the services would be offered to the medical staff on individual basis – thus without direct contract with the hospital – the service provider would have to take up full liability as he is the sole controller of his processing. But, if the service offered is tailored to the specific order of a certain general practitioner, one may again argue that the practitioner has decided on the purposes of the processing of personal data he wishes to perform and that the service provider only provides the means by following the directions given by the practitioner. In such scenario, one could thus argue that the service provider is only a processor [Verhenneman 2008]. A contractual agreement between all entities directly involved in the processing of personal data would therefore be advised. This will be needed to fully delineate the precise roles and corresponding liabilities of each actor. With regards to medical data, this will also assist in determining which staff member can access which data.

Also third parties may receive certain personal data. An example here is technical staff as third party to the case where an individual medical staff member acts as controller, rather than the hospital. Certain national DPAs could, however, limit transfers to third parties [Verhenneman 2008].

The data subject in such medical setting will usually be the patient. As the role of the patient with regards to the processing of personal data in a medical setting is rather limited, he will in general maintain the role of data subject. Such is, however, not always true. Considering the example of social network services, one can conclude that the providers of such social network services process personal data as part of their core business model. The person whose personal data is processed, namely the

\[245\] Note that even when a service provider successfully limits its responsibility to that of a mere processor, he will still be controlling certain personal data needed for providing his services.

\[246\] Note the deliberate distinction between the internal technical staff as potential third party and the external security staff mentioned in previous paragraph as potential processor. A processor cannot be an internal staff member of the controller.
user of such social network service, is therefore the data subject. However, this very same user processes personal data as part of his using the service. He personally determines the purposes for such processing – mostly leisure and social interaction – and also shares a degree of authority in determining the means of the processing, as he can personally determine which information he shares with the social network service. By establishing the purposes of his processing and by having a degree of control on the means thereof, the user of a social network service may be considered as a controller “with regards to the content he chooses to provide and the processing operations he initiates” [Van Alsenoy 2009]. The data subject to whom specific rights are granted in one processing within an application may, in other words, become the controller responsible for the fair and lawful execution of another processing within the same application.

From these two examples, one can once more determine the need for a clear demarcation of the different roles of the actors involved in the processing of personal data. As a particular application may contain different cases of processing of personal data, one will have to clearly distinguish these different cases and allocate the parties involved their appropriate roles. Regarding role definition in the context of data protection, one can remark that the most urgent matter is the demarcation of the roles of data controller and processor. This relationship would best be fully delineated in a contract, as such is the most certain way to ensure that the precise responsibilities and liabilities of the controller and the processor are adequately determined from the start of the processing on.

A clear role division is required (nr. 13) in the assessment of the liabilities of the parties involved.

5.3 Conclusion

This sector focused on specific issues regarding the current EU legal framework on liability to the IoT. From the general analysis of liability regulations, one can understand that there is no uniform concept of liability to be found in current legislation. As a result, there is also no specific legal framework on IoT liability currently in place. Consequently, general liability provisions – spread over divergent legal instruments over EU Member States – will have to be applied to the IoT.

The notion of liability differs according to the legal instrument one analyzes. In this general analysis, there was first a distinction made between the different types of liability found in the current legal realm.

Most fundamentally, one needs to distinguish civil liability from criminal liability. Within the context of civil liability, one can distinguish the culpa in contrahendo providing liability for damages caused during the negotiation phase of a contract. Second, there is the general contractual liability which provides liability for acts – or refraining from acting – that do not correspond to the contractual provisions one agreed to. For a non-contractual setting, the Aquilian liability or the tort of negligence can provide compensation to the person suffering from unlawfully inflicted damages, on the condition that he can prove his damages, the faulty act of the adverse party and causality between the former elements. Lastly, risk liability was described as a specific type of liability that does not require a specific element of fault and attributes liability solely on the basis of risk.

Next, a number of issues regarding specific liability concerns were discussed. As there currently does not exist a specific liability framework regarding the IoT, general provisions on liability will have to be applied to the IoT. Consequently, the specific issues relating to liability analyzed here are also applicable to the IoT.

First, the general framework of product liability was analyzed. As a type of risk liability, product liability does not need to have a proven element of fault. It is therefore a type of strict liability that holds producers liable to pay compensation for death or personal injuries caused by a defect in his product. In the EU, this was implemented through a 1985 Directive that provided for rather broad definitions of the concepts of product and producer. In order to be rewarded compensation, the person
sustaining the damage needs to prove the damage, the defect and the causal relationship between defect and damage. While certain limitations to these provisions apply, such as the development risk defense, and while the directive also provides for grounds for exoneration of liability, the provisions of this directive seem to have reached their desire effect. Recent Commission reviews indicate that these principles were fairly uniformly implemented and interpreted across EU Member States. For producers of IoT-related products, this means that the rules on EU product liability will also be applicable to them. A clear understanding of these rules – and their national deviations across the Member States – will therefore be needed.

Provisions on the liability of service providers can be found in the Directive on e-commerce. This directive describes a number of situations in which intermediary service providers may find themselves. As the Internet can be used as a medium for anonymous communication of harmful or illegal information, the EU wanted to prevent that the providers of services on the Internet would be held liable for such information. The directive describes the notions of mere conduit, caching and hosting and provides that the intermediary service providers cannot be held liable for such activities. They may still be asked to end or prevent certain infringements by their users. However, there is no general duty to monitor all information transmitted or stored by them or to actively locate illegalities therein. In this respect one should also note that the concept of service provider may have a divergent scope according to different legal instruments. Different interpretations of this same notion may lead to issues regarding the application of certain legislation to particular cases. It will therefore be important to establish the precise scope of the activities of a service provider to assess under which legislation his activities may resort. As the implementation of the IoT will also lead to an increase in services using this web of interconnections, the IoT service providers will want to establish the scope of the liabilities they can face regarding their services. They will therefore need a clear understanding of the different interpretations of the concept of service provider – and the consequences thereof – across the EU Member States.

Regarding contractual liability, it was concluded that – given the freedom of contract – the liability under a contract can be reduced if all parties involved consent to it. Exclusion clauses are particularly aimed at reducing the liability of the parties, either by providing that a party will not be held liable for a particular faulty act, by limiting the maximum liability of a party or by delineating a timeframe in which liability must be invoked. They can be incorporated into the contract between parties by signature, by notice or by custom set by previous courses of dealing. While exclusion clauses may exonerate a party from some liability, they cannot be absolute. If a judge during court proceedings deems an exclusion clause to be unreasonable, he will either reject the clause or limit its application to whatever he deems reasonable. Also certain legislation is aimed at preventing the abuse of exclusion clauses. Consumer protection legislation, for instance, excludes the use of certain terms that might compromise the legal protection of the consumer. In drafting contracts relating to the IoT, one will therefore have to make specific considerations regarding potential exclusion clauses as such clauses require careful drafting. Together with the rise in producers of IoT-related products and providers of IoT-related services, one can deduce that the IoT will lead to sometimes complex relations between its different actors. These actors may therefore want to establish their relationship and responsibilities in a contract. If these contracts include exclusions clauses limiting the liability of a certain party, it will become subject to limitations to such provisions, found in legislation and imposed by judges.

After the previously discussed liability under contract law, product liability and the liability of service providers, this sector also addressed the liability of the data controller under EU data protection legislation. Here, the specific responsibilities of the data controller were analyzed. It was also analyzed which remedies are offered to the person suffering damages from incompliant data processing, as well as the sanctions against such offence.

As services offered in the framework of the IoT are not likely to be limited to one particular State, this sector also analyzed the cross-border liability of such services. As it was already assessed that
national legislation on liability issues differs greatly between States and that the notion of liability has a different scope in particular legislation, it was concluded that one would need to refer a cross-border dispute on liability to the principles of private international law. For EU Member States, the Brussels I Regulation refers parties to the judge who will be competent to decide on their dispute. The Rome I Regulation will subsequently refer that judge to the national legislation he will need to apply to their dispute if this dispute concerns contractual issues. For disputes concerning non-contractual issues, the Rome II Regulation will refer the judge to the applicable national law. The Brussels I Regulation also contains provisions on the execution of a foreign judgment. Note that under the freedom of contract, parties are in principle free to themselves select their forum and the law applicable to their dispute. Such forum selection clauses and choice of law clauses need to be carefully drafted.

Lastly, this sector stressed once more the need for a clear demarcation of the different roles of the parties involved. If in a certain application several different cases of processing of personal data can be discerned, the parties involved in this application may all play several roles. In the example of a medical setting, for instance, it was noticed that a general practitioner may be a regular employee or a data controller, depending on his specific contractual bond with the hospital in which he exercises his profession. Also non-medical staff members may be involved in the processing of personal data. External service providers, for instance, could in one case be considered as processors, yet as controllers in another case. A contractual agreement between the data controller and the processor, delineating their precise roles and tasks, would therefore be highly recommendable.

From this analysis, a set of legal requirements on liability issues relating to the IoT was deduced. These legal requirements will be summarized under sector 6, summary of legal requirements.
6. **Summary of legal requirements**

In this deliverable the general legal privacy framework that devices should comply with as a prerequisite for trust was analyzed together with the general liability framework. This analysis has first demonstrated that different notions of trust in social sciences share a certain connection found in the element of risk. One could therefore conclude that trust involves one person taking a risk to confide in another person, herewith hoping he will benefit from this trust relationship. Although conferring trust should lead to a more beneficial position, most disciplines seem to agree that one should not confer a too high degree of trust upon an uncertain relationship, as such could lead to negative outcomes like exploitation.

Such notion can partially be found in the legal concept of legitimate expectations, whereby a citizen may confide in the behavior or act of a public legal entity based on expectations raised by previous behavior or acts by that public legal entity. Also here, the element of relying on expectations raised by another party is present. Also in evidence law one can find that the legal validity of evidence is based on a sort of reliance in the ability of the established criteria to filter out evidence that is deemed untrustworthy. While one can therefore already find the basic elements of trust in the law, one has to conclude that the concept of trust in the legal sense has not been fully developed yet. One could therefore propose a more coherent legal concept of trust that could be applied to the IoT.

From the analysis of policy documents, opinions and scholarly work relating to the IoT, one can deduce that the most urgent matters relating to the realization of the IoT from a legal point of view relate to the matters of data protection and liability. These matters were therefore selected for further analysis, with specific attention to their particular underlying issues relating to the IoT.

From the analysis of the specific data protection issues relating to the IoT, one can deduce the following legal requirements:

**r1.** Parties are required to establish which national data protection legislation(s) will be applicable to their processing of personal data. The applicable provisions regarding fair and lawful processing of personal data need to be complied with. (see section 4.1.1.9, requirements)

**r2.** Prior determination of the specific tasks and responsibilities of each party is required to fully assess the roles of each party. This will enable to determine which party is controller and which party is processor, as well as to assess the scope of their roles.

**r3.** IoT actors are required to ensure that they are aware of the scope of the notions of personal data, the household exception and sensitive data under the national legislation applicable to the processing of personal data under their control. Follow-up on the review of Directive 95/46/EC is required to ensure ongoing compliance with changing data protection principles.

**r4.** The prior determination of the precise purposes and means of the processing is required to ensure compliance with the principle of proportionality.

**r5.** Carefully drafted privacy policies and consent forms – for instance in a multi-layered format – are required to ensure compliance to the requirement of consent and the right to information. Note that such privacy policies and consent forms need to be compliant with national data protection legislation.

**r6.** More transparency and data minimization is required to ensure compliance to the right of access.

**r7.** The need for transparency is also required for the use of RFID. The citizen needs to be made aware of the presence of RFID tags surrounding him and should – ideally – be enabled to control these tags.
From the analysis of the specific liability issues relating to the IoT, one can deduct the following legal requirements:

r8. Given the rather strict application of product liability, producers are required to be made aware of the precise scope of these provisions.

r9. Precise delineation of the tasks of a service provider is required to assess which legislation can be applied to the particular situation of such service provider.

r10. While contractual liability can be limited by exclusion clauses, they require careful drafting as excessive clauses may be deemed unreasonable.

r11. The precise delineation of the tasks and responsibilities of controller and processor is required to clearly define their liabilities.

r12. International private law may provide guidance in cross-border disputes, but producers may benefit from using forum selection and choice of law clauses. These clauses do require careful drafting.

r13. Once more, role definition is stressed as being required in the assessment of the liabilities of the parties involved.
7. References

7.1 Legislative Sources

Founding treaties

Regulations

Directives

European Commission

• Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009) 3200, 10p.


European Council

• Council Resolution of 19 May 1981 on a second programme of the European Economic Community for a consumer protection and information policy, OJ C 133, 3 June 1981, 1 et. seq.

European Parliament


EDPS

Council of Europe
- Convention nr. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed at Strasbourg on 28 January 1981.

**OECD**
- OECD Recommendation of the Council of 23 September 1980 concerning guidelines governing the protection of privacy and transborder flows of personal data.

**Belgium**
- Chapter II, Title IV of Book III of the Belgian Civil Code.
- Article 46bis Belgian Code of Criminal Procedure (Wetboek van Strafvordering).
- Memorandum by the Belgian Chamber of Representatives 1997-1998, doc. 1566/1, 33-34.

**France**
- Sénat France, Proposition de Loi visant à mieux garantir le droit à la vie privée à l’heure du numérique, [www.senat.fr](http://www.senat.fr), 2009-2010, nr. 93

**United States of America**
- Sherman Antitrust Act of 1890 (30 February 1890).

**United Kingdom**
- Unfair Contract Terms Act 1977 (c 50).

### 7.2 Case law

**ECJ**
- ECJ C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy & Satamedia Oy, 2008, §44.

**United Kingdom**
- Caparo Industries plc v Dickman, [1990] 2 AC 605.
- Canada SS Lines Ltd v The King, [1952] AC 192.
- Donoghue v Stevenson, [1932] UKHL 100.
- Parker v South Eastern Railway, [1877] 2 CPD 416.

**United States of America**
- U.S. Supreme Court, Lochner v New York (1905), 198 U.S. 45-76.

**Belgium**
- Cass. 18 januari 2011, Nr. P.10.1347.N.
7.3 Legal literature


