Faculty of Law

Ghent University

2015-2016

THE RIGHT TO PRIVACY IN THE DIGITAL AGE

A Facebook case study on the impact of the 2016 data protection reform

Dissertation

'Master of Laws'

by

Charlotte De Cort

(Student number: 01104180)

Supervisor: Prof. dr. Yves Haeck

Co-supervisor: Andy Van Pachtenbeke

ACKNOWLEDGMENTS

First and foremost, I would like to thank my supervisor, Professor dr. Yves Haeck, for giving me the freedom to write and develop this dissertation about a subject that sincerely interested me. I would like to thank both my supervisor and my co-supervisor, Andy Van Pachtenbeke, for their guidance throughout both Master years. They have taught me legal speaking and writing skills, which will undoubtedly be of great importance in the future.

Aside from the professional guidance, this dissertation would never have been possible without the encouragement of my incredibly supportive family. I would like to thank my mother, for her countless pep talks and extraordinary printing services, my father, for his astounding calmness in stressful times, and my brother and sister, for their continuous efforts to lift my spirits during the tougher moments. Additionally, I would like to thank my grandma for lighting an overwhelming amount of candles and my dog for his unparalleled enthusiasm when welcoming me home. Together they provided me with indispensable practical and emotional support and ensured I remained confident in my abilities.

Lastly, I would like to thank Katrien Coenen, Denitsa Kuzeva, Marlies Van Dijck, Hanne Vyncke & Niels Tack, for taking the time to help me get the last details right.

Charlotte De Cort

17 May 2016

DUTCH ABSTRACT

Vele praktijken die sociale netwerken, zoals Facebook, vandaag gebruiken, roepen bij gebruikers vragen op. Zijn deze technieken verenigbaar met de huidige regelgeving? Vele praktijken zijn op zijn minst dubieus in verhouding tot de huidige regelgeving. De praktijken komen meer en meer in opspraak. Dit wordt aangetoond via twee zaken die in deze thesis besproken worden. De hervorming van de databeschermingsregelgeving zal een impact hebben op deze praktijken. De hervorming bestaat uit twee delen: (i) een nieuwe algemene verordening gegevensbescherming en (ii) de vervanging van de Safe Harbour beslissing door het EU – VS Privacy Schild.

De nieuwe algemene verordening gegevensbescherming zou de positie van individuele internetgebruiker moeten verbeteren. Er valt geen zwart-wit antwoord te geven op de vraag of dit ook zo is. De verordening creëert nieuwe rechten zoals onder andere het befaamde 'recht op vergetelheid'. Daarnaast wordt de vereiste van toestemming verzwaard, deze zal voortaan een duidelijke, actieve handeling vereisen. De algemene verordening gegevensbescherming heeft echter ook kansen laten schieten, zo bevatte het initiële voorstel van de Commissie onder andere de vereiste van *expliciete* toestemming.

Daarnaast zal de notoire Safe Harbour beslissing vervangen worden door het nieuwe 'EU – VS Privacy Schild". Deze nieuwe beslissing is reeds zwaar bekritiseerd. De kans bestaat, dat deze onmiddellijk aangevochten wordt.

Zowel de nieuwe algemene verordening gegevensbescherming als het EU – VS Privacy Schild tonen aan dat er een tendens is naar meer databescherming. Ondervragingen tonen aan dat EU-burgers hier ook meer en meer belang aan hechten. Aangezien Facebook belangrijk geworden is in het dagelijkse leven van vele mensen, hebben hun praktijken een enorme impact. De hervorming van de databeschermingsregelgeving zal een impact hebben op deze praktijken in de zin dat de regels op bepaalde vlakken nog strenger worden. Aangezien vele praktijken reeds dubieus zijn onder de huidige regelgeving, bestaat de kans dat de praktijken ook in de toekomst gewoon behouden zullen blijven. De verandering die waarschijnlijk de grootste impact zal hebben op de praktijk van ondernemingen zoals Facebook, is de invoering van hoge administratieve boetes. Die boetes kunnen opgelegd worden door nationale toezichthoudende autoriteiten. Die toezichthoudende autoriteiten zullen voortaan bovendien, bevoegd zijn voor de beoordeling van bedrijven die hun activiteiten op de EU richten ongeacht of ze gevestigd zijn binnen of buiten de EU.

CONTENTS

Chapter I. Introduction

"Privacy is dead and social media hold the smoking gun."

- PETE CASHMORE[1]

Along with the digital age, new challenges for our legal systems have occurred. Legal scholars all over the world are struggling to find answers to regulate the abundance of new technologies. One of the most challenging human rights to reconcile with this evolution is the right to privacy. Over the past years, new online social networks, such as Facebook, have emerged. While they have offered our society a whole new way of communicating, they have also posed challenges to the fundamental right to privacy.

Since its start in 2004, Facebook has become the largest online social network.[2] In 2015, it recorded over 1.5 billion users. When Facebook amended its Terms of Service[3] in 2015, a lot of people were worried about the impact on their privacy. Though the update did create some new concerns, most of Facebook's worrisome practices already existed prior to this update. It seems that along with technological advancements, people are becoming more willing to offer up a part of their right to privacy. As long as the benefits outweigh the costs, practices, such as location tracking, licensing users' photos, might be accepted by a part of the population. These practices, among others, will be discussed in this dissertation. This paper will pose the question if these – sometimes questionable – practices will still be lawful after the data protection reform of 2016, or if this reform will not bring about a significant change.

Chapter II will shortly describe the history of the right to privacy and give an indication of the background of the current legislation and why a reform was long overdue.

Chapter III will continue with the discussion of the data protection reform that took place in 2016. Firstly, the new General Data Protection Regulation, and the key differences with the old Data Protection Directive, will be discussed. Secondly, Chapter II will look at the the transition from the Safe Harbour agreement to the EU – US Privacy Shield following the

---

[1] Pete Cashmore is the CEO and founder of the popular blog Mashable, a Technorati Top 10 blog worldwide; See also http://mashable.com/people/petecashmore/.

[2] Facebook Newsroom. (n.d.). *Company Info*. [online] Available at: http://newsroom.fb.com/company-info/ [Accessed 5 May 2016].

[3] Facebook. (2016). *Terms of Service*. [online] Available at: https://www.facebook.com/terms [Accessed 5 May 2016]. Hereinafter: Terms of Service.

Schrems case. The most important question that will be posed in Chapter III is if this reform will impact internet users' right to privacy.

In **Chapter IV**, Facebook's different user agreements[4] and its ongoing practices, such as the abovementioned location tracking and licensing of users' photos, will be discussed. Other practices that will be discussed are (i) the way consent is given, (ii) the tracking of browsing activity and (iii) the advertisement practices. This chapter will assess these practices in light of the current legislation and the data protection reform.

In Chapters V and VI two legal cases brought against Facebook will be discussed. In **Chapter V**, the challenge posed by the Belgian Privacy Commission will be examined.[5] The Belgian Privacy Commission challenged the practice particularly of tracking browsing activity of non-Facebook users before the Belgian courts. In **Chapter VI**, a second challenge, from the Austrian citizen Maximilian Schrems, will be discussed. The case of *Max Schrems v. Data Protection Commissioner*[6] before the CJEU will be examined as it questioned the legitimacy of data transfers from the EU to the US. This case is particularly interesting since it had implications on the Safe Harbour Agreement between the US and the EU and consequently was the cause of the new EU – US Privacy Shield Agreement. Both cases will be examined with the same approach: (i) the facts, (ii) the claims of the applicants, (iii) the ruling, (iv) what effect did the ruling have, and lastly, (v) were the concerns, as expressed by the applicants in these cases, addressed by the 2016 data protection reform?

By **Chapter VII**, a final assessment will be made of the impact of the 2016 data protection reform on Facebook's practices.

By the end of this dissertation, as a reader, you will have a better idea of how Facebook operates, how its practices can conflict with privacy laws and whether or not the data protection reform will eliminate some of these existing conflicts.

---

[4] The Terms of Service, the Data Policy, and – to a lesser extent – the cookie policy; Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016]; Facebook. (n.d.). *Cookies, Pixels & Similar Technologies*. [online] Available at: https://www.facebook.com/help/cookies/update [Accessed 5 May 2016].

[5] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015).*

[6] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU).

Chapter II. History of the right to privacy

"Bene vixit, bene qui latuit."[7]

- OVID[8]

In 1879, Thomas Cooley, an American judge, described the right to privacy quite simply as "*the right to be let alone*".[9] The right to privacy, however, can be traced as far back as the fourteenth century. One of the earliest national laws on privacy, the Justices of the Peace Act in England for the arrest of peeping toms and eavesdroppers, dates back to 1361. In the following years, many other countries, such as Sweden and France, followed suit by introducing privacy laws.[10]

The right to privacy soon graduated to an international level. The international right to privacy, as it is known today, was first enacted in Article 12 of the Universal Declaration of Human Rights[11] of 1948, which states:

> *"No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks."*

Aside from the UDHR, the right to privacy is also featured in the International Covenant on Civil and Political Rights[12], the UN Convention on Migrant Workers[13] and the UN Convention on Protection of the Child[14]. The right to privacy, as inscribed in the UDHR, cannot be invoked by citizens directly. On a regional level, however, the right to privacy soon became enforceable.

---

[7] *"To live well is to live concealed."*
[8] Publius Ovidius Naso, known as Ovid in the English-speaking world, was a Roman poet who lived during the reign of Augustus.
[9] Warren, S. and Brandeis, L. (1980). The Right to Privacy. *Harvard Law Review*, IV(5).
[10] *The Rachel Affaire [1858] D.P. III 62 (Tribunal civil de la Seine)*; See also Hauch, J. (1994). Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris. *Tulane Law Review*, 68(1219).
[11] Hereinafter: UDHR.
[12] Art. 17 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, *UN Doc.* A/6316 (1966).
[13] Art. 14 UN General Assembly, *International Convention on the Protection of the Rights of all Migrant Workers and Members of Their Families*, 18 December 1990, *UN Doc.* A/RES/45/158 (1990).
[14] Art. 16 UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, *UN Doc.* A/RES/44/25 (1989).

The European Convention on Human Rights[15] was adopted in 1950 and entered into force in 1953. Article 8 ECHR, titled the "right to respect for private and family life", states the following:

> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The first paragraph of Article 8 ECHR contains the right to privacy in principle, while the second paragraph describes the conditions for interference with the right. The bases for interference with the right to privacy are therefore limited to (i) national security, (ii) public safety, (iii) the economic wellbeing of the country, (iv) prevention of disorder or crime, (v) the protection of health and morals and (vi) the protection of the rights and freedoms of others.

Every member of the Council of Europe has incorporated or given effect to the ECHR within their national laws, which requires them to act in accordance with the provisions of the ECHR.[16] To enforce the human rights enshrined in the ECHR two institutions were created to oversee enforcement, namely the European Commission of Human Rights[17] and the European Court of Human Rights. Both institutions have been active in the enforcement of Article 8 ECHR. The importance of the right to privacy is stressed as the protection offered by Article 8 ECHR is interpreted expansively and vice versa the restrictions are interpreted narrowly.[18]

Aside from the Council of Europe, the European Union also guarantees the right to privacy. Although the founding treaties of the EU did not contain human rights, the Charter

---

[15] Hereinafter: ECHR.
[16] European Union Agency for Fundamental Rights, (2014). *Handbook Data Protection*. p.14.
[17] The European Commission of Human rights was abolished by protocol 11 in 1988.
[18] Strossen, N. (1990). Recent US and International Judicial Protection of Individual Rights: A comparative Legal Process Analysis and Proposed Synthesis. *Hastings Law Journal*, 41, p.805.

for Fundamental Rights of the European Union[19] was enacted in 2000. Initially, the Charter was exclusively a political document. It became legally binding and a part of EU primary law through the Lisbon Treaty[20] in 2009. The EU is generally competent to pass legislation on data protection matters based on Article 16 of the Treaty on the Functioning of the European Union[21] and used this competence to include Article 7 on the respect for private and family life and Article 8 on the right to data protection in the Charter.[22]

As the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[23] predates Article 8 of the Charter, Article 8 of the Charter can be seen as an embodiment of established EU data protection legislation. Legislators were therefore not only able to explicitly mention data protection as a right, but also to refer to key data protection principles. These principles, such as consent as a basis for data processing and the right of access and rectification, were incorporated in Article 8 (2) of the Charter. Lastly, Article 8 (3) of the Charter confirms the existence of independent authorities to implement the principles mentioned in Article 8 (2) of the Charter.[24]

Until 2018, the Data Protection Directive will remain the most important EU legislative instrument on data protection. At the time of its adoption, several member states already had their own set of national data protection laws. In 1995, the establishment of the Data Protection Directive was crucial, however, to facilitate the newly established internal market by providing a high level of data protection.[25] The aim of the Data Protection Directive was the maximum harmonisation[26] of the data protection laws at the national

[19] Charter of Fundamental Rights of the European Union, *O.J.* C-326, 26 October 2012, pp.391–407. Hereinafter: the Charter.
[20] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, *O.J.* C 306, 17 December 2007, pp.1–271.
[21] Consolidated version of the Treaty on the Functioning of the European Union, *O.J.* C-326, 26 October 2012, pp.47–390. Hereinafter: TFEU.
[22] European Union Agency for Fundamental Rights, (2014). *Handbook Data Protection*. p.20.
[23] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L-281, 23 November 1995, pp.31–50. Hereinafter: Data Protection Directive.
[24] European Union Agency for Fundamental Rights, (2014). *Handbook Data Protection*. p.20.
[25] Recital (3) – (5) Data Protection Directive.
[26] Recital 1, 4, 7 and 8 Data Protection Directive.

level.[27] Therefore, member states have to ensure the national data protection rules fall within the framework set by the Data Protection Directive.[28]

The Data Protection Directive's territorial scope comprises the 28 EU member states, as well as the non-EU members that are a part of the European Economic Area, namely: Iceland, Liechtenstein and Norway.[29]

As a result of the changing digital landscape, the European Commission proposed a complete reform of the data protection legislation in 2012, stating it needed to be modernized in light of rapid technological developments and globalisation.[30] The reform package consisted of a proposal for a General Data Protection Regulation[31], to replace the Data Protection Directive, and a new directive[32], specifically aimed at regulating data protection in police and judicial cooperation in criminal matters.[33]

In the meantime, several judicial cases also started exposing weak spots in de Data Protection Directive. Whether or not these will be rectified by the new General Data Protection Regulation[34] remains to be seen. In the next chapter, we will discuss the differences between the Data Protection Directive and the GDPR.

---

[27] Joined cases *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* and *Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado* [2011]C-468/10 and C-469/10 (CJEU), §28-29.
[28] European Union Agency for Fundamental Rights, (2014). *Handbook Data Protection*. p.17.
[29] European Union Agency for Fundamental Rights, (2014). *Handbook Data Protection*. p.18.
[30] European Union Agency for Fundamental Rights, (2014). *Handbook Data Protection*. p.21.
[31] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM 2012/0011 (COD).
[32] European Commission, Proposal for a Directive on the protection of individuals with regards to processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25 January 2012, COM 2012/0010 (COD).
[33] European Commission, (2012). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*. [online] Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en [Accessed 9 May 2016].
[34] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* L-119, 4 May 2016, pp. 1-88. Hereinafter: GDPR.

Chapter III. Data Protection Reform

1. From the Data Protection Directive to the General Data Protection Regulation

> *"Individuals must be empowered: they must know what their rights are, and know how to defend their rights if they feel they are not respected. Our work in creating first-rate data protection rules providing for the world's highest standard of protection is complete."*[35]

1.1. Reform process

The current Data Protection Directive dates back to 1995, a time when less than 1% of the world's population had access to internet. By 2015 around 40% of the global population had access to internet, in the developed world this number even increases to 80%.[36] Needless to say, the Data Protection Directive had become outdated and was in desperate need for an update when the European Commission proposed a reform in 2012.

On 25 January 2012, the European Commission proposed a comprehensive reform of the EU's data protection rules.[37] The European Commission expressed two main goals: firstly, to increase users' control of their data, and secondly, to cut costs for businesses by creating a 'Digital Single Market'. The proposed reform contained two legislative proposals: a regulation as a general framework for data protection[38] and a directive specifically aimed towards data processed for the purposes of prevention, detection, investigation or

---

[35] Joint Statement European Commission First Vice-President Frans Timmermans, Vice-President in charge of the Digital Single Market Andrus Ansip, and Commissioner for Justice, Consumers and Gender Equality, Věra Jourová on the final adoption of the new EU rules for personal data protection. European Commission, (2016). *Joint Statement on the final adoption of the new EU rules for personal data protection*. [online] Available at: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm [Accessed 15 May 2016].

[36] Data available at: International Telecommunication Union (ITU). (2015). *Statistics - Global ICT Developments*. [online] Available at: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx [Accessed 14 May 2016].

[37] European Commission, (2012). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*. [online] Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en [Accessed 4 May 2016].

[38] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM 2012/0011 (COD).

prosecution of criminal offenses and related judicial activities[39]. The latter will not be discussed in this dissertation.

After a legislative process of more than four years, an agreement was reached through trilogue negotiations between the European Parliament, the European Commission and the Council.[40] The final version of the GDPR[41] was published in the Official Journal on 4 May 2016. It enters into force on 24 May 2016, but will only be applicable on 25 May 2018. Until then the Data Protection Directive will remain applicable. The new rules are promised to address the concerns expressed by European citizens[42] by strengthening existing rights and empowering individuals with more control over their personal data.

In what follows the most relevant measures from the new GDPR will be discussed in comparison to the Data Protection Directive.

1.2. Evolution to a regulation

The Data Protection Directive, as a directive, was never directly applicable in the member states. Each state had to individually implement the directive into its national laws.[43] Directives set goals to be achieved by a certain date, but allow for the member states to determine in what way they will reach these goals. This resulted in different, fragmented approaches to data protection across the EU. This situation is detrimental for both businesses, as they face conflicting requirements, and consumers, as they are not protected equally across the EU.

As an example we will look at and compare the enforcement of data protection laws in Germany, France and the United Kingdom.[44]

---

[39] European Commission, Proposal for a Directive on the protection of individuals with regards to processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25 January 2012, COM 2012/0010 (COD).
[40] European Commission, (2015). *Agreement on Commission's EU data protection reform will boost Digital Single Market*. [online] Available at: http://europa.eu/rapid/press-release_IP-15-6321_en.htm [Accessed 4 May 2016].
[41] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* L-119, 4 May 2016, pp. 1-88.
[42] European Commission, (2015). *Special Eurobarometer 431 "Data protection"*. [online] European Union, p.115. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf [Accessed 14 May 2016].
[43] Art. 288 TFEU.
[44] DLA Piper, (2016). *Data Protection Law of the World*. pp.137-149, 482-487.

In Germany, the violation of data protection laws is an administrative offence subject to pecuniary fines of up to 300 000 EUR per violation. A violation is considered to be a criminal offence, when the behaviour is wilful or in exchange for financial benefits. For a criminal offence the punishment can be a fine or imprisonment for up to two years. Additionally, German authorities can skim profits that resulted from the violation.[45] In practice, German data protection authorities were reluctant to enforce these rules. Very few official prosecution procedures were opened and the fines that were imposed were low. Recently, there has been a tendency to enforce data protection rules more strictly after amendments to the law were made in 2009, following several scandals[46] revealing the disclosure or misuse of personal data and.[47]

The French data protection authority, called the 'Commission Nationale de l'Informatique et des Libertés'[48], was given a wide range of investigative powers. The CNIL can verify all data processing and request any document it deems necessary to do so effectively.[49] Additionally, the CNIL is authorized to perform online inspections and issue compliance orders when a violation is found.[50] The CNIL is not even obliged to inform the company under investigation, until the investigation has been conducted.[51] If, after a notice or compliance order, the company does not comply with the data protection rules, the CNIL can pronounce a fine of up to 150 000 EUR for the first offense. For a second offense, within the following 5 years, the CNIL can order a fine of

---

[45] Art. 43 Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (*BGBl*. I S. 2954), neugefasst durch Bekanntmachung vom 14. Ja- nuar 2003 (*BGBl*. I S. 66), zuletzt geändert durch Gesetz vom 29.07.2009 (*BGBl*. I, S. 2254), durch Artikel 5 des Gesetzes vom 29.07.2009 (*BGBl*. I, S. 2355 [2384] und durch Gesetz vom 14.08.2009 (*BGBl*. I, S. 2814). (German Federal Data Protection Act).

[46] Ernst & Young, (2009). *Privacy and Data Protection Law: European Developments*; For example, in 2006 German telecom company lost personal data, such as addresses, cell phone numbers, and email addresses, of about millions of customers. Perez, M. (2008). T-Mobile Lost 17 Million Subscribers' Personal Data. *InformationWeek*. [online] Available at: http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210700232 [Accessed 4 May 2016].

[47] Paez, M. (2009). *Germany Strengthens Data Protection Act, Introduces Data Breach Notification Requirement*. [online] Jones Day. Available at: http://www.jonesday.com/germany-strengthens-data-protection-act-introduces-data-breach-notification-requirement-10-26-2009/#_edn15 [Accessed 4 May 2016].

[48] Hereinafter: CNIL.

[49] Art. 11, §2, (f) and art. 40, III Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *Journal officiel* du 7 janvier 1978 et rectificatif au *J.O.* du 25 janvier 1978.

[50] Art. 40, III, §4 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *Journal officiel* du 7 janvier 1978 et rectificatif au *J.O.* du 25 janvier 1978.

[51] DLA Piper, (2016). *Data Protection Law of the World*. pp.137-149.

up to 300 000 EUR and/or order the company to immediately cease all data processing.[52]

Lastly, in the United Kingdom, a violation of data protection rules is considered to be a criminal offense punishable with a fine of up to 5,000 GBP[53]. The British data protection authority, called the Information Commissioner's office[54], can also impose fines of up to 500,000 GBP for serious violations.[55] Serious violations are defined as "*serious and likely to cause substantial damage or distress and either the contravention was deliberate, or the data controller knew or ought to have known that there was a risk that the breach would occur and would be likely to cause substantial damage or distress, but failed to take reasonable steps to prevent the breach*."[56]

This comparison demonstrates that despite the maximum harmonisation of the Data Protection Directive, EU member states still have a lot of leeway when implementing the Data Protection Directive, which results in sometimes vastly different rules depending on the country you are in.

As the GDPR is a regulation as opposed to a directive, it will be directly applicable in every member state, meaning the rules will become a part of the national legal system and increase the harmonization of data protection rules in the EU. Although member states may need to modify national laws in order to comply with the GDPR or adopt additional legislation to give the GDPR full effect, this does not change the fact that the GDPR, as a regulation, in itself has legal effect in the member states regardless of any national law.[57] In principle, the data protection laws in every member state will be the same.[58] In a couple of limited exceptions, such as processing data in the employment context[59], national ID

[52] Art. 45 and 47 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *Journal officiel* du 7 janvier 1978 et rectificatif au *J.O.* du 25 janvier 1978.
[53] Provision 60 Data Protection Act 1998. 5,000 GBP is the maximum fine for level 5 violations that can be imposed by a UK Magistrates' Court.
[54] Hereinafter: ICO.
[55] ICO, (2015). *Information Commissioner's guidance about the issue of monetary penalties prepared and issued under Section 55C (1) of the Data Protection Act 1998*. pp.6-8.
[56] Provision 55A Data Protection Act 1998.
[57] Craig, P. and De Búrca, G. (1998). *EU law*. Oxford: Oxford University Press, p.105.
[58] Art. 288 TFEU.
[59] Recital 155 GDPR; Art. 88 GDPR.

numbers[60], and professional secrecy obligations[61] member states will still be able to adopt specific legislation.[62]

Barring these exceptions, this new regulation will ensure a consistent approach across member states. This does not mean every single detail will be applied in a uniform way. Different courts of law in different member states may apply and interpret the GDPR differently. The European Court of Justice[63] will, however, be able to play a unifying role through preliminary questions[64] and the appeals procedure[65]. Through preliminary questions national courts can ask questions regarding interpretation and via the appeals procedure, the CJEU will be able to judge if member states are fulfilling their obligations under the GDPR.

1.3. Definitions

Many of the core definitions under the Data Protection Directive, such as controller and processor, will remain unchanged. The GDPR, however, has also expanded the scope of some definitions, such as personal data and sensitive personal data, and restricted the scope of others such as consent. In addition, new definitions, such as a definition for profiling have been added. In what follows, we will discuss these changes.

1.3.1. A broader definition of 'personal data'

Under the Data Protection Directive, personal data was 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"*[66]. There was a lot of debate on whether or not online identifiers, such as an IP address, fall within this definition of personal data.[67] The answer to this

[60] Art. 87 GDPR.
[61] Art. 90 GDPR.
[62] Paez, M., von Diemar, U., Little, J., Robertson, E., Bru, P., Haas, O. and De Muyter, L. (2015). *Agreement Reached on the European Reform of Data Protection*. [online] Jones Day. Available at: http://www.jonesday.com/agreement-reached-on-the-european-reform-of-data-protection-12-17-2015/ [Accessed 4 May 2016].
[63] Hereinafter: CJEU.
[64] Art. 267 TFEU.
[65] Art. 265 and 268 TFEU.
[66] Art. 2 (a) Data Protection Directive.
[67] Lee, P. (2015). *Getting to know the GDPR, Part 1 - You may be processing more personal information than you think*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-1-you-may-be-processing-more-personal-information-than-you-think [Accessed 4 May 2016].

question is especially important for online companies such as Facebook who store data per IP address.[68]

Like the Data Protection Directive, the GDPR's scope is limited to the protection of personal data. The GDPR defines personal data as: *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*[69] The GDPR settles the previously mentioned debate by explicitly stating online identifiers fall within the definition of personal data. Online businesses, especially those in the social media business will be impacted by this change,[70] even more so considering the extraterritorial scope as will be discussed in Section 1.4.3 of this chapter on the extra-territorial character of the GDPR.

Under the Data Protection Directive, companies often tried to escape the scope of the Data Protection Directive by anonymising the personal data they collected. The Article 29 Working Party tried to make a recommendation on how this was possible in practice while still complying with the Data Protection Directive. They came to the conclusion, however, that it is virtually impossible to anonymise personal data.[71]

The GDPR has created a new concept, called "pseudonymisation", aimed at regulating this existing practice of anonymisation. Pseudonymisation is: *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."*[72] Personal data that has undergone the process of pseudonymisation, but can still be attributed to a natural person through the use of additional information, should still be considered as information on an identifiable person.[73]

---

[68] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[69] Art. 4 (1) GDPR.
[70] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[71] Article 29 Working Party, (2014). *Opinion 05/2014 on Anonymisation Techniques*. p.23.
[72] Art. 4 (5) GDPR.
[73] Recital 26 GDPR.

Although this pseudonymised data will still be considered as personal data when it falls within the definition of Article 4 (1) GDPR, individuals' rights will be restricted through exceptions to certain provisions within the GDPR when their data has been pseudonymised. Firstly, there is an exception to the data breach notification requirements as the risk of pseudonymised data causing harm is significantly lower.[74] Secondly, there will be an exemption from the need to comply with data subjects' right of access, right to correct and erase data along with data portability requests.[75] Lastly, companies will have a greater flexibility to conduct data profiling[76] without the data subject's consent as the processing of pseudonymised data is unlikely to significantly affect a data subject as required by Article 22 (1) GDPR and explained in Recital 71 GDPR.

Article 25 GDPR emphasises the importance of pseudonymisation by mentioning it as an appropriate technique for data controllers to implement the data protection principles from the GDPR in an effective way. This requirement is repeated in Article 32 GDPR, for both the controller and the processer of personal data, to ensure the secure processing of personal data.[77] These articles, combined with incentives through relaxed obligations, emphasise the importance of pseudonymisation and will reward companies who use the technique effectively.

While these rules do reduce the risk of data leeks for consumers, they will also result in exceptions to rights consumers previously had without exception[78]. The technique of pseudonymisation will grant exceptions to data subjects' right of access[79], right to rectification[80], right to erasure (right to be forgotten)[81], right to restriction of processing[82] and right to data portability[83].

[74] Art. 34 (1) and (3) GDPR.
[75] Art. 11 (2) GDPR.
[76] Art. 22 GDPR.
[77] Art. 32 (1) (a) GDPR.
[78] Art. 12 Data Protection Directive.
[79] Art. 15 GDPR.
[80] Art. 16 GDPR.
[81] Art. 17 GDPR.
[82] Art. 18 GDPR.
[83] Art. 20 GDPR.

1.3.2. Safeguards for sensitive personal data and vulnerable groups

1.3.2.1 A broader definition of 'sensitive personal data'

Articles 9 and 10 GDPR provide additional protection for 'sensitive personal data'. Large scale processing of sensitive personal data will additionally require controllers to perform a data protection impact assessment to identify any and all potential risks involved with the processing of this data.[84]

Article 9 (1) GDPR prohibits the processing of, firstly, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, and secondly, genetic data and biometric data in order to uniquely identify a person or data concerning health or sex life and sexual orientation. The protection of genetic and biometric data is new compared to the Data Protection Directive. Article 9 (2) GDPR contains exceptions to this principle, such as explicit consent, reasons of substantial public interest and public health. Member states will be able to install additional safeguards for the processing of genetic data, biometric data or health data.

Article 10 GDPR specifies the conditions for the processing of data relating to criminal convictions and offenses.

1.3.2.2 Newly introduced concept of 'vulnerable groups'

Contrary to the Data Protection Directive, the GDPR also includes additional protection for vulnerable groups such as children. The underlying reason to protect children is explained in Recital 38 GDPR by affirming the fact that children may be less aware of the risks they face. This additional protection is implemented in the following ways:

- The principle of transparency demands clear and plain language when communicating information to a child;[85]
- To process data of children under the age of sixteen, parental consent is required. Member states will be able to lower this age to thirteen years old.[86]

---

[84] Art. 35 (3) (b) GDPR; See also Lee, P. (2015). *Getting to know the GDPR, Part 1 - You may be processing more personal information than you think*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-1-you-may-be-processing-more-personal-information-than-you-think [Accessed 4 May 2016].
[85] Recital 58 GDPR.
[86] Art. 8 (1) GDPR

Setting of the age limit at sixteen years has already caused criticism in some member states such as Belgium. In Belgium, the Flemish Office of the Children's Rights Commissioner stated this limitation is out of touch with reality, as a majority of children already use Facebook at the age of fourteen. Additionally, the Flemish Office of the Children's Rights Commissioner believes the protection of children through education and privacy awareness campaigns is more effective. Flemish Office of the Children's Rights Commissioner has requested the Belgian Privacy Commission to lower the age limit in Belgium to thirteen.

1.3.3. A stricter definition of 'consent'

The GDPR's stricter requirements for consent have been the subject of a lot of discussion. "Consent" is one of the most frequently used grounds to justify the processing of personal data.[87] This will probably continue under the GDPR. The reform can therefore have implications on the practice of a lot of companies.[88]

Under the current Data Protection Directive, consent to processing needs to be given unambiguously by the data subject. Even though this is a strict requirement, it still allows for consent[89] to be implied. Only in specific cases, such as the processing of sensitive personal data, explicit consent is required.[90]

Recital 31 of the GDPR states that consent must be freely given, specific, informed, and unambiguous. In the initial proposal the European Commission proposed to establish explicit consent as a new higher standard in the GDPR.[91] This was supported by the European Parliament.[92] The Council, however, preferred to maintain the standard of unambiguous consent, as was required under the Data Protection Directive, even though

---

[87] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[88] Dunphy-Moriel, M. and Power, L. (2015). *Getting to know the General Data Protection Regulation, Part 3 – If you receive personal data from a third party, you may need to "re-think" your legal justification for processing it.* [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-general-data-protection-regulation-part-3-if-you-receive-personal-data-from-a-third-party-you-may-need-to-re-think-your-legal-justification-for-processing-it [Accessed 4 May 2016].
[89] Art. 7 Data Protection Directive.
[90] Art. 8 (2) (a) Data Protection Directive.
[91] Recital 25 European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM 2012/0011 (COD).
[92] European Parliament, Legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Ordinary legislative procedure: first reading, 12 March 2014, C7-0025/2012 – COM 2012/0011(COD).

this offers a lower grade of protection to data subjects.[93] The final version of the GDPR, resulting from the trilogue negotiations, contains a middle ground between these opposite positions. The GDPR, like the Data Protection Directive, requires unambiguous consent, but consent will also require an affirmative action. Recital 31 further explains this through some examples: *"ticking a box when visiting an Internet website, choosing technical settings for information society services or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data".* Consequently, silence, pre-ticked boxes or inactivity cannot constitute consent under the GDPR.

A practice that immediately comes to mind when discussing the issue of online consent, is the use of cookies. Under the Data Protection Directive, it sufficed that people implicitly consented to the use of cookies, for example, by not actively objecting to it. Under the GDPR, this will no longer be possible. Every user or visitor of a website will need to provide unambiguous consent through an affirmative action. The notice of the use of cookies will need to become even more prominent.

Aside from the new definition of consent, the GDPR will have three additional consent-related requirements compared to the Data Protection Directive.

Firstly, data subjects will now have the right to withdraw their consent at any time.[94] The withdrawal of consent must be as easy as the giving of consent. Before data subjects give their consent, the data controller must inform them of the right to withdraw consent. When data subjects withdraw their consent, they have the right to have their data erased and no longer processed.

Secondly, if there is a clear imbalance between the data subject and the controller, it will be assumed consent was not given freely.[95] The recital specifies this will be applicable, in particular, when the data controller is a public authority.

Lastly, consent must be specifically obtained for each data processing act. This means a request for consent must be clearly distinguishable from other matters in a

[93] European Council, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 15 June 2015, COM 2012/0011 (COD).
[94] Art. 7 (3) GDPR.
[95] Recital 43 GDPR.

written document. Additionally, the request for consent must be presented through an intelligible and easily accessible form, using clear and plain language.[96]

Like the Data Protection Directive[97], the GDPR will require explicit consent for sensitive personal data[98], keeping in mind the concept of sensitive personal data is broader under the GDPR, as it also includes genetic and biometric data[99]. Under the GDPR, the data controller will be required to obtain explicit consent in two additional situations[100]: (i) when making a decision about the data subject based solely on automated processing, including profiling[101], and (ii) when transferring personal data to a country that does not offer an adequate level of protection.[102]

1.3.4. Newly introduced definition for 'profiling'

The current Data Protection Directive does not contain any definition of 'profiling'. It only refers, without defining, to 'automated individual decisions' and never mentions the term 'profiling' explicitly. The GDPR defines profiling as follows:

> *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;"*[103]

This definition contains three main elements: (i) any form of automated processing, (ii) concerning personal data and (iii) with the purpose of evaluating personal aspects.

The rules set by the Data Protection Directive gave every person the right not to be subjected "*to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data"*[104]*.* The Data Protection

---

[96] Art. 7 (2) GDPR.
[97] Art. 8 (2) (a) Data Protection Directive.
[98] Art. 9 (2) (a) GDPR.
[99] Art. 9 (1) GDPR.
[100] Maldoff, G. (2016). *Top 10 operational impacts of the GDPR: Part 3 – consent*. [online] The International Association of Privacy Professionals. Available at: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/ [Accessed 4 May 2016].
[101] Art. 22 (2) (c) GDPR.
[102] Art. 49 (1) (a) GDPR.
[103] Art. 4 (4) GDPR. Editing by author.
[104] Art. 15 Data Protection Directive.

Directive provided an exception for cases where (i) this automated processing was performed in the course of entering into or performance of a contract, or (ii) the automated processing was authorized by law.[105]

The GDPR's rules regarding profiling can be found in Article 22 GDPR and are quite similar to the rules in the Data Protection Directive. Article 22 (1) GDPR states that *"the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."*[106] Article 22 (2) GDPR continues with the exceptions to this rule, including the same two exceptions from the Data Protection Directive, and adding a third exception for cases where the data subject has given explicit consent.

When the use of profiling is justified by a contractual relationship or explicit consent, the GDPR requires the data controller to *"implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests"*[107]. These measures must at least guarantee the possibility of a human intervention, the right for data subjects to express their point of view, obtain further information about the decision based on the automated processing, and the right to contest this decision.[108]

In addition to these safeguarding measures, data controllers have an obligation to notify data subjects about (i) the existence of automated decision making, including profiling, (ii) the logic involved and (iii) the significance and the envisaged consequences for the data subject.[109] This information is also included in data subjects' right of access.[110]

With regards to sensitive personal data, profiling is explicitly prohibited by the GDPR, with the exception of cases where the data subject provided explicit consent or cases where profiling is necessary for reasons of public interest.[111] Data subjects cannot consent to

---

[105] Art. 15 (2) (b) Data Protection Directive.
See also Proust, O. (2015). *Getting to know the GDPR, Part 5: Your big data analytics and profiling activities may be seriously curtailed*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-5-your-big-data-analytics-and-profiling-activities-may-be-seriously-curtailed [Accessed 4 May 2016].
[106] Art. 22(1) GDPR.
[107] Art. 22 (3) GDPR.
[108] Art. 22 (3) GDPR.
[109] Art. 13 (2) (f) GDPR; Art. 14 (2) (g) GDPR.
[110] Art. 15 (1) (h) GDPR.
[111] Art. 22 (4) j° Art. 9(1) and 9(2) (a) & (g) GDPR.

profiling, implicitly or explicitly, when there is a law stating that the prohibition cannot be lifted by consent.[112]

Although the rules concerning profiling in the GDPR are not vastly different from the rules pertaining 'automated individual decision' in the Data Protection Directive, the new definition of profiling will create a clearer framework for the national Data Protection Authorities[113] and courts to work with, as well as give organisations and individuals more legal certainty.

The obligation to notify data subjects, as well as the prohibition of profiling based on sensitive personal data, are extensions of individuals' rights. Coupled with explicit consent as a new legal basis for profiling, individuals will be more aware and more actively involved in allowing these kind of activities to take place.

Unfortunately, the GDPR does not clarify the meaning of the terms 'legal effect' or 'significantly affects' used in Article 22 (1) GDPR.[114] Privacy professionals reason that activities such as credit monitoring will fall within the concept of profiling, as they could significantly impact your chances of, for example, obtaining financing. Targeted advertising on the other hand, is seen as not significantly impactful towards individuals, and would, consequently, not be considered as profiling.[115] This statement holds true as targeted advertising, as invasive as it may be, does not affect significant aspects of an individual's daily life. Even though some activities will clearly fall within profiling, others might fall within a grey area, which will need to be filled in by national DPA's and courts. The lack of definition will most likely lead to different interpretations by DPA's and national courts across Europe.

1.4. Expanded Scope

In comparison to the Data Protection Directive, the scope of the GDPR will be expanded both materially and territorially. In what follows, we will first discuss the expansion of the material scope, which has been affected by the broader definitions as discussed in Section 1.3, and which will now also include data processors. Afterwards, we will discuss the

[112] Art. 9 (2) (a) GDPR
[113] Hereinafter: DPA.
[114] See also Proust, O. (2015). *Getting to know the GDPR, Part 5: Your big data analytics and profiling activities may be seriously curtailed*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-5-your-big-data-analytics-and-profiling-activities-may-be-seriously-curtailed [Accessed 4 May 2016].
[115] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.

consequences of the extra-territorial applicability of the GDPR as it focuses on the country of destination.

1.4.1. Material scope: definitions

As discussed under Section 1.3 on definitions, the changes to definitions and the addition of new definitions also effect the material scope of the regulation as defined in Article 2 GDPR. These conclusions will not be reiterated here.

1.4.2. Material scope: GDPR also applies to data processors

The current Data Protection Directive, generally, contains obligations for data controllers and not for processors. This last category is only subjected to obligations imposed on them through contractual relationships with data controllers.[116] Data controllers were obliged to choose a processor who would provide sufficient guarantees in respect of the technical security measures and organizational measures, and were solely responsible for failure to comply with the Data Protection Directive.

The definitions of 'controller' and 'processor' have remained consistent throughout the data protection reform. As privacy lawyer Mark Webber explained: processors are understood to be "*organisations that are purely service providers and only deal with data as their customers tell them to.*"[117] Since the status of 'processor' is so advantageous to organisations, a lot of them try to get classified as a processor to escape obligations under the Data Protection Directive. As technology evolved, however, data controllers and processors have become more inextricably linked, which is why the GDPR will be applicable to the processing of data by data controllers *and* processors[118] as they both play a critical role in the protection of data subjects' data.[119]

[116] Art. 17 (3) Data Protection Directive; See also Patrikios, A. (2015). *Getting to know the GDPR, Part 2 – Out-of-scope today, in scope in the future. What is caught?* [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-2-out-of-scope-today-in-scope-in-the-future-what-is-caught [Accessed 4 May 2016].
[117] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[118] Recital 13 GDPR. The majority of the obligations will still be focused on data controllers.
[119] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.

1.4.3. Geographical scope: extra-territoriality

The geographical scope of the current Data Protection Directive is restricted to data controllers that have been established within the EU.[120] The new GDPR will shift its focus to the country of destination. Like the Data Protection Directive, the GDPR will be applicable to data controllers established inside the EU[121], but, as discussed in Section 1.4.2, the GDPR will also be applicable to processors established inside the EU. In addition, the GDPR will be applicable to data controllers *and* processors that: (i) offer goods and services to EU residents[122] and (ii) monitor behaviour of EU residents[123]. The latter is aimed at the targeted advertising industry.[124]

The GDPR will be applicable to every data controller and processor in- or outside of the EU that is targeting EU citizens.[125] This is a huge step forward for institutions such as the Article 29 Working Party that have been trying to regulate businesses who are active in the EU, but not established in the EU. Previously, they tried to do this via cookies which are placed on someone's device and therefore indicate a presence in the EU.[126] This roundabout way of trying to regulate these companies is not ideal. Under the GDPR, such contrivances will no longer be necessary.[127] If companies want to benefit from the European market in the future, they will have to play by EU rules.

To enable supervisory authorities to communicate with companies established outside of the EU, the GDPR obliges them to appoint a representative[128] within the EU.[129] It is possible companies will be able to forum shop by assigning this representative[130] in a country where the supervisory authority has been lenient or tolerant in the past. Whether this will happen, remains to be seen.[131]

The concept of 'targeting' EU citizens is not a new one. A similar concept has been used in EU e-commerce rules and has been broadly interpreted. The target language of the site,

---

[120] Art. 4 Data Protection Directive. See also *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (es), Mario Costeja González* [2014]C-131/12 (CJEU), §55-56.
[121] Art. 3 (1) GDPR.
[122] Art. 3 (2) (a) GDPR.
[123] Art. 3 (2) (b) GDPR.
[124] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[125] Art. 3 GDPR.
[126] For more details, see Article 29 Working Party, (2010). *Opinion 8/2010 on applicable law*. p.25.
[127] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[128] Art. 4 (17) GDPR.
[129] Art. 27 GDPR.
[130] Art. 26 (3) GDPR.
[131] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.

accepting Euros as a currency and delivering to people in the EU, are all indications that a business targets the EU market.[132] The concept in the GDPR will probably reflect that of the e-commerce rules. EU e-commerce rules have taught us, however, that although the rules target and are applicable to companies outside of the EU, enforcing them has proved difficult. This is also something that will need to be addressed in the future. A supervisory authority with limited resources will perhaps not be able to enforce these rules on its own.[133]

1.4.4. Overview

Data controllers established within the EU	Their data processing activities were already subjected to the rules of the Data Protection Directive.
Processors established within the EU	Their data processing activities did not fall within the material scope of the Data Protection Directive, but will be subjected to the GDPR's direct statutory obligations for processors.[134]
Data controllers & processors established outside of the EU	Their data processing activities did not fall within the scope of the Data Protection Directive. If these organisations collect and process data belonging to EU residents, they will fall within the scope of the GDPR.

[132] Art. 6 (1) (b) Regulation No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), *O.J.* L-177, 4 July 2008, pp.6–16.
See also Ragno, F. (2009). The Law Applicable to Consumer Contracts under the Rome I Regulation. In: F. Ferrari and S. Leible, ed., *Rome I Regulation: The Law Applicable to Contractual Obligations in Europe*, 1st ed. Munich: sellier. european law publishers, pp.147-149.
[133] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[134] Art. 28 (3) GDPR.

1.5. Individual's rights are strengthened

1.5.1. Existing rights are broadened

Firstly, the GDPR will strengthen the right of access in comparison to the Data Protection Directive. Under the Data Protection Directive, organisations were allowed to charge a small fee.[135] Under the GDPR, data subjects must be able to call on their right of access for free[136]. Only if the request to have access to the data is manifestly unfounded or excessive the controller may charge a reasonable fee or can refuse the right of access. The controller will bear the burden of proof with regards to the manifestly unfounded or excessive character of the data subject's request.[137] In practice, the effect of this change might not have a huge impact considering few countries currently allow a fee to be charged.[138]

Secondly, the GDPR will expand the information data controllers need to provide in order to comply with the data subject's right to be provided with fair processing information. The Data Protection Directive only set out a minimum of information regarding the processing that needed to be provided. In the future, the data controller will need to provide more detailed information as provided under Article 13 (2) GDPR.[139] Recital 39 GDPR - again[140] - refers to the basic principle of transparency[141] and prescribes that the fact that data is being collected, used, consulted or otherwise processed, as well as to which extent the data will be processed should be communicated to the data subjects. The communication of this information must be transparent, meaning it must be easily accessible, easy to understand and clear and plain language should be used. The type of information that should be communicated can depend on the context and the purpose of the processing. If the data processing includes profiling, the data subject should be made aware of this practice and its consequences. In addition to the list in Article 13 (1) GDPR, Article 13 (2) GDPR contains a list of the information that should be communicated to the data subject specifically to ensure fair and transparent processing. The latter includes the existence of the different rights data subjects have, the right to lodge a complaint to a supervisory authority, whether the provision of this data is a contractual requirement and the existence

[135] Art. 12 Data Protection Directive.
[136] Art. 12 (5) GDPR.
[137] Art. 12 (5) GDPR.
[138] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[139] Recital 39 GDPR gives the identity of the controller and the purpose of the processing as examples of information that should be provided.
[140] Section 1.3.2.2 of Chapter III on the protection of vulnerable groups.
[141] Art. 5 (1) (a) GDPR.

of practices such as profiling. The intention of the lawmakers seems to be to inform data subjects of their rights as thoroughly as possible. It is, however, questionable, if this goal will not be compromised by the sheer amount of information data subjects have to wade through.

Finally, the right to object to the processing of data was given a broader scope. Whereas the the right to object to the processing of data was only available in limited circumstances under the Data Protection Directive,[142] it will now also be available to data subjects in cases where the processing is based on the legitimate interests of the controller or is undertaken for specific marketing purposes.[143] The data subject will no longer need to provide specific justifications to exercise this right.

1.5.2. New rights

The GDPR introduces two new key rights for data subjects: the right to be forgotten (Section 1.5.2.1) and the right to data portability (Section 1.5.2.2).

1.5.2.1 The right to be forgotten

The right to be forgotten is not entirely new, the Data Protection Directive already contained a narrower right to erasure for data which was no longer necessary for the specified purpose.[144] The right to be forgotten emerged as a principle through the case law of the CJEU, i.e. the *Costeja v. Google* case.[145] This case gave individuals the right to have their data removed from search engines, such as Google.[146]

The implementation of the right to be forgotten in the GDPR was highly debated and was the subject of 118 amendments throughout the legislative process.[147] Throughout this process, the European Parliament[148] proposed a watered down version of the right to be forgotten, going back to calling it the 'right to erasure'. Additionally, the Council proposed to

---

[142] Art. 14 Data Protection Directive.
[143] Art. 21 (1) – (3) GDPR.
[144] Art. 12 Data Protection Directive.
[145] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González* [2014]C-131/12 (CJEU).
[146] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[147] Lobbyplag. (n.d.). *LobbyPlag: Amendments*. [online] Available at: http://lobbyplag.eu/map/article/17 [Accessed 9 May 2016].
[148] European Parliament, Legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Ordinary legislative procedure: first reading, 12 March 2014, C7-0025/2012 – COM 2012/0011(COD).

remove the data controller's obligation to make sure third parties also erase the data,[149] which was proposed by the Parliament.[150] In the final version of the GDPR, even the name, which had changed back and forth in previous versions, is a compromise: "Right to erasure ('right to be forgotten')".[151] A former Associate General Counsel at Google[152] already called the final version of the right to be forgotten ambiguous on key points, going as far as calling it "*the gift of lifetime employment*" for data protection lawyers.[153]

Under the GDPR, this right will no longer be restricted to search engines, it will apply to any controller that stores your data. The *Costeja v. Google* case already established that search engines are data controllers.[154] An important question will be whether intermediaries, such as Facebook or Wikipedia, will be seen as controllers. This will impact situations where, for example, someone requests Facebook or Twitter, which are intermediary hosting platforms, to take down a post from another user about the individual who requests the takedown.[155]

One of the main arguments against imposing this obligation on intermediaries is that intermediaries do not always control what information is processed. On online social networks, for example, it is the user himself who decides what information or data to upload, the intermediary subsequently only processes this data based on instructions given

---

[149] European Council, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 15 June 2015, COM 2012/0011 (COD).

[150] See also Van Canneyt, T. and Power, L. (2015). *Getting to know the GDPR, Part 4 – "Souped-up" individual rights*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-4-souped-up-individual-rights/ [Accessed 4 May 2016].

[151] Art. 17 GDPR.

[152] *"Daphne Keller is the Director of Intermediary Liability at the Stanford Center for Internet and Society. She was previously Associate General Counsel for Intermediary Liability and Free Speech issues at Google. In that role she focused primarily on legal and policy issues outside the U.S., including the E.U.'s evolving "Right to Be Forgotten." Her earlier roles at Google included leading the core legal teams for Web Search, Copyright, and Open Source Software."* The Center for Internet and Society. (n.d.). *Stanford Law School - Daphne Keller*. [online] Available at: http://cyberlaw.stanford.edu/about/people/daphne-keller [Accessed 14 May 2016].

[153] Keller, D. (2015). *The Final Draft of Europe's "Right to Be Forgotten" Law*. [online] Center for Internet and Society. Available at: http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law [Accessed 4 May 2016].

[154] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González* [2014]C-131/12 (CJEU), §41.

[155] Keller, D. (2015). *The Final Draft of Europe's "Right to Be Forgotten" Law*. [online] Center for Internet and Society. Available at: http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law [Accessed 4 May 2016].

by the user.[156] Recital 18 of the GDPR explains that social networking purely for household activities, will not fall within the scope of this regulation. It also states, however, that controllers and processors who provide the means for this activity fall within the scope of the GDPR. This recital, combined with the fact that DPA's have been strict towards online social networks, such as Facebook, in the past, leads to the conclusion that online social networks will likely need to comply with the obligations regarding the right to be forgotten. When these intermediaries decide whether or not they want to take this risk, they will take into account the high fines imposed on failure to comply. The introduction of these administrative fines will be discussed under Section 1.8 of this chapter.

How organisations should comply with a request regarding the right to be forgotten is not entirely clear yet. The GDPR does not contain a procedure, nor does it contain guidelines in balancing these claims with the freedom of expression or dealing with invalid claims. Some legal scholars suggest the procedure contained in the E-Commerce Directive[157] should be applied as it contains this type of guidelines and would ensure consistent procedures for the removal of data regardless of the legal basis of the request. There is, however, much discussion on whether or not the E-Commerce Directive is even applicable, as the text of the E-Commerce Directive[158] and the GDPR[159] seem contradictive on the applicability.[160]

The E-Commerce Directive states that companies do not have to take content offline until they have verified the validity of the claim and weighed it against other interests. The GDPR and its fines might conflict with these instructions. The GDPR does not contain penalties for organisations who remove too much data, but it does contain fines for not removing data in accordance with the right to be forgotten The fines could potentially promote the removal of data before examining the validity or weighing the removal against other rights and freedoms. It is not desirable for organisations to be encouraged to remove data without thorough examination.

---

[156] Keller, D. (2015). *The Final Draft of Europe's "Right to Be Forgotten" Law*. [online] Center for Internet and Society. Available at: http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law [Accessed 4 May 2016].
[157] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *O.J.* L-178, 17 July 2000, pp.1-16. Hereinafter: E-Commerce Directive.
[158] Art. 12 and 15 E-commerce Directive.
[159] Sartor, G. (2013). *Providers' liabilities and the right to be forgotten*. European University Institute, p.9.
[160] Keller, D. (2015). *The Final Draft of Europe's "Right to Be Forgotten" Law*. [online] Center for Internet and Society. Available at: http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law [Accessed 4 May 2016].

Finally, Recital 66 GDPR and Article 17 (2) GDPR require the controller, contacted by the data subject, to contact other controllers who are processing the data subject's data to inform them about the request. This will often be applicable in cases were controllers subcontracted their processing activities to other companies.

1.5.2.2 Right to data portability

Aside from the right to be forgotten, individuals will have another new right: the right to data portability.[161] This gives data subjects the right to retrieve their data from a specific data controller and transfer this data to another data controller. The goal of this new right is to avoid service providers from keeping customers locked-in, simply because they have their data.[162] Critics, however, have expressed several concerns about this new right to data portability.[163]

The first criticism concerns the right to data portability's relation to EU competition and US antitrust law, both of which were created to solve the abovementioned lock-in problems. These laws require that market dominance is shown in order to avoid targeting small, start-up companies. Critics worry that the obligations imposed by the right to data portability apply, without any distinction, to large companies and small start-up companies. Considering the new software that will be needed and the fact that this software will need to be aligned worldwide, the costs for start-ups might be to big to bear.[164]

The second criticism, which is the most relevant to this dissertation, is that the right to data portability might actually reduce the quality of data protection that individuals receive, by creating a bigger risk of infringement on a data subject's right to data security[165]. This criticism stems from the increasing tension between access to information and the security thereof. The right to data portability allows a person to request a lifetime of personal data. One would rationally assume companies check the identity of the person requesting this information. The GDPR conversely states that the right to data portability must be acknowledged without hindrance, which may encourage companies to not check identities

[161] Art. 20 GDPR.
[162] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[163] Swire, P. and Lagos, Y. (2013). Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. *Maryland Law Review*, 72, pp.336-339.
[164] Swire, P. and Lagos, Y. (2013). Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. *Maryland Law Review*, 72, pp.335-380.
[165] Art. 32 GDPR.

as thorough[166] in order to avoid fines of "*up to 20 000 000 EUR, or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher*"[167].

While this second criticism seems acceptable, the majority of the risks to data security can be dealt with by putting in place the necessary security safeguards. This includes performing thorough identity checks, which is also in line with organisations' basic duty of care in accordance with the data subject's right to security.[168]

1.5.3. Restrictions to rights

Article 23 GDPR contains the limited grounds for restriction of the rights found in Articles 12 to 22 GDPR. The grounds for restriction range from defence and national security, to protection of judicial independence and judicial proceedings and the protection of the data subject or the rights and freedoms of others.

Article 23 (2) GDPR specifies that any law that restricts the rights on these grounds, must specify certain facts, specifically (i) the purposes of the processing or categories of processing, (ii) the categories of personal data, (iii) the scope of the restrictions introduced, (iv) the safeguards to prevent abuse or unlawful access or transfer, (v) the risks for the rights and freedoms of data subjects and (vi) the right of data subjects to be informed about the restriction, unless this may be prejudicial to the purpose of the restriction.[169]

1.6. Obligations of data controllers and data processors

1.6.1. Accountability principles

Ever since the European Commission proposed the new GDPR in 2012, the principle of accountability has been at the forefront of the new legislation. The concept of accountability is not a new one. The Organisation for Economic Co-operation and Development[170] has been

[166] Swire, P. and Lagos, Y. (2013). Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. *Maryland Law Review*, 72, pp.335-380.
[167] Art. 83 (5) (b) GDPR.
[168] Art. 32 GDPR.
[169] Art. 23 (2) GDPR.
[170] Hereinafter: OECD.

issuing its Guidelines on the Protection of Privacy and Transborder Data Flows, including the principle of accountability, since 1980.[171] The latest version was issued in 2013.[172]

National lawmakers have also been paying attention to the principle of accountability. The CNIL, the French DPA, for example, published its own accountability standards in 2015.[173] The same trend occurs globally in countries such as Canada[174] and Australia[175]. Most of these guidelines are similar to the guidelines set out by the OECD.[176] Inside the EU regulatory framework, however, the principle of accountability has never been as important as it is in the new GDPR.

Currently, the Data Protection Directive includes some obligations that fall within the concept of accountability.[177] Firstly, there is the processing notice, which requires the provision of specific information about intended processing activities to individuals.[178] Secondly, the Data Protection Directive includes the requirement for organisations to notify the national DPA's of intended processing activities.[179] Lastly, the requirement for organisations to have appropriate technical and organisational measures ensuring privacy and security of the personal data they are processing, also falls within the accountability principle.[180]

The principle of accountability will be a core principle in the new GDPR and can be found throughout the entirety of the text. The principle itself is formulated in Article 5 (2)

---

[171] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016; OECD, (2011). *Thirty years after the OECD Privacy Guidelines*. [online] Available at: http://www.oecd.org/sti/ieconomy/49710223.pdf [Accessed 4 May 2016].
[172] OECD, (2013). *Privacy Guidelines*. Available at: http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm [Accessed 20 April 2016].
[173] CNIL, (2015). *Un nouveau label CNIL gouvernance Informatique et Libertés*. [online] Available at: https://www.cnil.fr/fr/un-nouveau-label-cnil-gouvernance-informatique-et-libertes [Accessed 4 May 2016].
[174] Office of the Privacy Commissioner of Canada, (2012). *Getting Accountability Right with a Privacy Management Program*.
[175] Australian Law Reform Commission, (2008). *Report 108 Volume 2*. pp.1132-1134.
[176] Davidson, B. (2016). *Getting to know the General Data Protection Regulation, Part 7 - Accountability Principles = More Paperwork*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-7-accountability-principles-more-paperwork [Accessed 4 May 2016].
[177] Davidson, B. (2016). *Getting to know the General Data Protection Regulation, Part 7 - Accountability Principles = More Paperwork*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-7-accountability-principles-more-paperwork [Accessed 4 May 2016].
[178] Art. 12 (a) Data Protection Directive.
[179] Art. 18 Data Protection Directive.
[180] Art. 17 (1) Data Protection Directive.

GDPR, and exists of two aspects: firstly, the data controller is responsible for compliance, and secondly, the data controller must be able to demonstrate its compliance.

The obligations surrounding the principle of accountability are set out more clearly in Articles 24 to 31 GDPR. The obligations of organisations will mainly consist of the following four measures: firstly, they will need to ensure they put a documentation system in place **(i)**, secondly, they will need to ensure their systems comply with the regulation **(ii)**, thirdly, they will need to ensure technical compliance **(iii)** and lastly, they will – in some circumstances – be required to appoint a data protection officer **(iv)**.[181]

(i) Documentation system

Article 30 GDPR creates a broad obligation for the data controller[182] and processor[183] to maintain records of its processing activities. Article 30 (5) GDPR contains an exception to this obligation for organisations employing less than 250 persons, unless the processing:

- is likely to pose a risk to the rights and freedoms of the data subjects; or
- is not occasional; or
- includes sensitive personal data.[184]

(ii) Systems compliance: 'privacy by design' and 'privacy by default'

Throughout every product's development process, from start to finish, organisations will need to take into account privacy concerns.[185] This idea, commonly referred to as 'privacy by design'[186], expects organisations to design their products and other activities for compliance. Organisations will need to consider privacy in anything and everything they do.[187]

---

[181] Davidson, B. (2016). *Getting to know the General Data Protection Regulation, Part 7 - Accountability Principles = More Paperwork*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-7-accountability-principles-more-paperwork [Accessed 4 May 2016].
[182] Art. 30 (1) GDPR.
[183] Art. 30 (2) GDPR.
[184] As defined in Articles 9 (1) and 10 GDPR.
[185] Davidson, B. (2016). *Getting to know the General Data Protection Regulation, Part 7 - Accountability Principles = More Paperwork*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-7-accountability-principles-more-paperwork [Accessed 4 May 2016].
[186] Art. 25 (1) GDPR.
[187] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.

The current Data Protection Directive does not contain the concept of 'privacy by design'. It also does not contain any obligation to consider privacy issues from the design stage of a project. As mentioned above, the Data Protection Directive only included the obligation to implement appropriate technical and organisational measures to protect personal data against unlawful processing.[188] The GDPR's inclusion of the privacy by design principle ensures privacy can no longer be an afterthought.[189] It will require companies to design compliant policies, procedures and systems at the outset of any development process.[190]

When implementing the necessary measures, several things should be taken into account:

> *"Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organisational measures (…)"*[191]

The risk-based approach was added at the initiative the Council[192]. Permitting businesses to take these factors into account, will provide them with more flexibility. Consequently, his might create difficulties regarding the interpretation in the future.[193]

In addition to 'privacy by design', the GDPR also introduces the concept 'privacy by default'.[194] This concept is meant to ensure that, when data controllers implement the

---

[188] Mahmood, S. and Power, L. (2016). *Getting to know the General Data Protection Regulation, Part 6 – Designing for compliance*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-6-designing-for-compliance/ [Accessed 4 May 2016].

[189] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.

[190] Art. 25 (1) GDPR.
See also Mahmood, S. and Power, L. (2016). *Getting to know the General Data Protection Regulation, Part 6 – Designing for compliance*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-6-designing-for-compliance/ [Accessed 4 May 2016].

[191] Art. 32 (1) GDPR. Editing by author.

[192] European Council, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 15 June 2015, COM 2012/0011 (COD).

[193] Mahmood, S. and Power, L. (2016). *Getting to know the General Data Protection Regulation, Part 6 – Designing for compliance*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-6-designing-for-compliance/ [Accessed 4 May 2016].

required appropriate technical and organisational measures, by default, only necessary personal data for each specific purpose of the processing will be processed.[195] Article 25 GDPR specifies that this requires organisations to evaluate the amount of data they collect, the extent of the processing, the period of storage and the accessibility. By default, the amount of data should be restricted to what is necessary for the intended purpose and it should not be stored longer than necessary in light of the intended purpose. Article 25 GDPR also specifically states that, without the data subject's consent, the data should not be available to an indefinite amount of people.

The fundamental difference between the Data Protection Directive and the GDPR is that, whereas the Data Protection Directive only required organisations to ensure that excessive personal data was not processed and stored longer than necessary, the GDPR now additionally requires specific technical and organisational measures be put in place to meet these requirements.[196] Automated processes for erasure of particular personal data after a specific period, can be an example of a measure taken to comply with the regulation regarding the period of storage.

(iii) Technical Compliance

Technical compliance pertains mainly to the security of data through techniques, such as pseudonymisation and encryption, to ensure the integrity of the organisation's systems. Organisations should be able to demonstrate the resilience of their systems when confronted with a physical or technical incident, as well as put procedures in place to test systems at various moments in various situations.

As a part of technical compliance organisations will also need to put procedures in place in case of a data breach. This subject will be discussed in Section 1.6.2 of this chapter.

---

[194] Art. 25 (2) GDPR.
[195] Mahmood, S. and Power, L. (2016). *Getting to know the General Data Protection Regulation, Part 6 – Designing for compliance*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-6-designing-for-compliance/ [Accessed 4 May 2016].
[196] Mahmood, S. and Power, L. (2016). *Getting to know the General Data Protection Regulation, Part 6 – Designing for compliance*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-6-designing-for-compliance/ [Accessed 4 May 2016].

(iv) Personnel

One of the key requirements for compliance with the accountability principle will be the appointment of a data protection officer[197]. Section 1.6.3 of this chapter will go into further detail about the different aspects of the appointment of a DPO.

1.6.2. Data breaches must be notified

The GDPR requires organisations that suffer a data breach to report this to the national DPA within 72 hours of becoming aware of the breach.[198] In addition, if the breach poses a high risk to data subjects' rights and freedoms, the organisation also needs to notify the affected data subjects without undue delay.[199]

The burden of proof for this notification requirement will rest upon the organisation itself. Consequently, it will be crucial for organisations to document this process sufficiently, including full details of the breach, its consequences, and the measures taken to address the breach.[200]

1.6.3. Appointment of a data protection officer

Under the current Data Protection Directive, there is no provision requiring companies to appoint a DPO. Member states did have the authority to exempt companies, who appointed a DPO, from the duty to register with the local DPA. Member states were given a broad range to implement this feature of the Data Protection Directive. As a result, various rules apply across Europe.

The new GDPR will harmonize the appointment of a DPO, making it a mandatory obligation for certain data controllers and processors.[201] In what follows we will discuss which companies will need to appoint a DPO as well as the rights and obligations of the DPO.

---

[197] Hereinafter: DPO.
[198] Art. 33 GDPR.
[199] Art. 34 GDPR.
[200] Davidson, B. (2016). *Getting to know the General Data Protection Regulation, Part 7 - Accountability Principles = More Paperwork*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-7-accountability-principles-more-paperwork [Accessed 4 May 2016].
[201] Privacylawblog.fieldfisher.com. (2016). *Getting to know the General Data Protection Regulation - Part 8*. [online] Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-8-you-may-need-to-appoint-a-data-protection-officer/ [Accessed 4 May 2016].

1.6.3.1 Which companies must appoint a DPO?

Throughout the legislative process a number of ways were suggested to determine which companies would be required to appoint a DPO. Initially, the European Commission proposed to make the appointment of a DPO mandatory for every company that employs more than 250 people.[202] The European Parliament instead proposed to adjust this to every company that processes data of more than 250 people.[203] The final version of the GDPR was watered down in the trilogue negotiations, with Article 37 GDPR specifying which data controllers and processors will fall under the obligation. The obligation will apply to all data controllers and processors:

- that are public authorities processing personal data, with the exception of courts acting in their judicial authority; or
- whose core activities involve regular and systematic monitoring of data subjects on a large scale; or
- whose core activities involve the large scale processing of special categories of data as defined in Articles 9 and 10 GDPR.

A missed opportunity seems to be the lack of a definition for 'core activities' or 'large scale'. At first glance the underlying intention was to broadly capture data controllers and processors who deal with so-called 'big data'.[204] While definitions could have had either a restricting effect, or an expanding effect, they would have certainly been able to create more legal certainty for data subjects. It remains to be seen how the national DPA's and courts will interpret Article 37 GDPR.

Recital 24 GDPR suggests that the second type of data controllers and processors, namely those whose core activities involve regular and systematic monitoring of data

---

[202] Art. 35 (1) (b) European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM 2012/0011 (COD).

[203] European Parliament, Legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Ordinary legislative procedure: first reading, 12 March 2014, C7-0025/2012 – COM 2012/0011(COD).
See also Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.

[204] Privacylawblog.fieldfisher.com. (2016). *Getting to know the General Data Protection Regulation - Part 8*. [online] Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-8-you-may-need-to-appoint-a-data-protection-officer/ [Accessed 4 May 2016].

subjects on a large scale, is only intended to capture companies who are engaged in the online behaviour tracking or profiling of data subjects[205], and therefore not all big data companies.

Likewise, some legal scholars already assume the third type of data controllers and processors will only capture companies whose services are focused on helping other companies address compliance requirements with regards to HIPAA requirements[206] or requirements to store patient records for large public sector health authorities.[207] They theorize this third category was not meant to apply to all companies processing special categories of data. However, since there is no explicit mention of this in any part of the GDPR, it seems premature to restrict this third category to this very specific set of companies.

Both the second and the third category also require the processing activity to be a core business. This will exclude companies, who may be undertaking activities such as profiling and tracking, but not as a part of their core activities. This will be the case for companies who, for example, profile or track their employees.

Member states are given the opportunity to install further requirements regarding the appointment of a DPO. This creates the possibility to impose stricter rules through national law.[208]

1.6.3.2 What are the rights and obligations of the DPO?

The GDPR does not contain specific requirements for the DPO, it only contains a general requirement that the DPO must have "*expert knowledge of data protection law and practices*".[209] This should enable him to fulfil the duties set out in Article 39 GDPR:

> *"The data protection officer shall have at least the following tasks:*

---

[205] Privacylawblog.fieldfisher.com. (2016). *Getting to know the General Data Protection Regulation - Part 8*. [online] Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-8-you-may-need-to-appoint-a-data-protection-officer/ [Accessed 4 May 2016].

[206] HIPAA requirements stem from the US Health Insurance Portability and Accountability Act of 1996. It sets standards for protecting sensitive patient data.

[207] Privacylawblog.fieldfisher.com. (2016). *Getting to know the General Data Protection Regulation - Part 8*. [online] Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-8-you-may-need-to-appoint-a-data-protection-officer/ [Accessed 4 May 2016].

[208] Art. 37 (4), 38 (5) and 39 (1) (a-b) GDPR.

[209] Art. 37 (5) GDPR.

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter."[210]

In addition to these duties, the DPO will be subjected to some other obligations. The DPO will be subject to confidentiality and rules regarding conflicts of interest.[211]

The DPO will also be entitled to certain rights as a consequence of his function. Firstly, he will have the right to have access to sufficient resources to perform his tasks and invest in his ongoing training.[212] DPO's must have access to the company's data processing personnel and operations.[213] The GDPR also obliges the DPO to report directly to the highest management level of the company[214], warranting the handling of data protection issues up to the board level.[215]

The DPO could be an employee or a third party. Data protection lawyers are already advising their clients to opt for a third party as a DPO, as an employee as DPO is entitled to special protection against dismissal.[216]

---

[210] Editing by author.
[211] Art. 38 (5) and (6) GDPR.
[212] Art. 38 (2) GDPR.
[213] Art. 38 (1) GPDR; See also Privacylawblog.fieldfisher.com. (2016). *Getting to know the General Data Protection Regulation - Part 8*. [online] Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-8-you-may-need-to-appoint-a-data-protection-officer/ [Accessed 4 May 2016].
[214] Art. 36 (3) GDPR.
[215] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.
[216] Phil Lee and Mark Webber, "GDPR 1.0 - Top 10 Things You Need To Know!", 2016.

1.7. International data exports

The current Data Protection Directive contains a bottom line stating businesses are prohibited from transferring personal data to a third country outside of the European Economic Area if that country does not provide adequate data protection.[217] The European Commission was given the power to approve particular countries, through adequacy decisions, and thereby confirm these countries provide an adequate level of data protection.[218] One of the most important examples in this regard is the Safe Harbour Decision. The Safe Harbour Decision will soon be replaced by the EU – US Privacy Shield, which will be discussed in detail in Section 2 of this chapter.

In addition, businesses can transfer data to a third country, which may not provide an adequate level of data protection, as long as they regulate the transfer of data themselves through contractual rules or binding corporate rules.[219] These contractual rules are often based on the model clauses approved by the European Commission. Further rules regarding the international transfer of data are different in each member state.

The data protection reform did not introduce any major changes to the data transfer regime under the Data Protection Directive. Data transfers will still be prohibited to countries that do not offer adequate protection.[220] The European Commission will still be able to approve particular countries[221] and the adequacy decisions issued while the Data Protection Directive was in force will remain valid.[222] The GDPR does, however, provide a mechanism for frequent re-evaluation of the data protection in third countries, containing the explicit possibility to repeal, amend or suspend these adequacy decisions.[223]

In addition, data transfers will exceptionally be allowed based on conditions such as explicit consent and legitimate interest.[224] The latter will only be possible if the data transfer is not repetitive and concerns a limited amount of data subjects.[225]

---

[217] Art. 25 (1) Data Protection Directive.
[218] Art. 25 (6) Data Protection Directive; See also Power, L. (2016). *Getting to know the GDPR, Part 9 – Data transfer restrictions are here to stay, but so are BCR*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-9-data-transfer-restrictions-are-here-to-stay-but-so-are-bcr/ [Accessed 4 May 2016].
[219] Art. 26 (2) Data Protection Directive.
[220] Art. 44 GDPR.
[221] Art. 45 (1) GDPR.
[222] Art. 45 (9) GDPR.
[223] Art. 45 (5) GDPR.
[224] Art. 49 (1) GDPR.
[225] Art. 49 (1) (h) GDPR.

The GDPR will still allow companies to guarantee adequate protection through use of model clauses or binding corporate rules.[226] The model clauses approved by the European Commission under the Data Protection Directive[227] will remain valid.[228] The GDPR also states that when using these model clauses, no additional authorization from DPA's will be necessary,[229] as is the case in some member states now.

1.8. Introduction of administrative fines

While the Data Protection Directive did not contain any mention of administrative fines, the GDPR introduces very high administrative fines for violations of the regulation. The fines can go up to 10 000 000 EUR[230] for some violations and up to 20 000 000 EUR[231] for others.

These fines might prove to be the best encouragement for companies to take the right to privacy to heart. On the contrary, they might also encourage companies to take steps that infringe on other rights such as the freedom of expression when erasing data as mentioned under Section 1.5.2.1 of this chapter. It will be crucial to put measures in place ensuring these cases are few and far between.

[226] Art. 46 (2) GDPR.
[227] Art. 26 (4) Data Protection Directive.
[228] Art. 46 (5) GDPR.
[229] Art. 46 (2) GDPR.
[230] Art. 83 (4) GDPR.
[231] Art. 83 (5) - (6) GDPR.

2. Data Transfers to the United States of America: from Safe Harbour to the EU – US Privacy Shield

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."[232]

- EDWARD SNOWDEN[233]

2.1. Invalidation of the Safe Harbour Agreement

The Safe Harbour Agreement was an agreement between the EU and the US dating back to 2000. It comprised a system of self-certification set up by the US State Department. Organisations could take part in this system and thus commit themselves to protect European data in accordance with seven principles set out by the Safe Harbour Agreement.[234] This agreement was given effect by the European Commission's adequacy decision: the Safe Harbour Decision.

In October 2015, the CJEU declared the Safe Harbour Decision invalid in the *Schrems* case.[235] This ruling was based partly on revelations from Edward Snowden evidencing mass surveillance on European citizens by the National Security Agency[236]. The *Schrems* case[237] will be discussed in more detail in Chapter VI. All data transfers to the US based on the certification offered by the Safe Harbour Agreement *after* this ruling are illegal. A lot of companies' data transfer practices are compromised by this legal uncertainty, which is why the negotiations for the EU – US Privacy Shield gained momentum.[238] The European

---

[232] Snowden, E. (2015). *Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLU's Jameel Jaffer. AUA. • /r/IAmA*. [online] reddit. Available at: https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/crglgh2 [Accessed 15 May 2016].

[233] *"Edward Snowden is a former National Security Agency subcontractor who made headlines in 2013 when he leaked top secret information about NSA surveillance activities."* Biography. (2016). *Edward Snowden*. [online] Available at: http://www.biography.com/people/edward-snowden-21262897 [Accessed 15 May 2016].

[234] Lee, P. (2016). *The Privacy Shield – is it any good then?*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/the-privacy-shield-is-it-any-good-then/ [Accessed 4 May 2016].

[235] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU).

[236] Hereinafter: NSA.

[237] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU).

[238] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.3.

Commission announced the new agreement in February 2016 stating it could *"restore trust in transatlantic data flows since the 2013 surveillance revelations"*[239].

Before the EU – US Privacy Shield can be applied to data transfers, the European Commission must give effect to the agreement by adopting an adequacy decision. Following the comitology procedure, the European Commission cannot adopt its adequacy decision before obtaining an opinion from the Article 29 Working Party. In its opinion, the Article 29 Working Party has already criticised the new agreement.[240] This criticism, as well as the criticisms from other parties, will be discussed under Section 2.3 of this chapter.

2.2. Seven core principles

Like the Safe Harbour Agreement, the EU – US Privacy Shield will work with a self-certification system based on seven principles.[241] This time, however, the principles are promised to be more detailed.[242] The seven core principles comprised in the EU – US Privacy Shield are: (i) notice, (ii) choice, (iii) accountability for onward transfer, (iv) security, (v) date integrity and purpose limitation, (vi) access and (vii) recourse, enforcement and liability.[243] Additionally, the EU – US Privacy Shield contains a number of supplemental principles. These supplemental principles can serve multiple purposes. Firstly, they address special situations such as the handling of sensitive data and journalistic exceptions. Secondly, they contain extra requirements and clarifications to the core principles.[244]

2.2.1. Notice

The notice principle will be similar to the right to information data subjects receive under EU data protection laws. Organisations will be obligated to provide them information

---

[239] European Commission, (2016). *Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield*. [online] Available at: http://europa.eu/rapid/press-release_IP-16-433_en.htm [Accessed 6 May 2016].
[240] Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*.
[241] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, pp.4-5.
[242] Lee, P. (2016). *The Privacy Shield – is it any good then?*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/the-privacy-shield-is-it-any-good-then/ [Accessed 4 May 2016].
[243] EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, pp.4-7.
[244] Lee, P. (2016). *The Privacy Shield – is it any good then?*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/the-privacy-shield-is-it-any-good-then/ [Accessed 4 May 2016].

about subjects such as the type of data collected, the purpose of the processing and the existence of the right of access.[245]

Additionally, organisations will need to make the privacy policy available to the public and provide a link to the US Department of Commerce's website, which contains more information about data subjects' rights and the available mechanisms for recourse.[246]

In the first place, this information must be provided when data subjects are asked to give personal data. If this is not possible, the information may be provided afterwards as soon as possible. The notice must be given in clear and noticeable language.[247]

2.2.2. Choice

The choice principle offers data subjects the right to opt out at any time if their data will be disclosed to a third party or used for a materially different purpose. In the case of sensitive personal data, organisations will need to obtain affirmative and express consent (opt-in) to use the data for a different purpose or to disclose it to a third party.[248]

2.2.3. Accountability for onward transfer

This principle entails that the transfer of data to controllers or processors can only take place on the basis of a contract for limited and specified purposes and only if that contract provides an equal level of protection as guaranteed by the seven core principles.[249]

This principle should be read together with the notice principle and the choice principle, which allow data subjects to opt out, or in the case of sensitive personal data, to opt in for future transfers.[250]

---

[245] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.4.
[246] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.4.
[247] EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, pp.4-5.
[248] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.4; EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, p.5.
[249] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.5; EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, p.5.

If damage arises, caused by the transfer of data in the chain of processing, the burden of proof will lie with the organisation acting as the processor or controller of the data. The organisation will need to prove they were not responsible for the event that caused the damage. If they cannot provide proof, they will be held responsible as the original data controller or processor of the data.[251]

2.2.4. Security

The security principle is similar to the requirement to provide security of processing under the GDPR.[252] It requires organisations to put in place reasonable and appropriate security measures taking into account the risks involved in the processing and the nature of the data.[253]

In the case of sub-processing, the EU – US Privacy Shield requires a contract that guarantees the same level of protection as provided by the seven core principles, and ensures the proper implementation.[254]

2.2.5. Date integrity and purpose limitation

The data integrity and purpose limitation principle is a manifestation of the EU data protection laws which require the collection of personal data to be limited to what is relevant for the specified purpose. *A contrario* it prohibits the processing of any personal data contrary to the purpose for which is was initially collected or subsequently authorised by the data subject.[255]

---

[250] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.5; EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, p.5.
[251] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.5; EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, pp.5-6.
[252] Art. 32 GDPR.
[253] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.4; EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, p.6.
[254] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, pp.4, 20-21.
[255] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, pp.4-5.

As long as the organisation retains the information, it is obliged to comply with this principle and take reasonable steps ensuring that the data is: *"reliable for its intended use, accurate, complete and current."*[256]

2.2.6. Access

The access principle is the expression of the right of access provided to data subjects under EU data protection law. Unlike the new GDPR, this principle still allows the organisation to charge a non-excessive fee. [257]

The restriction of this right is possible only in exceptional circumstances.[258] For example, the EU – US Privacy Shield also provides an exception for cases where the rights of other individuals would be violated, or where the right of access would create a burden or expense disproportionate to the individuals' privacy risk.[259] The right of access, however, cannot be refused on the basis of cost when the data subject offers to pay these costs.[260] When the right of access is denied, the burden of proof will lie upon the organisation to prove these conditions were fulfilled.[261]

Along with the right of access, the access principle also gives data subjects the right to correct, amend or delete any information if it is either inaccurate, or has been processed in violation of the seven core principles.[262]

---

[256] EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, p.6.
[257] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.5; EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, p.18.
[258] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.5; EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, p.17.
[259] EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, p.16.
[260] EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, p.18.
[261] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.5.
[262] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.5; EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, p.6.

2.2.7. Recourse, enforcement and liability

Once organisations participate in the self-certification system, they are bound by the seven core principles. Their participation must be re-certified annually. To ensure effective privacy protection, a system for ensuring compliance must be put in place.[263] This can be achieved in two possible ways. The first possibility is a system of self-assessment, including (i) internal procedures for the training on the implementation of privacy policies, and (ii) periodical review in an objective manner. The second possibility consists of outside compliance reviews such as auditing or random checks.[264]

The EU – US Privacy Shield also requires follow-up procedures to ensure declarations made by organisations about their privacy policies are true and have been implemented as stated. This requirement is of special importance when violations have already been exposed.[265]

The next step in ensuring effective privacy protection is putting in place a system to offer recourse to affected data subjects when the seven core principles are not respected.[266] The EU – US Privacy Shield will require a readily available and independent recourse mechanism. Data subjects' complaints must be solved expeditiously and free of charge. One possibility offered by the EU – US Privacy Shield to aide in complying with the effective recourse obligations, is to cooperate with the national DPA's. In case non-compliance is uncovered, the EU – US Privacy Shield requires rigorous sanctions.[267]

Additionally, the ombudsperson is a completely new mechanism established in Annex III of the EU – US Privacy Shield. The ombudsperson, who will work independently from the US intelligence services, will deal with complaints from EU citizens when they fear their data has been used unlawfully in the area of national security.[268]

---

[263] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.5.
[264] European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, p.5.
[265] EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, pp.6-7, 14-15.
[266] EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, pp.21-25.
[267] EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, pp.6-7, 9-10.
[268] European Commission, (2016). *EU-U.S. Privacy Shield: Frequently Asked Questions*. [online] Available at: http://europa.eu/rapid/press-release_MEMO-16-434_en.htm [Accessed 6 May 2016].

2.3. Criticism

Although the new EU – US Privacy shield has not even entered into force yet, it has already caused an abundance of criticism. Noticeable was the criticism of Edward Snowden, whose revelations triggered the invalidation of the Safer Harbour Agreement in the first place. Snowden stated: "*it's not a 'Privacy Shield,' it's an accountability shield. Never seen a policy agreement so universally criticized."*[269] In what follows, the criticisms expressed by the Article 29 Working Party and the national DPA's will be discussed.

2.3.1. Opinion of the Article 29 Working Party

Despite the fact that the Chair of the Article 29 Working Party expressed that the initial reaction to the EU – US Privacy Shield was positive, the Article 29 Working Party addressed several concerns and shortcomings.[270] The Article 29 Working Party based its opinion[271] on the current Data Protection Directive, Article 8 ECHR and Articles 7, 8 and 45 of the Charter, as well as the *Schrems case*[272].

Firstly, the Article 29 Working Party considers the EU – US Privacy Shield, consisting of a draft adequacy decision and seven annexes, to be too complex and inconsistent. The Article 29 Working Party actually had to have several meetings with US Representatives and the European Commission to clarify some aspects of the agreement.[273]

Secondly, the Article 29 Working Party does not believe the EU – US Privacy Shield offers protection equivalent to the EU data protection rules as key principles such as data retention[274] cannot be found in the new agreement.[275] It stated that "*the language used in the draft adequacy decision does not oblige organisations to delete data if they are no longer necessary. This is an essential element of EU data protection law to ensure that data is kept for*

---

[269] Snowden, E. (2016). *Edward Snowden on Twitter*. [online] Twitter. Available at: https://twitter.com/Snowden/status/694571566990921728 [Accessed 6 May 2016].
[270] Cropper, L. (2016). *EU-US Privacy Shield: The Article 29 Working Party raises its concerns*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/eu-us-privacy-shield-the-article-29-working-party-raises-its-concerns/ [Accessed 3 May 2016].
[271] Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*.
[272] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU).
[273] Cropper, L. (2016). *EU-US Privacy Shield: The Article 29 Working Party raises its concerns*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/eu-us-privacy-shield-the-article-29-working-party-raises-its-concerns/ [Accessed 3 May 2016].
[274] Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*. pp.3, 17.
[275] Cropper, L. (2016). *EU-US Privacy Shield: The Article 29 Working Party raises its concerns*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/eu-us-privacy-shield-the-article-29-working-party-raises-its-concerns/ [Accessed 3 May 2016].

no longer than necessary to achieve the purpose for which the data were collected."[276] Additionally, the opinion states that the application of the purpose limitation principle[277] is unclear.[278]

Thirdly, the Article 29 Working Party has expressed major concerns about individuals' ability to invoke their rights. The ombudsperson mechanism provided by the EU – US Privacy shield is said to be too complex and therefore ineffective.[279] The Article 29 Working Party suggested the use of national DPA's as a point of contact when compensation is needed by EU data subjects.[280]

Fourthly, the Article 29 Working Party stated that the EU – US Privacy Shield allows for derogations for national security purposes and does not exclude the continued collection of massive and indiscriminate data.[281] The Article 29 Working Party reiterated that massive and indiscriminate collection of data can never be considered lawful by European data protection standards because of the lack of proportionality. Nevertheless, the Article 29 Working Party has stated that jurisprudence[282] on the collection of personal data with the purpose of battling crime is inconclusive and thus awaits the CJEU's decision on data retention expected in 2016.[283]

Aside from these concerns, the Article 29 Working Party has also stated the adequacy decision of the European Commission will need to be reviewed after the GDPR comes into force to confirm conformity with the higher level of data protection ensured by the GDPR.

Although this opinion is not binding to the European Commission, it carries a lot of weight. The Article 29 Working Party has made specific suggestions to improve the

---

[276] Article 29 Working Party, (2016). Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision. p.57.
[277] See also Section 2.2.5 of this chapter.
[278] Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*. pp.3, 24-25.
[279] Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*. pp.45-51, 57.
[280] Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*. p.27.
[281] Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*. pp.52-57.
[282] Joined cases *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Davis and Others,* C-203/25 and C-698/15 (CJEU).
[283] Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*. p.39.

agreement.[284] The overall consensus seems to be that the EU – US Privacy Shield still does not ensure an adequate protection of EU data subjects' data when transferred to the US.

2.3.2. National DPA's

The British DPA, the ICO, has issued a statement acknowledging the EU – US Privacy Shield is still unstable, but assuring organisations it will not use its enforcement powers in the foreseeable future. The Article 29 Working Party confirmed the use of binding corporate rules and model clauses were still valid, but the ICO urges organisations not to rush their decision about which mechanism to rely upon.[285]

On the opposing end, the French DPA, CNIL, and the German DPA's have started to question organisations on the alternative transfer mechanisms they rely on currently while awaiting the new agreement.[286]

3. Conclusion

While the data reform promised to strengthen individuals' rights, the end result is not as straightforward.

Firstly, The GDPR has certainly expanded individuals' right to erasure by giving it a legal basis and created additional protection for children. Additionally, it has created a stricter requirement for consent, but missed the opportunity to take it one step further and require explicit consent. The obligation to appoint a DPO and the addition of principles such as privacy by design, privacy by default and the accountability principle, are definite improvements. They are aimed at stimulating organisations to take privacy by heart. The most important motivator for organisations, however, will probably be the threat of administrative fines, which, as discussed, in turn might also have some negative effects.

---

[284] Cropper, L. (2016). *EU-US Privacy Shield: The Article 29 Working Party raises its concerns*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/eu-us-privacy-shield-the-article-29-working-party-raises-its-concerns/ [Accessed 3 May 2016]; Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*.
[285] Cropper, L. (2016). *EU-US Privacy Shield: The Article 29 Working Party raises its concerns*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/eu-us-privacy-shield-the-article-29-working-party-raises-its-concerns/ [Accessed 3 May 2016]; Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*.
[286] Cropper, L. (2016). *EU-US Privacy Shield: The Article 29 Working Party raises its concerns*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/eu-us-privacy-shield-the-article-29-working-party-raises-its-concerns/ [Accessed 3 May 2016]; Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*.

The conclusion on the GDPR can therefore not be one hundred percent positive or negative. It can still be critiqued on a number of issues, there does seem to be a willingness and a tendency to improve individuals' rights regarding their data. The differences between the European Commission's initial proposal and the final GDPR, however, show that the different interests at stake prevent some of the more impactful proposals.

Secondly, the EU – US Privacy Shield is criticised by many as being more of the same compared to the Safe Harbour Agreement. The draft adequacy decision as it is now, is still missing some crucial safeguards as mentioned by the Article 29 Working Party. It is, however, still possible some of the Article 29 Working Party's suggestions will be taken into account by the European Commission. If the final adequacy decision does not guarantee an adequate level of data protection it will be contested immediately, which might prompt an entirely new agreement.

In the following chapter Facebook's Terms of Service and Data Policy[287] will be discussed. Based on the analysis of Chapter III, Chapter IV will question how Facebook's practices might conflict with the existing and the future legal framework.

[287] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].

Chapter IV. Facebook

"Privacy is no longer a social norm."[288]

- MARK ZUCKERBERG[289]

1. Introduction

As of 30 September 2015, Facebook had over 1,5 billion users who logged in monthly. Over one billion of them log in daily.[290] Initially the social network was only available to students at Harvard. Later, this was expanded to anyone over the age of thirteen.[291] Since using Facebook is in essence free of charge, the users are the products that Facebook profits from. Every user essentially offers up a piece of their privacy to use Facebook. Facebook uses and sells this data to interested parties, to provide services such as targeted marketing.

The terms to which every user agrees are separated into multiple agreements. The three policies of interest for this paper are the Terms of Service, the Data Policy[292], and to a lesser extent the Cookie Policy[293]. Facebook's Terms of Service, as a basis for all other agreements, are roughly 10 000 words long.

A Facebook profile has started to play a significant role in how people communicate. Consequently, users, sometimes unknowingly, sign away a part of their right to privacy in order to enjoy these advantages. Facebook has recognised this issue and has made efforts to translate these terms into basic explanations about some of the most frequently asked questions, but on the other side it has continuously implemented further reaching rights to use users' data.

---

[288] Johnson, B. (2010). Privacy no longer a social norm, says Facebook founder. *The Guardian*. [online] Available at: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [Accessed 15 May 2016].

[289] "*Mark Zuckerberg is co-founder and CEO of the social-networking website Facebook, as well as one of the world's youngest billionaires."* Biography. (2016). *Mark Zuckerberg*. [online] Available at: http://www.biography.com/people/mark-zuckerberg-507402 [Accessed 15 May 2016].

[290] Facebook Investor Relations. (2015). *Facebook Reports Third Quarter 2015 Results - Facebook*. [online] Available at: http://investor.fb.com/releasedetail.cfm?ReleaseID=940609 [Accessed 5 May 2016].

[291] Clause 4 (5) Terms of Service. Age requirements may vary depending on the country.

[292] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].

[293] Facebook. (n.d.). *Cookies, Pixels & Similar Technologies*. [online] Available at: https://www.facebook.com/help/cookies/update [Accessed 5 May 2016].

2. Practices

2.1. How do users give their consent?

As an online social network, Facebook, in order to process personal data must justify this based on one of the legitimate grounds found in Article 7 of the Data Protection Directive. The type of justification Facebook can use depends on the data it collects. For example, the basic information needed to start up a Facebook profile can be deemed information necessary for the performance a contract as listed in Article 7 (b) Data Protection Directive.[294] Another example can be information processed to ensure system security, which can be collected based on Article 7 (f) Data Protection Directive, namely legitimate interest.[295] Anything outside of these purposes, however, can only be justified by consent, which, according to the Data Protection Directive[296], needs to be unambiguous.[297]

As discussed in Chapter III, the definition of consent will change under the GDPR. As Facebook relies quite heavily on consent as a justification for their practices, this will certainly impact them. While the Data Protection Directive still allowed implicit consent, this will no longer be possible under the GDPR. Not actively protesting new Terms of Service or the use of cookies, for example, will no longer constitute consent under the GDPR. Users will need to actively give their consent in order to justify Facebook's processing of their personal data. When it comes to sensitive personal data, explicit consent will be required, this was already the case under the Data Protection Directive and will therefore not have a huge practical impact. Facebook will have to keep in mind that the definition of sensitive personal data will be broader as it will include genetic and biometric data. They may come into contact with this kind of information through linked health-related applications.

Taken into consideration the fact that obtaining consent will become more difficult, it is worth mentioning that a Belgian report already questions the validity of the consent

---

[294] Van Eecke, P. and Truyens, M. (2010). Privacy and social networks. *Computer Law & Security Review*, 26(5), pp.535-546.
[295] Van Eecke, P. and Truyens, M. (2010). Privacy and social networks. *Computer Law & Security Review*, 26(5), pp.535-546.
[296] Art. 7 (a) Data Protection Directive.
[297] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.12. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

obtained by Facebook, as a justification for processing under the Data Protection Directive.[298]

Like the GDPR, the Data Protection Directive required consent to be given freely, specifically, informed and unambiguously.[299] The report questions whether the consent obtained by Facebook was given freely, whether it was specific, whether it was informed and whether it was unambiguous.

Firstly, the report questioned if the consent was given freely. The Article 29 Working Party has stated that freely given consent assumes that the consumer has a real choice and "*no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent."*[300] The report questions whether this is reconcilable with Facebook's dominant market position in addition to its all-or-nothing approach.[301] This stance has been confirmed by the Article 29 Working Party, stating that users should be able to use the social network regardless of the fact that they consent to, for example, behavioural advertising.[302] Additionally, the report criticises the fact that the Terms of Service extend this consent to all of Facebook's partner services, stating that Facebook "*effectively leverages its strong position as an online social network to legitimise the tracking an profiling of individuals' behaviour across services and devices"*[303]*.*

Secondly, the report questions whether the consent obtained by Facebook is specific as required under the Data Protection Directive. This means that the data subject must be able to ascertain for which purposes the processing will take place.[304] The report argues that

---

[298] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] pp.8, 13-17. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[299] Art. 4 (11) GDPR; Art. 2 (h) Data Protection Directive.
[300] Article 29 Working Party, (2011). *Opinion 15/2011 on the definition of consent*. p.11.
[301] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.14. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[302] Article 29 Working Party, (2011). *Opinion 15/2011 on the definition of consent*. p.18.
[303] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.15. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[304] Article 29 Working Party, (2011). *Opinion 15/2011 on the definition of consent*. pp.21-25.

Facebook's Data Policy[305] is anything but specific, stating vague purposes such as 'promote safety and security', or 'provide, improve and develop services'. On the contrary, Facebook makes an effort to inform users of the categories of data that will be shared when linking their Facebook account to an application. The extent of information other parties, such as third-party partners or customers, have access to, remains unclear, let alone who these other parties are exactly.[306]

Thirdly, the report questions whether the consent is informed. This conclusion is based primarily on the fact that the average user will never read the Terms of Service or Data Policy, even if they are not insurmountably long. The CJEU has ruled that simply linking to these terms proves insufficient with regards to consumer protection.[307] Data subjects have the right to be given a minimum amount of information as required by Article 10 of the Data Protection Directive, including information regarding the purposes of processing and the identity of people or organisation that will have access to the data, which as explained above is vague at best.[308]

Lastly, the report ascertains that the consent obtained by Facebook is not unambiguous. This means there can be no misunderstanding about the fact that the data subject has consented. As Facebook's default settings share data with 'friends of friends', and users need to take active steps to undo this, they have by definition not actively taken any steps to consent with these settings. Even though the Article 29 Working Party questioned this practice, the Data Protection Directive, still allows for consent to be implicit. This is not taken into account in the report. Their argument only stands true when the processing involves sensitive personal data and explicit consent is required.[309]

---

[305] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].
[306] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.15. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[307] *Content Services Ltd v. Bundesarbeitskammer* [2012]C-49/12 (CJEU), §50.
[308] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.16. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[309] Art. 8 (2) (a) Data Protection Directive.

2.2. Location Tracking

2.2.1. How does Facebook gather location data?

To its advertisers, Facebook states the following on how they gather information on the location of their users: *"Facebook uses information from multiple sources such as current city from profile, IP address, data from mobile devices if location services are enabled, and aggregated information about the location of friends."*[310]

While the current city mentioned on your profile and the IP address are logical sources of information, data from mobile devices and aggregated information through friends may be surprising to some users. In what follows we will discuss these last two sources.

Firstly, Facebook is able to track its users' location data through their smart devices. This is possible by using different sensors such as GPS, Wi-Fi, Bluetooth etc. If you do not want your device to send this kind of information to the organisations of the apps you use, it is possible to turn location sharing off on the device itself. This can be done for all apps or for each app individually.[311]

The Facebook mobile application requests the use of location data to use certain location-based services. The user must first allow the application access to the location data of their device to use these services. Once this authorization is given, however, there is no way to restrict it through further preferences or settings.[312] Facebook requires the user to make an "all or nothing" choice.

There is one service, however, that Facebook does not enable by default. This service, called "Nearby Friends", allows users to see which friends are nearby and get a notification

---

[310] Facebook. (n.d.). *How does Facebook know when people are in the locations I am targeting? - Help Center*. [online] Available at: https://www.facebook.com/business/help/133609753380850 [Accessed 19 April 2016]. Editing by author.

[311] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.73. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

[312] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.73. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

when someone is nearby.[313] This function remains active even when the application is not actively being used. There is, however, no guarantee that Facebook cannot use this information for other purposes. Facebook, for example, sells this knowledge for advertising purposes, by allowing advertisers to target specific audiences based on their location.[314]

Secondly, Facebook can gather location information on its users via information gathered through their friends. If a users' friend uploads photos of him, or checks him in, in certain locations, Facebook can use this shared location data.[315]

Even if a data subject turns of his location sharing on his smart device, it is likely that the data subject himself might be sharing location data unintentionally simply by using Facebook. For example, when uploading a photo taken with a smart device, it often contains metadata, including the location where the photo was taken. Inadvertently the user is sharing this information with Facebook.[316]

2.2.2. Applicable legislation

Under the current Data Protection Directive, the collection and use of location data is processing of personal data.[317] The Article 29 Working Party has also emphasized the delicate nature of location data[318], even though they do not fall within the definition of sensitive personal data.[319]

The Article 29 Working Party also states that location data should be deleted after a justified period of time. The location data cannot be retained longer than is necessary for its

---

[313] Facebook. (n.d.). *Nearby Friends | Facebook Help Center | Facebook*. [online] Available at: https://www.facebook.com/help/629537553762715/ [Accessed 19 April 2016].
[314] Facebook, "What option do I have when selecting people within a location", https://www.facebook.com/business/help/755086584528141 [last retrieved on 19 April 2016].
[315] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016]; See also Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.74. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[316] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.73. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[317] Article 29 Working Party, (2011). *Opinion 13/2011 on Geolocation services on smart mobile devices*. p.20.
[318] Article 29 Working Party, (2011). *Opinion 13/2011 on Geolocation services on smart mobile devices*. p.19.
[319] Art. 9 GDPR.

purpose and providers of geolocation applications must ensure that it is deleted at the appropriate time.[320] In 2013 Facebook's Data Policy stated that: "*we only keep it until it is no longer useful to provide your services"*[321], which is in line with the opinion of the Article 29 Working Party. It is interesting to note that, after its revision in 2015, the Facebook Data Policy no longer mentions limiting the retention of location data.

Belgian researchers concluded by saying that Facebook, to comply with the data protection legislation, should *"offer more granular in-app settings for sharing of location data, with all parameters turned off by default."*[322]

The GDPR, containing the privacy by default principle, confirms what these Belgian researchers said in 2015. As discussed under Section 1.6.1 of Chapter III, privacy by default requires that appropriate technical and organisational measures are put in place to ensure that only necessary personal data for each specific purpose of the processing will be processed.[323] This means that the collection of information will need to be looked at separately for each specific purpose. In the future, the storage of location data will require appropriate technical and organisational measures to ensure this data is kept no longer than necessary.

---

[320] Article 29 Working Party, (2011). *Opinion 13/2011 on Geolocation services on smart mobile devices*. p.19.

[321] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].
See also Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.74. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

[322] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.75. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

[323] Mahmood, S. and Power, L. (2016). *Getting to know the General Data Protection Regulation, Part 6 – Designing for compliance*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-6-designing-for-compliance/ [Accessed 4 May 2016].

2.3. Tracking of browsing activity

A group of Belgian researchers was asked by the Belgian Privacy Commission to prepare a technical report[324] on Facebook's tracking practice through social plug-ins[325]. Tracking is considered to be the "*collection of users' web browsing activities across different websites"*[326]. Their findings sparked a debate, and eventually even led to a court case. The case itself will be discussed under Chapter V. In this section we will look at the practice of tracking through social plug-ins and the conclusions from the technical report.

Facebook can track people through the use of social plug-ins. When visiting a site containing one of these social plug-ins, Facebook places a cookie in the data subject's browser. The fact that the Like Button is found on 32% of the top 10 000 sites shows that Facebook collects data on an enormous group of people.[327] It is not necessary for the data subject to interact with the social plug-in for information to be gathered.[328]

Facebook's Data Policy explains they can use the data collected through these social plug-ins to: provide, improve and develop services, communicate with you, show and measure ads and services and promote safety and security.[329] Facebook's Cookie Policy indicates information gathered through cookies can be used for: authentication, security

[324] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[325] Facebook Developers. (n.d.). *Social Plugins - Documentation - Facebook for Developers*. [online] Available at: https://developers.facebook.com/docs/plugins [Accessed 18 April 2016].
[326] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.2. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[327] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.2. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[328] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.90. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[329] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016]; Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.93. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

and site integrity, advertising, localisation, site features and services, performance and analytics & research.[330]

2.3.1. Which data subjects are affected?

The report analyses Facebook's tracking practice on two groups: (i) non-Facebook uses, (ii) Facebook users. The latter is divided into current Facebook users and Facebook users who have deactivated their account. The report concluded each abovementioned group was tracked by Facebook at one point or another.

Firstly, the report shows that non-Facebook users who visited a public Facebook page, without ever making an account, are tracked through cookies. These cookies gather information, such as the website visited, the browser used, the language preferences and the operating system.[331] The report also showed that Facebook places a cookie on certain non-Facebook pages, allowing them to track people even if they have never visited a Facebook page.[332] For example, a Facebook cookie was found on the third party website mtv.com, users who never visit a Facebook page, but do visit mtv.com will also be tracked. One of these cookie has a lifespan of two years, which means Facebook can collect this data as long as the data subject does not manually remove the cookie from his browser.[333]

Secondly, the report looks at Facebook users, differentiating between those who still have an account and those who have deactivated it. With regards to Facebook users another distinction must be made: whether the user is logged in or not. When a Facebook user remains logged in, eleven cookies are placed on the browser, one of which is used for advertising purposes.[334] These cookies are only removed after the browser, not the tab, is

---

[330] Facebook. (n.d.). *Cookies, Pixels & Similar Technologies*. [online] Available at: https://www.facebook.com/help/cookies/update [Accessed 5 May 2016].
[331] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.2. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[332] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.12. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[333] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.6. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[334] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] pp.13, 21. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].

closed.[335] As a logged in Facebook user, Facebook along with the information about the browser, website etc., will also receive the user's Facebook ID, allowing them to link the activity to a specific user.[336] When a Facebook user is logged out cookies are still placed and data is still collected. Logging out therefore does not stop Facebook from tracking a data subject's browsing activity.[337]

One would expect that deactivating your account ends this practice. The report, however, shows that deactivating an account does not remove these cookies and does not prevent Facebook from tracking your browsing activity.[338] The cookies placed collect the same information as they do with logged out Facebook users.[339] Facebook's Cookie Policy states that the tracking of non-Facebook users is necessary to ensure security.[340]

2.3.2. Opting out

Facebook responds to criticism by pointing out users and non-Facebook users have the possibility to 'opt out'.[341] Facebook therefore assumes everyone, by default, has implicitly consented, by not opting-out, even if they never accepted Facebook's Terms of Service.

The report conducted research to see if the opt-out method, as suggested by Facebook, eliminates all cookies. Again, a distinction was made between (i) people who do not have cookies in their browser, non-Facebook users who have never visited a Facebook page or a

---

[335] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.13. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[336] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.15. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[337] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] pp.15-17. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[338] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.18. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[339] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.18. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[340] Facebook. (n.d.). *Cookies, Pixels & Similar Technologies*. [online] Available at: https://www.facebook.com/help/cookies/update [Accessed 5 May 2016].
See also Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.98. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[341] Facebook. (n.d.). *Control the ads you see - About Advertising on Facebook*. [online] Available at: http://facebook.com/about/ads [Accessed 18 April 2016].

third party website containing a Facebook cookie, or logged out Facebook users who cleared their cookies after logging out, and (ii) people with cookies, i.e. everyone else.

People without cookies who used the European opt-out site ended up with an additional cookie to indicate the opt-out. However, after the opt-out procedure Facebook had again placed a cookie with a lifespan of two years in the user's browser. Both the opt-out cookie and the standard tracking cookie were sent to Facebook when subsequently visiting a website containing a social plug-in. Each visit to a site containing a plug-in can therefore still be linked by Facebook using the standard tracking cookie.[342] It is peculiar that this did not happen when opting out through a US or Canadian opt-out site. When opting out through these websites, only the opt-out cookie was placed with a lifespan of five years.[343]

People who still have cookies in their browser when opting out are also treated differently. Through the European opt-out site, Facebook again placed the opt-out cookie, but did not remove any of the other cookies it had previously stored in the browser. The researchers confirmed that when subsequently visiting sites containing a Facebook social plug-in, Facebook still received the uniquely identifying cookies after the opt-out. Even after logging out, this practice persists.[344] This time, when opting out through US or Canadian sites, the end result is the same; Facebook still tracks data subjects' browsing activity using social plug-ins.[345] In their response, Facebook promised that when a user opts-out they would no longer use the collected data for advertising purposes,[346] a fact which has not been confirmed independently.

---

[342] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.19. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[343] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.21. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[344] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.22. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[345] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] p.22. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[346] Facebook Newsroom. (2015). *Setting the Record Straight on a Belgian Academic Report*. [online] Available at: http://newsroom.fb.com/news/h/setting-the-record-straight-on-a-belgian-academic-report/ [Accessed 16 May 2016].

The report concludes that the opt-out method, as suggested by Facebook, does not stop tracking by Facebook. Facebook still collects information on its users regardless of whether they are logged in or not.[347]

2.3.3. Alternative ways of avoiding tracking

Data subjects who want to prevent being tracked can enlist other tools that limit tracking through social plug-ins.

A first example is the "Social Share Privacy Tool", which blocks the social plug-ins from loading until you actually want to use them. This tool is also endorsed by the French DPA, CNIL.[348] If a data subject uses Mozilla Firefox as a browser, they have the option of blocking third-party social plug-ins through their settings.[349] Additionally, there are several add-ons available to install in your browser to block these social plug-ins that allow Facebook to track data subjects' browsing activities, such as "Facebook Disconnect"[350], "Privacy Badger"[351] or "Ghostery"[352], as recommended by the Belgian DPA, the Belgian Privacy Commission.[353]

2.3.4. Applicable legislation

For starters, Facebook, as a data controller is obliged to comply with its obligations under the current Data Protection Directive.[354] Additionally, Article 5 (3) E-Privacy Directive requires prior consent for cookies placed via social plug-ins. There are two exceptions to this requirement: (a) when the sole purpose of the storage or access is the transmission of a communication, or (b) when the storage or access is strictly necessary in order to provide

---

[347] Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] pp.22-23. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].
[348] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.99. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[349] Mozilla Support. (n.d.). *Disable third-party cookies in Firefox to stop some types of tracking by advertisers | Firefox Help*. [online] Available at: https://support.mozilla.org/en-US/kb/disable-third-party-cookies. [Accessed 7 May 2016].
[350] Available at https://disconnect.me.
[351] Available at https://www.eff.org/privacybadger.
[352] Available at https://www.ghostery.com.
[353] Belgian Privacycommission.be. (n.d.). *Ik ben een internetgebruiker, hoe kan ik mij beschermen tegen tracking door social plug-ins? | Privacycommissie*. [online] Available at: https://www.privacycommission.be/nl/ik-ben-een-internetgebruiker-hoe-kan-ik-mij-beschermen-tegen-tracking-door-social-plug-ins [Accessed 18 Apr. 2016].
[354] Art. 6 (1) (c) Data Protection Directive.

an information society service explicitly requested by the user. Exception (b) is of particular importance for an online social network such as Facebook.

Article 29 Working Party has clarified the meaning of the latter exception. It stated that exception (b) cannot be used to justify tracking via social plug-ins of non-members. The same applies to users when they are not logged in.[355] The Article 29 Working Party stated the following: *"Social networks that wish to use cookies for additional purposes (or a longer lifespan) beyond CRITERION B have ample opportunity to inform and gain consent from their members on the social network platform itself."*[356]

On the impaired functioning of the opt-out mechanism, the Article 29 Working Party stated that an opt-out mechanism cannot be considered an adequate mechanism to obtain informed consent from the average user, especially in relation to behavioural advertising.[357]

When the GDPR becomes applicable, Facebook will need to rethink this practice. The GDPR recognizes the principles of privacy by design and privacy by default. This means that privacy will need to become a concern throughout every process and should be guaranteed by default. This means, for example, the amount of data collected should be limited to what is necessary and the period of storage should be limited to what is necessary.[358]

2.4. Advertising Practices

As a multinational company, Facebook gets most of its profits through advertising.[359] The most valuable component of Facebook's business model is therefore comprised of the amount of Facebook users and the amount of information, such as location data, they share. Users may not be paying for the service in the traditional sense, but they are giving up private information in exchange for using Facebook. This practice has created a new, more personal way for advertisers to target their clients. Facebook's Terms of Service state the following on advertisements and other commercial content served or enhanced by Facebook:

---

[355] Article 29 Working Party, (2012). *Opinion 04/2012 on Cookie Consent Exemption*. p.9.
[356] Article 29 Working Party, (2012). *Opinion 04/2012 on Cookie Consent Exemption*. p.9.
[357] Article 29 Working Party, (2010). *Opinion 2/2010 on online behavioural advertising*. p.15.
[358] Section 1.6.1 of Chapter III.
[359] Facebook Investor Relations. (2015). *Facebook Reports Third Quarter 2015 Results - Facebook*. [online] Available at: http://investor.fb.com/releasedetail.cfm?ReleaseID=940609 [Accessed 5 May 2016].

"Our goal is to deliver advertising and other commercial or sponsored content that is valuable to our users and advertisers. In order to help us do that, you agree to the following:

1. *You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.*

2. *We do not give your content or information to advertisers without your consent.*

3. *You understand that we may not always identify paid services and communications as such."*[360]

Facebook uses a method called 'behavioural advertising' to target advertisements to specific audiences. Additionally, Facebook uses its users' friends to advertise products or services through 'social advertisements' and 'sponsored stories'. In what follows each of these methods will be discussed.

2.4.1. Behavioural advertising

By default, Facebook is allowed to use the information it collects to target advertisements to specific audiences.[361] It combines the data it collects through Facebook with data collected from third parties or other Facebook services and companies.[362]

(i) Combination with data from third parties

The first way in which Facebook combines its data with data gathered from third parties is the "custom audience" feature. When advertisers buy advertisements on

[360] Clause 9 Terms of Service.
[361] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.38. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[362] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.55. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

Facebook they are able to select custom audiences. This allows advertisers to reach their own customers through Facebook.[363] In this case Facebook combines its own user information with the information provided by the advertiser (third party) to target advertisements. Advertisers can provide information from their own customer lists, information on people that visit their website or use their mobile application.[364]

A second way in which Facebook combines its data with data collected from third parties is the "lookalike audiences" feature. This allows advertisers who have set up a custom audience to target other Facebook users with a similar profile. Firstly, Facebook analyses the users from the custom audience and looks for common patterns and afterwards, based on these patterns, it looks for similar profiles. This can be based on information such as demographics, location, interests etc.[365]

After creating a custom audience or a lookalike audience, advertisers can further specify the audience they would like to reach. Advertisers are given several targeting options.[366]

---

[363] Facebook. (n.d.). *What is a custom audience? - Help Center*. [online] Available at: https://www.facebook.com/help/341425252616329 [Accessed 5 May 2016].

[364] Facebook. (n.d.). *What is a custom audience? - Help Center*. [online] Available at: https://www.facebook.com/help/341425252616329 [Accessed 5 May 2016].

[365] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] pp.63-64. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

[366] Facebook. (n.d.). *Audience Targeting Options - Help Center*. [online] Available at: https://www.facebook.com/help/633474486707199 [Accessed 21 April 2016].
See also Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] pp.61-62. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

Figure 1. Facebook's basic targeting options[367]

Firstly, advertisers can target audiences based on location. Advertisers can even specify whether they want to reach people living in a certain location, people who recently visited a certain location or people traveling in a certain location.[368] A second option is targeting based on more demographics, including education level, specific schools, fields of study etc.[369] A third option is to target audiences based on age and gender.[370] A fourth option is to target people based on their interests. Advertisers could for example target their advertisement to people interested in sports. Facebook will look for this interest via things people share on their timelines, apps used, pages liked and other activities on *and off* Facebook.[371] A fifth option is targeting based on preferences to select audiences based on certain purchase behaviours or travel preferences. [372] Finally, Facebook provides the option to target audiences based on connections, this allows advertisers to target people who already have a connection with them or vice versa.

---

[367] Facebook. (n.d.). *Audience Targeting Options - Help Center*. [online] Available at: https://www.facebook.com/help/633474486707199 [Accessed 21 April 2016].
[368]Facebook. (n.d.). *What options do I have when selecting people within a location? - Help Center*. [online] Available at: https://www.facebook.com/help/755086584528141 [Accessed 21 April 2016].
[369] Facebook. (n.d.). *How do I target education levels, specific schools, fields of study or specific graduation years? - Help Center*. [online] Available at: https://www.facebook.com/help/227971680551772 [Accessed 21 April 2016].
[370] Facebook. (n.d.). *Can I target my ad to people based on their age and gender? - Help Center*. [online] Available at: https://www.facebook.com/help/813939365351532 [Accessed 21 April 2016].
[371] Facebook. (n.d.). *What is interests targeting? - Help Center*. [online] Available at: https://www.facebook.com/help/188888021162119 [Accessed 21 April 2016].
[372] Facebook. (n.d.). *What are audience behaviours? - Help Center*. [online] Available at: https://www.facebook.com/help/243268465859743 [Accessed 21 April 2016].

Additionally, they can target both groups and friends of people who are connected to the advertiser.[373]

(ii) Combination with data from other Facebook services and companies

In 2013, Facebook acquired an ad serving, management and measurement platform, called Atlas. Its goal was to provide advertisers with a more complete view of their advertisement campaigns across devices, and to connect online advertising with offline purchase behaviour. This service is meant to provide advertisers with tangible evidence of the positive impact of digital advertising on offline sales.[374]

To allow advertisers to target audiences across different devices, Atlas will link data subjects to devices. It remains unclear which information will be used to do this.[375] Via Atlas, Facebook will bring together information gathered through Facebook itself, with information gathered across other Facebook platforms and services, such as Instagram.[376]

Instinctively one could think behavioural advertising qualifies as profiling. This practice will, however, not fall within the definition of profiling in the GDPR.[377] As discussed in Section 1.3.4, privacy lawyers have theorized that targeted advertisements do not have a significant impact on a data subject's life and therefore do not qualify as profiling.

---

[373] Facebook. (n.d.). *What is connections targeting? - Help Center*. [online] Available at: https://www.facebook.com/help/186282224754628 [Accessed 21 April 2016].
[374] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] pp.65-66. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[375] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.66. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[376] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.67. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[377] Art. 4 (4) GDPR.

2.4.2. Advertisements with social actions

"Your profile picture or name may be paired with an ad to show your activity on Facebook (ex: if you follow the Starbucks Page). Keep in mind that your name and profile picture will only appear to the people who have permission to view your Page likes."[378]

Facebook's Terms of Service allow Facebook to use a users' name, profile picture, content and information in connection with commercial, sponsored or related content.[379] If a user has specified a specific audience for this information through their privacy settings, Facebook is obliged to respect this.

A social advertisement is a regular advertisement that mentions a user's name and the fact that this user liked a particular brand. Social ads appear in the sidebar (figure 2). A sponsored story on the other hand appears in the users' newsfeed (figure 3).

Figure 2. Social Ad[380]

[378] Facebook. (n.d.). *Does Facebook use my name or photo in ads? - About Facebook Ads | Facebook Help Center*. [online] Available at: https://www.facebook.com/help/769828729705201/ [Accessed 5 April 2016].
[379] Clause 9 (1) Terms of Service.
[380] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.38. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

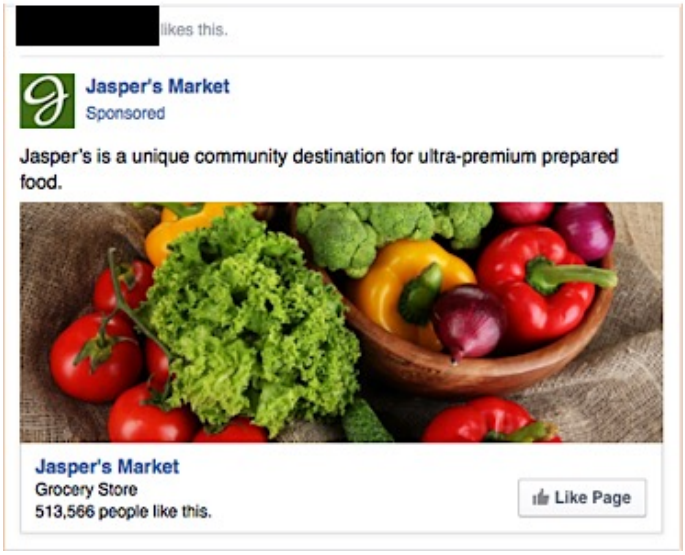

Figure 3. Sponsored Story[381]

Through their settings, users can opt out of these ads. As the GDPR will require companies to adhere to the principle of privacy by default,[382] the opt-out mechanism can be questioned. To provide the maximum amount of protection of users' right to privacy, privacy by default requires a system where users actively opt in to these services. This is also in line with the new definition of consent, which requires an affirmative action from the data subject. In cases were sensitive information is processed, users will even have to give explicit consent.

Additionally, privacy by default requires that only the information strictly necessary for each specific purpose is processed. The necessity test applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility in light of the purpose.[383] With regard to the purpose of the processing, Facebook only gives vague information to its users about the purpose. We will discuss this issue in the next section.

[381] Facebook Ad Settings. (n.d.). *Facebook*. [online] Available at: https://www.facebook.com/settings?tab=ads [Accessed 14 May 2016].
[382] Art. 25 (2) GDPR.
[383] Art. 25 (2) GDPR.

2.4.3. Vague and non-specific Terms of Service and Data Policy

One of the major issues with Facebook's Terms of Service and Data Policy is that they use non-restrictive language. Both the current Data Protection Directive[384] and the future GDPR[385] require organisations to inform the data subjects on the purpose of the collection of their data. Facebook's Data Policy only sets out four main and vague purposes applicable to the sharing and/or combining of all personal data collected. There is no differentiation between specific categories of data.[386]

Additionally, the Data Policy contains a variety of catch-all provisions allowing Facebook to share and combine all the data it has gathered. When it is unclear whether specific, more protecting, provisions are applicable, the user can only fall back on these catch-all terms providing extensive rights to Facebook.[387]

Moreover, Facebook determined the categories of parties they can share users' data with. In doing so, the Terms of Service use a range of terms, which can result in confusion.[388] Some of the terms used are: third parties, advertising, measurement or analytics partners, providers of integrated third-party features, partners who globally support our business, service providers, vendors, third-party companies, third-party customers, third-party partners etc. This seems irreconcilable with the GDPR's provision that requires organisations to use clear and understandable language. The use of several confusing and conflicting terms will therefore conflict with data subjects' right to be informed.

---

[384] Art. 10 Data Protection Directive.
[385] Art. 13 (1) (c) GDPR.
[386] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016]; Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] pp.68-69. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[387] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016]; Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.69. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[388] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.69. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

2.5. The licensing of users' content

When signing up to Facebook and agreeing to the Terms of Service, users grant Facebook a license to the content they place online. This content, such as photos and videos, is automatically protected by intellectual property rights.[389] While the license is subjects to the users' privacy settings, it is formulated incredibly broad.

Firstly, the license granted to Facebook is non-exclusive, which means users can still use and exploit their own content. Secondly, the license granted to Facebook is worldwide, which means Facebook can use the users' content worldwide. Thirdly, the license can be transferred and sublicensed, which means Facebook can authorize a third party to use its users' content. Fourthly, the license is given royalty free, which means users can never claim any of the profits Facebook makes from using, transferring or sublicensing the content.

This practice, however, is not subjected to data protection laws. It is subjected to intellectual property law. The license is subject to the rules of copyright law, which are not harmonized by European law. To know whether or not this license is valid, one must look at the national copyright law.

In Germany, courts have already investigated this license in 2012.[390] German law requires that no more rights are granted than necessary for the intended purpose.[391] This principle, also known as the "doctrine of intended purpose", determines that the scope of the license needs to be determined in light of the specific purpose of the agreement. The Berlin District Court decided that an automatic, worldwide license granted by simply accepting the Terms of Service was invalid and declared it not enforceable. The Berlin District Court held that: "*such a broad transfer contradicts the core idea of the doctrine of intended purpose."*[392]

---

[389] Clause 2 (1) Terms of Service.
[390] Landgericht Berlin, Urtail vom 6. März 2012, (16 O 551/10), accessible at http://openjur.de/u/269310.html.
[391] Art. 31 (5) Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das durch Artikel 7 des Gesetzes vom 4. April 2016 (BGBl. I S. 558) geändert worden ist. (German Copyright Act).
[392] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.79. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

Aside from copyright law, this license has also been called into question through the Article 3 of the Unfair Contract Terms Directive.[393] Some legal scholars have questioned whether the license does not create a significant imbalance in the parties' rights and obligations.[394]

Even though this issue might be considered a privacy issue by the average user, we will not go into further detail as it does not pertain to the data protection law and would therefore take us beyond the scope of this dissertation.

3. What rights do users have and are they effective?

The GDPR was meant to strengthen and broaden data subjects' rights. In this section we will discuss the rights insofar as they are relevant for Facebook users and if they have the ability to exercise these rights effectively.

One major change in the GDPR, which applies to all of the rights we will discuss in this section, is the introduction of fines as discussed in Section 1.8 of Chapter III.[395] These fines will give the national DPA's more powers regarding the enforceability of data protection laws.

3.1. Right of access

Both the Data Protection Directive[396] and the GDPR[397] give data subjects the right to freely exercise their right of access. Facebook has put in place a mechanism for users to download the information Facebook has collected about them.[398] The problem with this

[393] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *O.J.* L-95, 21 April 1993, pp. 29-34.
[394] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.45. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[395] Art. 83 (5) (b) GDPR.
[396] Art. 12 Data Protection Directive.
[397] Art. 15 GDPR.
[398] Facebook. (n.d.). *How can I download my information from Facebook? | Facebook Help Center | Facebook.* [online] Available at: https://www.facebook.com/help/212802592074644 [Accessed 30 April 2016]; See also Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.106. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

mechanism, is that it only provides users with a fraction of the information actually held by Facebook.[399]

Austrian activist, Maximilian Schrems, has addressed this issue, and has written an informal manual for Facebook users on how to gain access to the entirety of their data.[400] The first recommended step is to send an e-mail to Facebook, which will result in the following standard reply, referring the data subject to the abovementioned mechanism:

> *"(…) Thank you for contacting us to make a data request. You can access your data on Facebook in several ways. First, you can access your personal data from your account (ex: on your timeline or in your activity log). Second, we provide a tool that allows you to download a copy of your account data. This tool is available from the Account Settings page. (…)"*

As this reply does not give the data subjects the right of access as provided by the GDPR, or the current Data Protection Directive, data subjects are encouraged to file a complaint with the Irish DPA, as this is where Facebook's subsidiary is located.[401] At this time, the Irish DPA is no longer processing these complaints. This inactivity is a blatant disregard to Facebook users' right of access. As a result, the final option for Facebook users to exercise their right of access effectively is to file a purely political complaint with the European Commission against the Republic of Ireland for non-enforcement of EU law. As this practice is already non-compliant with the current Data Protection Directive, it will remain illegal under the GDPR.

3.2. Right to be informed

Under the Data Protection Directive, data controllers were obliged to inform data subjects about the identity of the controller and the purpose of the processing[402]. Member states were allowed to expand this obligation insofar as it was necessary to guarantee fair processing in a specific situation. This supplemental information could pertain to the recipients or categories of recipients of the data subjects' data, the existence of the right of access, the right to be rectify and others.[403] Several member states, including Belgium[404],

---

[399] Data Protection Commissioner, (2012). *Facebook Ireland Limited – Report of Re-Audit*. p.22.
[400] Europe versus facebook. (n.d.). *Get Your Data*. [online] Available at: http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html [Accessed 14 May 2016].
[401] Europe versus facebook. (n.d.). *Get Your Data*. [online] Available at: http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html [Accessed 14 May 2016].
[402] Art. 10 and 11 Data Protection Directive.
[403] Art. 10 (c) Data Protection Directive.

have used this option. Facebook's Data Policy is supposed to inform Facebook users as required by the Data Protection Directive.

Firstly, the Data Policy identifies Facebook's establishment in Ireland, Facebook Ireland Ltd., as the data controller for Facebook users outside of the US or Canada.[405]

Secondly, the Data Policy also provides a broad overview of the different purposes.[406] As discussed in Section 2.4.3, however, this overview is vague and non-specific. It pertains to all data collected by Facebook and therefore does not make it possible to determine the specific purpose for the collection of specific data. The Data Policy is written in a very non-restrictive way, only giving examples of possible processing operations, but not limiting them. This practice has already been criticised in an evaluation of Google's privacy policy: "*Google should avoid indistinct language such as "we can" / "we may …", but rather say "if you use services A and B, we will …"."*[407] These phrases are used abundantly in Facebook's Data Policy.[408] As the Data Protection Directive specifically requires the limitation of the purpose of the processing of data to be specific[409], the vague and broad descriptions employed by Facebook cannot be considered to be in line with the Data Protection Directive.[410]

Lastly, as some countries in Europe might require a wider range of information to be provided, we will briefly look at the information provided in regard to (i) the recipients or

---

[404] Art. 9, §1 Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 13 maart 1993. Hereinafter: Belgian Privacy Act.
[405] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].
[406] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].
[407] Article 29 Working Party, (2014). *Letter to Larry Page. Google Privacy Policy - Appendix*. p.2; See also CNIL, (2012). *CNIL Review of Google's New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data across Services*. p.2, and College Bescherming Persoonsgegevens, (2013). *Investigation into the Combining of Personal Data by Google - Report of Definitive Findings*. Den Haag, pp.66-68.
[408] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016]; Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] p.104. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[409] Art. 6 (1) (b) Data Protection Directive; See also Article 29 Working Party, (2013). *Opinion 03/2013 on Purpose Limitation*. pp.15 *et seq*.
[410] Article 29 Working Party, (2013). *Opinion 03/2013 on Purpose Limitation*. p.16; See also Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.104. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

categories of recipients of data, (ii) the categories of data that are processed and (iii) the data subjects' rights. In Section 2.4.3 the description of recipients of data have already been discussed: Facebook uses a splatter of different terms, resulting in confusing and misleading information. Furthermore, Facebook does not provide a clear overview of all the categories of data it collects.[411] Lastly, Facebook's Data Policy does not refer to any of the rights data subjects are entitled to.[412]

As these practices were already questionable under the Data Protection Directive, this will also be the case under the GDPR. The GDPR will now grant a harmonized right to be informed across Europe. Additionally, the principle of transparency in the GDPR requires this information be easily accessible, easy to understand and clear and plain language should be used. This conflicts with the confusing way the Data Policy is currently drafted.

3.3. Right to object

Through their privacy settings, Facebook offers users the possibility to object to the processing of their data by determining the audience[413]. There is, however, no simple way to object to the processing of data for advertisement purposes. Facebook only lets users opt out of socials ads, but does not let users opt out of sponsored stories. With regards to advertising based on activities on Facebook, monitored through tracking, Facebook does not provide an opt-out option on their site, but refers users to an opt-out mechanism. As discussed in Section 2.3.2, research has shown this opt-out mechanism does not actually prevent Facebook from placing a tracking cookie in the users' browser, making it ineffective. Additionally, this mechanism does not provide for an effective right to object as the process is quite long and needs to be repeated on every device.[414]

---

[411] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] pp.104-105. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

[412] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].

[413] The audience can be set to: friends, friends of friends or public.

[414] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] pp.107-108. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

The GDPR will offer data subjects more grounds to object to the processing of their data, more specifically in the case of direct marketing.[415] Additionally, the GDPR will require Facebook to explicitly inform data subjects about the existence of this right at the latest in the first written communication.[416] The communication of this right must be clear and separate from any other information.

3.4. Right to erasure (Right to be forgotten)

Facebook's Data Policy does not explicitly inform Facebook users of their right to erasure.[417] They do offer two ways to delete information: (i) delete the information manually through the activity log on the users' profile, or (ii) delete your account.[418] The Data Policy also states that when using option (i), information will still be stored *"as long as it is necessary to provide products and services to you and others"*[419]. When opting to delete your account, Facebook promises to delete the things posted by the Facebook user, such as photos or status updates. The Data Policy does not, however, mention anything about the erasure of chat logs, location data or behavioural data.[420] The Data Policy only mentions that information associated with a Facebook user's account will be kept until the account is deleted. It is unclear what "information associated with the account" includes.[421]

The Data Policy and the Terms of Service state clearly that only information posted by the Facebook user himself, will be deleted.[422] The deletion of one's account does not have any consequences for data about the data subject posted by others. While the Data Policy does not contain a referral to the data subjects' right to erasure regarding this type of data, it

---

[415] Art. 21 (2) - (3) GDPR.
[416] Art. 21 (4) GDPR.
[417] Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].
[418] Section IV Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].
[419] Section IV Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].
[420] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.108. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].
[421] Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3*. [online] p.109. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016]; See also Data Protection Commissioner, (2012). *Facebook Ireland Limited – Report of Re-Audit*. p.42.
[422] Clause 2 (2) Terms of Service; Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].

does offer a tool to request removal for privacy law reasons. This tool, however, only allows the Facebook user to request the removal of pictures. This is in stark contrast with the right to erasure which applies to any type of personal data.[423]

Article 12 of the Data Protection Directive already contained a right to erasure for data that was no longer necessary for the specified purpose. When the CJEU recognised the right to be forgotten as a principle, this principle needed to be implemented in the GDPR. As discussed in Section 1.5.2.1 of Chapter III, the right to be forgotten will offer a broader spectrum of grounds for individuals to request the erasure of their data. Since this practice was already questioned under the Data Protection Directive, it will remain incompatible with the GDPR.

[423] Art. 17 (1) GDPR.

Chapter V. Belgian Privacy Commission v. Facebook

"Facebook is the social network par excellence which almost half of all Belgians are a member of. The way in which these members' and all Internet users' privacy is denied calls for measures. With this recommendation we have taken a first step towards Facebook and all Internet stakeholders who use Facebook, in order to ensure they start working in a privacy-friendly way. It's bend or break."[424]

- WILLEM DEBEUCKELAERE[425]

Whether you are a user of Facebook or not, every third party site containing a "like" or "share" plug-in places a cookie from Facebook in your browser. This cookie allows Facebook to track your browsing activity on every site you visit. As Facebook users implicitly consent to this practice by joining Facebook, this could not be challenged by the Belgian Privacy Commission. The practice, however, of tracking people who do not use and have never used Facebook, was challenged in court by the Belgian Privacy Commission.[426]

In this chapter we will firstly review the facts of the case, afterwards we will look at the claims of both parties and the decision of the Belgian Court of First Instance. Lastly, we will examine whether the data protection reform has addressed the concerns posed by the Belgian Privacy Commission.

1. Facts

Both Facebook Inc., established in the US, Facebook Ireland Ltd. and Facebook Belgium SPRL were defendants in this case. Facebook Ireland, incorporated in Ireland, offers Facebook as a service to users in Europe. European Facebook users therefore do not enter into a contract with Facebook Inc. Facebook Belgium SPRL was incorporated in Belgium in 2001 to ensure relations with the public administration and lobbying.

---

[424] Belgian Privacy Commission, (2015). *On 13 May the Belgian Privacy Commission adopted a first recommendation of principle on Facebook.* [online] Available at: https://www.privacycommission.be/en/news/13-may-belgian-privacy-commission-adopted-first-recommendation-principle-facebook [Accessed 15 May 2016].

[425] Willem Debeuckelaere is the president of the Belgian Privacy Commission.

[426] Belgian Privacy Commission, (2015). *The judgment in the Facebook case*. [online] Available at: https://www.privacycommission.be/en/news/judgment-facebook-case [Accessed 4 May 2016].

Following the revision of Facebook's Terms of Service in 2015, the Belgian Privacy Commission approached a team of researchers. Their report, published on 31 March 2015, found that Facebook also processes personal data of data subjects who have never had a Facebook account.[427] This investigation prompted extensive correspondence between the Belgian Privacy Commission and Facebook. During this time, Facebook stated that Facebook Ireland Ltd. should be considered to be the data controller regarding European Facebook users. Additionally, Facebook rejected the applicability of Belgian privacy laws and consequently, the competence of the Belgian Privacy Commission. Facebook argued that the only competent DPA in Europe was the Irish DPA. Lastly, Facebook stated that sensitive personal data is not used for targeted advertising.

The Belgian Privacy Commission issued a recommendation relating to the use of social plug-ins and cookies of Facebook.[428] The Belgian Privacy Commission stated that Belgian privacy laws were applicable to this practice and that it was competent regarding the tracking of the browsing activity of Belgian internet users by Facebook. It also found the practice of tracking of the browsing activity through cookies of users who do not have a Facebook account, a violation of Belgian privacy law. The Belgian Privacy Commission subsequently ordered Facebook to refrain the use of long-life[429] and unique identifier cookies with regards to non-Facebook users.

The Belgian Privacy Commission served notice of default to Facebook Inc. and Facebook Belgium SPRL for violations of Belgian Privacy Act and Article 129 of the Act of 13 June 2005 on electronic communication. Both parties remained firm in their positions, which resulted in the initiation of summary proceedings before the Dutch-Speaking Court of First Instance in Brussels by the President of the Belgian Privacy Commission, Willem Debeuckelaere.

Four major issues were addressed by the Court: (i) the competence of the Belgian courts, (ii) whether or not there was processing of 'personal data', (iii) whether or not there was urgency, and lastly (iv) whether or not the Belgian Privacy Act was violated.

---

[427] For more information about the report: see Section 2.3 of Chapter IV.
[428] Belgian Privacy Commission, (2015). *On 13 May the Belgian Privacy Commission adopted a first recommendation of principle on Facebook.* [online] Available at: https://www.privacycommission.be/en/news/13-may-belgian-privacy-commission-adopted-first-recommendation-principle-facebook [Accessed 15 May 2016].
[429] As discussed in Section 2.3.1 of Chapter IV, some cookies have a lifespan of two years.

2. Claims of the parties

2.1. Competence of the Belgian Courts

The defendants argued Facebook Ireland Ltd. is the sole contractual party in regard to European Facebook users and is the only legal entity controlling the personal data of European internet users. The defendants therefore argued that the Belgian courts were not competent as only the Irish courts have jurisdiction regarding this case.[430]

This case was a landmark case as a national court determined it was competent to judge on this issue. This issue had been contested by Facebook for years based on the fact that their main European headquarters is based in Ireland. Belgium's situation was unique in this aspect, as Facebook had a small subsidiary based in Belgium for lobbying activities. Facebook argued this Belgian subsidiary never handled any personal data, and that the handling of personal data happened solely by the company based in Ireland. The Court agreed with the Belgian Privacy Commission referring to the *Costaja v. Google* case from 2014.[431] In this case the CJEU ruled that if there is a local establishment (*in casu* Facebook Belgium SPRL) and the activities of this establishment are inextricably linked to the activities of the data controllers, the local law is applicable (*in casu* Belgian law).[432] The Court stated the following:

> *"That Facebook Belgium itself does not process the personal data or that it is said not to conclude contract with advertisers, is irrelevant. The determining factor for the application of Article 4.1.a) of Directive 95/46/EC is not based on that, but on the finding that the activities of Facebook Belgium are therefore also inextricably linked to the activities of the operator of the social network site."*[433]

This reasoning also applied in this case, as Facebook Belgium SPRL performs lobbying activities in Belgium for the Facebook group and is involved in both marketing activities and

---

[430] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, pp.3-4.
[431] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited* 15/57/C (Dutch Speaking Court of First Instance Brussels 2015), p.14.
[432] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González* [2014]C-131/12 (CJEU), §52 - 57.
[433] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.16.

the selling of advertisement space, activities inextricably linked to the activity of the data controller.[434]

2.2. Claims relating to fundamental rights and freedoms are always urgent

In accordance with Belgian law[435], there is urgency when *"the fear of damage of a certain scope, or of serious inconvenience makes it necessary to take an immediate decision"*[436]. The Belgian Privacy Commission based its argument on the fact that claims related to the protection of basic rights and freedoms are always considered urgent as they concern the fundamental rights and freedoms of the entire society. The preamble of the Data Protection Directive shows that its aim is the protection of the right to privacy as a fundamental right.[437]

Additionally, the Belgian Privacy Commission argued that this case concerns millions of people as the plug-ins and cookies can be found on millions of websites across the internet. For example, Facebook's "Like"-button, one of the most popular plug-ins, can be found on no less than 32% of the 10 000 most visited websites.[438] This practice gives Facebook access to sensitive personal data such as information related to health, sexual, religious or political preference.[439]

As these plug-ins can be found on all types of websites, it is nearly impossible for an internet user not to come into contact with them at one point or another, resulting in the placement of a Facebook tracking cookie.

2.3. This case concerns the "processing" of "personal data"

Facebook argued the collected data could only lead to the identification of a computer, and not an individual data subject.[440] Through the tracking cookie Facebook places in data subjects' browser, it gathers information that uniquely identifies the internet browser of an

---

[434] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.15.
[435] Art. 584, §1 Gerechtelijk Wetboek, *BS* 31 oktober 1967, p.11360. (Belgian Judicial Code); Court of Cassation, 21 May 1987, *Pas*. 1987, I, 1160.
[436] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.18.
[437] Recital 10 Data Protection Directive.
[438] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.9.
[439] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.19.
[440] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.21.

internet user. Facebook, however, also gathers information, such as an IP address, that can directly or indirectly identify individuals.

While there was discussion on whether or not the definition of personal data encompasses an IP address, both the CJEU[441] and the Article 29 Working Party[442] have stated an IP address should be considered as personal data since it allows users to be uniquely identified. Furthermore, Facebook inadvertently confirmed this with their argument that cookies also serve a security purpose in determining who can access Facebook, implying they can identify individuals.[443] This argument will be discussed in Section 2.4.1 of this chapter.

As Facebook automatically processed the IP addresses, the Court decided this constituted the processing of personal data subject to the Belgian Privacy Act.

2.4. The Belgian Privacy Act was violated

2.4.1. Violation of Article 4, §1, 1° and 2° Belgian Privacy Act

2.4.1.1 Facebook did not obtain unambiguous, informed consent

The Irish DPA had previously argued that some cookies are not subject to the required unambiguous consent as they are necessary to provide a service.[444] Security cookies belong to this category. These cookies, however, have to be deleted at the end of every session, which does not happen to the tracking cookie as it remains in the data subject's browser for a period of two years.[445]

Facebook argued it obtained consent through the following steps. When visiting a Facebook page for the first time, a non-Facebook user will see a banner alerting them to the use of cookies. At this time no cookie is placed yet. The banner links to an explanation about the use of cookies, but this explanation does not mention the tracking cookie specifically. Only if a user continues to another Facebook page, such as the Terms of Service, a cookie

---

[441] *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011]C-70/10 (CJEU), §51.
[442] Article 29 Working Party, (2007). *Opinion 4/2007 on the concept of personal data.* pp.16-17.
[443] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.22.
[444] Data Protection Commissioner, (n.d.). *Guidance Note on Data Protection in the Electronic Communications Sector*. p.3.
[445] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.24.

will be placed. Facebook argues, at this point, the internet user has been informed of the use of cookies and has therefore unambiguously consented by continuing to use Facebook. Similarly, when a non-Facebook user clicks on a Facebook plug-in, such as a Like-button, outside of Facebook no cookie is placed. When the user, however, clicks cancel, a cookie is placed.[446]

The Belgian Privacy Commission argued that the fact that an internet user visited a Facebook page once, cannot be considered as consent to Facebook's Terms of Service.

With regard to Facebook users, the Court concluded it can be assumed they have implicitly, but unambiguously consented to Facebook's use of cookies. With regard to internet users who have never had a Facebook account the Court concluded that this practice did not comply with the required unambiguous, informed consent[447]. In the first case, a user, who, for example, goes on to read the Terms of Service, is still gathering information. In the second case, an interaction such as clicking cancel indicates the wish of the user not to use the service.[448]

2.4.1.2 No other grounds for processing were applicable

The Court concluded that Facebook could not rely on consent and the processing of data subjects therefore seemingly violated Article 4, §1, 1° and 2° of the Belgian Privacy Act. To conclude a violation, however, the Court first had to investigate whether any other grounds for processing[449] could be invoked.

Firstly, as mentioned in Section 2.3 of this chapter, Facebook tried to argue that these cookies play a crucial role in securing the personal data of their users as required by the Belgian Privacy Act[450]. The Court rejected this argument stating that: "*This would create a completely absurd situation in which Facebook users have to grant explicit consent to the processing of their personal data, and non-users of Facebook – without having granted any consent – would have to tolerate that their personal data are also processed to secure the personal data of others. This is obviously impossible: every data subject must be able to consent*

[446] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.24.
[447] Art. 5 (a) Belgian Privacy Act.
[448] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.24.
[449] Art. 5 Belgian Privacy Act.
[450] Art. 16, §4 Belgian Privacy Act.

to the processing of his personal data himself."[451] Moreover, the Court even called the processing of personal data of non-Facebook users entirely excessive, excluding the possibility that the processing was appropriate and therefore legitimate under the Belgian Privacy Act.[452]

Secondly, the Court rejected the argument that these cookies safeguarded a vital interest of non-Facebook users[453].

Thirdly, the Court rejected the possibility of legitimizing the processing based on an instruction to perform the processing in the public interest or in the exercise of official authority.[454] The Court deemed it unpersuasive that the processing of personal data of non-Facebook users was necessary to secure Facebook services, stating that: *"the defendants do not make it plausible that an attack of the Facebook platform would be possible through plug-ins which are not actually used by users who access a page outside the Facebook domain"*.[455]

Finally, the Court examined the final ground which allows processing when it is necessary to promote the legitimate interests of the controller or the third party to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject claiming protection under the Belgian Privacy Act.[456] The Court applied the necessity test. Firstly, criminals can easily circumvent the use of cookies through specific software. The processing as executed by Facebook, therefore, cannot effectively play a vital role in the security of Facebook services. Secondly, the method used has an enormous impact on non-Facebook users' fundamental right to privacy. Thirdly, Facebook had other, less invasive, security options to achieve the same results.

In conclusion, the Court held that no other grounds legitimised Facebook's practice of tracking non-Facebook users.

---

[451] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.27.
[452] Art. 16, §4 Belgian Privacy Act; *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.27.
[453] Art. 5 (d) Belgian Privacy Act.
[454] Art. 5 (e) Belgian Privacy Act.
[455] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.28.
[456] Art. 5 (f) Belgian Privacy Act.

2.4.2. Violation of Article 4, §1, 2° and 3° Belgian Privacy Act

Facebook is one of the biggest online social networks and has a powerful position in the digital landscape impacting millions of internet users. This position creates an imbalance in their relations with individuals.

When weighing Facebook's interest against those of non-Facebook users, it is clear that Facebook uses its position of power to disproportionally infringe on non-Facebook users' rights. This disproportion constitutes an additional violation of Article 4, §1, 2° and 3° Belgian Privacy Act considering the scale of the personal data collected by Facebook and the indicated purpose.

2.5. Outcome

The Court ordered the defendants: *"in respect of every Internet user on Belgian territory who has not registered as a member of the online social network of Facebook, to cease:*

- *placing a [tracking] (…) cookie when they land on a web page of the facebook.com domain without providing them with prior sufficient and adequate information about the fact that Facebook places the [tracking] (…) cookie with them and about the way Facebook uses that [tracking] (…) cookie through social plug-ins;*

- *collecting the [tracking] (…) cookie through social plug-ins placed on third-party websites."*[457]

In addition to the costs of the proceedings, Facebook was sentenced to pay a sum of 250 000 EUR per started period of 24 hours in which the order for cessation was not complied with. The Court stated this amount was adequate in light of Facebook's financial results.[458]

The implications of this judgment for the future are not entirely clear yet. Facebook has declared it will appeal this decision and has shut down all public Facebook sites for non-Facebook users. It is without doubt, that this will pose problems for restaurants and

[457] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, p.32.
[458] *Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015)*, pp.31-32.

businesses who refer to their public Facebook page as their website.[459] It does not seem likely that Facebook will comply without a fight.

Since then, it has been confirmed that Facebook has appealed the case. A hearing has been scheduled for 11 May 2016. This appeal does not suspend the enforcement of the judgment of the Belgian Court of First Instance.

Following the Belgian Privacy Commission's example, several other DPA's, among others, the French DPA, the Dutch DPA, the Spanish DPA and several German DPA's[460], have started investigations into Facebook's practices.[461]

3. Are the concerns addressed by the data protection reform?

As the Belgian Court of First Instance already declared a violation, the Data Protection Directive already provided sufficient rules to contest Facebook's tracking practice. The GDPR, however, will build on the Data Protection Directive by expanding the territorial scope, setting stricter requirements for consent and offering DPA's more powers regarding enforceability.

Firstly, Facebook will no longer be able to contest the fact that Belgian courts are competent to handle cases regarding Belgian Facebook users and non-Facebook users. This is due to the GDPR's scope, which includes an extra-territorial facet. Whether or not Facebook has a subsidiary in a member state will no longer be relevant as both Facebook Inc., established in the United States of America, as Facebook Ireland Ltd., established in Ireland, target EU internet users. This will be the basis for the competence of the national courts and DPA's in every EU member state.

---

[459] Drozdiak, N. (2015). Belgian Privacy Watchdog Hails Facebook Court Ruling. *Wall Street Journal*. [online] Available at http://www.wsj.com/articles/belgian-privacy-watchdog-hails-facebook-court-ruling-1447162169 [Accessed 4 May 2016].

[460] Because of Germany's state structure, there are multiple data protection authorities.

[461] Bracy, J. (2016). *CNIL gives Facebook three months to comply with privacy order*. [online] International Association of Privacy Professionals. Available at: https://iapp.org/news/a/cnil-gives-facebook-three-months-to-comply-with-privacy-order/ [Accessed 10 May 2016]; Meyer, D. (2016). Facebook Hit With German Antitrust Investigation Over User Terms. *Fortune*. [online] Available at: http://fortune.com/2016/03/02/facebook-germany-antitrust/ [Accessed 14 May 2016]; Fioretti, J. (2016). French data privacy regulator cracks down on Facebook. *Reuters*. [online] Available at: http://www.reuters.com/article/us-facebook-france-privacy-idUSKCN0VH1U1 [Accessed 14 May 2016].

Secondly, the GDPR contains a stricter definition of consent. Consent will no longer be a justification for processing when it is implicit. Instead, internet users will need to take affirmative action in order to consent with Facebook's tracking policies. Consequently, the ineffective opt-out mechanism suggested by Facebook will no longer be acceptable. Users will have to opt-in to these practices. This is additionally confirmed by the GDPR's principle of privacy by default.

Thirdly, and perhaps most importantly, the DPA's will be equipped with more powers to enforce the new data protection rules. DPA's will be able to impose noticeable fines. It is possible these fines will prove to be the most powerful motivator for organisations to comply with the GDPR.

Chapter VI. Maximilian Schrems v. Data Protection Commissioner

"The question is, do we have a fundamental right to data protection in Europe, do we have a private sphere in Europe, and do we enforce it? Because until now we have been living in a big lie."[462]

- MAXIMILIAN SCHREMS[463]

In June 2014, Maximilian Schrems, an Austrian citizen, brought a case before the Irish High Court, which asked two preliminary questions to the CJEU. The ruling in this case had severe consequences as Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce[464] was declared invalid. This affected all data transfers based on the Safe Harbour Agreement, which became illegal.

Mr. Schrems argued that the Safe Harbour Decision, giving effect to the Safe Harbour Agreement between the EU and the US, did not give consumers any kind of protection as it allows over 3 000 US Companies, including Facebook, to repatriate European Personal Data without ensuring an adequate level of data protection..[465]

In this chapter we will consecutively discuss the facts of the case, the considerations of the CJEU and the new EU – US Privacy Shield. Finally, we will review whether or not the concerns raised by Mr. Schrems will be addressed by the 2016 data protection reform.

---

[462] Fioretti, J. (2015). Max Schrems: the law student who took on Facebook. *Reuters*. [online] Available at: http://www.reuters.com/article/us-eu-ireland-privacy-schrems-idUSKCN0S124020151007 [Accessed 15 May 2016].

[463] Maximilian Schrems is an Austrian PhD student and privacy activist.

[464] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, *O.J.* L-215, 25 August 2000, pp.7-47. Hereinafter: Safe Harbour Decision.

[465] Schechner, S. (2014). Max Schrems Vs. Facebook: Activist Takes Aim at U.S.-EU Safe Harbor. *Wall Street Journal*. [online] Available at: http://blogs.wsj.com/digits/2014/11/20/max-schrems-vs-facebook-activist-takes-aim-at-u-s-eu-safe-harbor/ [Accessed 4 May 2016].

1. Facts

Facebook Ireland Ltd., located in Ireland, is a subsidiary from Facebook Inc.., which is located in the United States. When signing up to Facebook, users living in the EU enter into an agreement with Facebook Ireland Ltd. Some, or all, of the personal data from these users is entirely or partly transferred to servers in the US owned by Facebook Inc.[466]

On 25 June 2013 an Austrian law student named Maximilian Schrems took the initiative to submit a complaint to the Irish DPA, called the Data Protection Commissioner. He objected to the transfer of his data to servers in the US, citing that the law and practice in force did not provide adequate protection as required by the Data Protection Directive. In light of recent revelations made by Edward Snowden, Mr. Schrems felt his data was no longer adequately protected. The main security risk was posed by public authorities of the US, the NSA in particular.[467]

The Irish DPA stated it was not required to investigate Mr. Schrems' complaint on the basis that it was unfounded as there was no concrete evidence that the NSA had actually accessed Mr. Schrems' data. Additionally, the Irish DPA argued that the European Commission had found in the Safe Harbour Decision that the United States provided an adequate level of protection based on the Safe Harbour Agreement.[468]

This decision was challenged by Mr. Schrems before the Irish High Court. Although the Irish High Court recognised the electronic surveillance of European data by US intelligence services was necessary and indispensable, it also acknowledged that Edward Snowden's revelations showed a significant overreach on the part of the NSA and other federal agencies. It argued that the practice of mass surveillance, when carried out indiscriminately, is not a proportionate restriction to the right to privacy as required by the Irish constitution.[469]

In order to determine whether the surveillance of Mr. Schrems' data was lawful in accordance with Irish data protection laws, several factors needed to be proven: firstly, that the surveillance was targeted towards specific people or groups of people, secondly, that the targeting of certain people was based on objective factors, thirdly, that the surveillance was

[466] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §27.
[467] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §28.
[468] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §29.
[469] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §30-33.

carried out in the interest of national security or the suppression of crime, and lastly, that there were appropriate and verifiable safeguards ensuring the previous factors were complied with. In light of this, the Irish High Court decided the Irish DPA should have continued its investigation of Mr. Schrems' case as the practice of undifferentiated surveillance is inherently contrary to these principles.[470]

The Irish High Court concluded that the Safe Harbour Decision and the associated Safe Harbour Agreement did not guarantee an adequate level of protection as required by EU data protection laws. Even though Mr. Schrems did not formally question the legality of the adequacy decision, the Irish High Court referred two preliminary questions to the CJEU. Firstly, the Irish High Court questioned if the DPA's are absolutely bound by adequacy decisions when determining if a country ensures an adequate level of data protection.[471] Secondly, the Irish High Court asked if the DPA may and/or must conduct its own investigation in light of factual developments after the publication of the decision of the European Commission.[472]

2. Considerations of the CJEU

2.1. Competence of the national DPA

The CJEU first investigated the powers of the DPA's within the meaning of Article 28 of the Data Protection Directive, which regulates the DPA's when the European Commission has adopted an adequacy decision as provided in Article 25 (6) of the Data Protection Directive.

The CJEU starts by pointing out the independence of the DPA's is imperative to their task of ensuring the protection of individuals.[473] For the same reason, the DPA's have been given a broad range of powers.[474] While the Data Protection Directive states DPA's are only competent to investigate the processing of personal data in their own member state[475], the CJEU states that the transfer of personal data should be considered as processing[476] as

[470] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §33.
[471] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §35-36.
[472] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §36.
[473] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §41.
[474] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §43.
[475] Art. 28 (1) and (6) Data Protection Directive.
[476] Art. 2 (b) Data Protection Directive.

defined by the Data Protection Directive carried out in a member state.[477] The DPA's are therefore competent to investigate the transfer of data to a third country.[478]

Article 25 of the Data Protection Directive imposes several obligations to ensure the transfer of data to third countries does not endanger the data protection of European data subjects. Both a member state and the European Commission can find whether or not a third country provides an adequate level of protection. The European Commission can do this through adequacy decisions, like the one based on the Safe Harbour Agreement. This adequacy decision, which is binding to all member states, obliges member states to take the necessary measures to comply with the decision. Until this decision is declared invalid, member states, or their organs, cannot adopt measures that contradict it.[479]

Only the CJEU is competent to declare an adequacy decision invalid. Until this happens, however, data subjects must retain the right to lodge a complaint with their national DPA. The DPA must subsequently be able to investigate this claim independently, regardless of an existing adequacy decision. Likewise, if a DPA finds the claim unfounded, data subjects must retain the right to contest this decision before a court of law.[480]

The CJEU concluded that an adequacy decision: *"does not prevent a supervisory authority of a Member State (…) from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country (…)."*[481]

2.2. Validity of the Safe Harbour Agreement

Under the Data Protection Directive, transfers of data to third countries are lawful when the third country provides an adequate level of protection.[482] The Data Protection Directive, however, does not contain a definition of the term 'adequate'. The only available explanation is that the level of protection should be evaluated in light of all the circumstances surrounding a data transfer.[483] The underlying goal of Article 25 Data Protection Directive is

[477] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §45. *Parliament v. Council and Commission* [2006]C-317/04 and C-318 04 (CJEU), §56.
[478] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §44-45, 47.
[479] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §50-52.
[480] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §57-64.
[481] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §66.
[482] Art. 25 (1) Data Protection Directive.
[483] Art. 25 (2) Data Protection Directive.

the implementation of the obligation in Article 8 (1) of the Charter. It aims for the continuation of a high level of data protection when transferring data to a third country.[484]

The term 'adequate' does not require third countries to provide a level of data protection *identical* to the EU. As the Advocate General asserted,[485] and as confirmed by the CJEU, the term must be understood as requiring a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU by virtue of the Data Protection Directive and in light of the Charter.[486] Consequently, at the time of taking an adequacy decision, the European Commission should ensure an adequate level of protection, and afterwards periodically re-evaluate whether the data protection standards are upheld factually and legally.[487]

The CJEU started with the following analysis. Firstly, the Safe Harbour principles are only applicable to US organisations receiving data from the EU, and are therefore not applicable to US public authorities.[488] Secondly, the Safe Harbour Decision contains an exception to the applicability of the Safe Harbour principles for national security reasons and when there is a conflict with US law. The Safe Harbour Decision does not contain a reference to rules balancing these interferences with fundamental rights.[489] Thirdly, the Safe Harbour Decision does not contain any information about a system to offer recourse to data subjects.[490] Lastly, and above all, EU data protection laws allow interference only insofar as it is strictly necessary. In light of Edward Snowden's revelations, which evidenced the generalised storage of all the personal data transferred from the EU without any differentiation, limitation or exception, this principle was not respected in the slightest.[491] For these reasons the European Commission did not sufficiently ensure an adequate level of protection for the transfer of data to the US and the Article 1 of the Safe Harbour Decision does not comply with the requirements set out in Article 25 (6) of the Data Protection Directive.[492]

---

[484] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §68-72.
[485] Opinion of Advocate General Bot, *Maximilian Schrems v. Data Protection Commissioner* [2016] C-362/14 (CJEU), §141.
[486] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §73.
[487] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §75-76.
[488] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §82.
[489] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §84-88.
[490] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §89-90, 95.
[491] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §91-94.
[492] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §96-98.

Lastly, the CJEU also investigated the Safe Harbour Decision insofar as it restricted the national DPA's competence to investigate data subjects' complaints. Article 3 of the Safe Harbour Decision restricts the powers of the national DPA's. The Data Protection Directive, however, does not allow for adequacy decisions to limit these powers.

The CJEU found that Articles 1 and 3 of the Safe Harbour Decision were invalid for the abovementioned reasons. Since the other articles of the Safe Harbour Decision are inextricably connected to Article 1 and 3, the entire decision was declared invalid.[493]

2.3. Outcome

In its judgment on 6 October 2015 the CJEU ruled that:

(i) National supervisory authorities have the competence to examine EU - third country data transfers when examining a claim where a person contends that the law and practices in force in that third country do not ensure an adequate level of protection;

(ii) The Safe Harbour Decision is invalid.

On 2 February 2016 the European Commission and the United States agreed on a new framework agreement for transatlantic data transfers: the EU – US Privacy Shield.[494] This political agreement is said to reflect the requirements set by the CJEU in its ruling on 6 October 2015 in the *Schrems* case and as discussed above in Section 2 of this chapter.

As a consequence of the *Schrems* case the new data transfer pact between the US and the EU will explicitly contain an option for the EU to suspend the pact if any new concerns regarding privacy arise.[495] The detailed contents of the new EU – US Privacy Shield have already been addressed in Section 2 of Chapter III.

---

[493] *Maximilian Schrems v. Data Protection Commissioner* [2016]C-362/14 (CJEU), §98, 104-106.
[494] European Commission, (2016). *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*. [online] Available at: http://europa.eu/rapid/press-release_IP-16-216_en.htm [Accessed 4 May 2016].
[495] Fioretti, J. (2015). *EU can suspend new data transfer pact with U.S. if worried about privacy: Official*. [online] Reuters. Available at: http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKBN0TT1FG20151210?feedType=RSS&feedName=technologyNews#ZPodROJISjvM0iwL.97 [Accessed 4 May 2016].

3. Are the concerns addressed by the data protection reform?

As evidenced by the criticism on the EU – US Privacy Shield, discussed in Section 2.3 of Chapter III, the EU – US Privacy shield is far from perfect. While it is not final yet, and the European Commission might still take into account some of the recommendations made by the Article 29 Working Party, it seems likely that the EU – US Privacy Shield will not address the concerns expressed by Maximilian Schrems in this case because, firstly, there are no major changes to the system of adequacy decisions, secondly, the new recourse mechanism is said to be too complex, and thirdly, the EU – US Privacy Shield does not prohibit mass surveillance.

Firstly, the GDPR does not make any radical changes to the regime of adequacy decisions. The only relevant change is the explicit mention of the possibility to repeal or amend adequacy decision and the necessity of periodic review. The question still remains if the European Commission will actively use this possibility. These requirements, however, also come from the judgment of the CJEU in this case. The CJEU explicitly said it is the European Commission's duty to review adequacy decisions in light of new evidence regarding the level of data protection in a certain country.

Secondly, the EU – US Privacy Shield tries to offer data subjects a new recourse mechanism for concerns regarding national security. The mechanism of the ombudsperson can surely be used by data subjects, such as Maximilian Schrems, if similar information about the NSA arises. The Article 29 Working Party's evaluation of this mechanism, however, is not positive. The mechanism, as it is now, is too complex and therefore does not provide effective recourse.

Thirdly, the EU – US Privacy Shield still contains an exception to the seven core principles for reasons of national security. The EU – US Privacy Shield does not contain any provision that prohibits the mass and indiscriminate surveillance of European data. The exception for national security reasons does not contain any obligation of proportionality.

Chapter VII. Conclusion

"There is no law of physics that says that it is impossible to have privacy. We can have privacy, if that is what we as a society choose."[496]

- BARBARA SIMONS[497]

This dissertation started with a quote that stated: "privacy is dead and social media hold the smoking gun." The 2016 data protection reform, however, proves that EU citizens are not willing to simply give up their right to privacy. The two cases discussed also prove that Facebook's practices are not always compliant with the current EU data protection legislation.

Since these practices already pose problems under the Data Protection Directive, it is likely this will continue to be the case unless Facebook changes it's Terms of Service drastically. The improvements in the GDPR offer data subjects more rights, but those only mean something if they are enforced. As more and more national DPA's are starting to pay attention to Facebook's practices, it is likely that more of them will be contested. The most important question for the future will therefore be if the 2016 data protection reform creates new effective ways to enforce the EU data protection laws. Both the GDPR and the EU – US Privacy Shield contain both improvements and shortcomings.

The GDPR will certainly have a positive impact on the enforceability of EU data subjects' rights. Firstly, the inclusion of the accountability principle and the principles of privacy by design and default ensure organisations will have to take into account the impact of their practices on privacy in every phase of their projects. Additionally, the appointment of a DPO will ensure someone is constantly evaluating organisations' privacy policies. Thirdly, the extra-territorial facet of the GDPR will put an end to Facebook's unremitting argument that only the Irish DPA is competent to handle EU citizens' complaints against Facebook. If national DPA's are given sufficient resources they will be able to play a crucial role in

---

[496] Rainie, L. and Anderson, J. (2014). *The Future of Privacy - Elaborations: More Expert Responses*. [online] Pew Research Center: Internet, Science & Tech. Available at: http://www.pewinternet.org/2014/12/18/elaborations-more-expert-responses-4/ [Accessed 16 May 2016].

[497] "*Barbara Simons is a highly decorated retired IBM computer scientist, former president of the ACM, and current board chair for Verified Voting." Rainie, L. and Anderson, J. (2014). The Future of Privacy - Elaborations: More Expert Responses. [online] Pew Research Center: Internet, Science & Tech. Available at: http://www.pewinternet.org/2014/12/18/elaborations-more-expert-responses-4/ [Accessed 16 May 2016].*

fighting violations of the right to privacy. Lastly, the GDPR will impact organisations' stances on privacy as it now offers the opportunity to national DPA's to impose considerable fines. In the past, fines have proven to be a powerful motivator for organisations, which might make these fines the most important innovation in the GDPR. The GDPR, however, also missed some opportunities. The initial proposal contained the standard of explicit consent. Additionally, there is a trend in the EU to provide consumers with more information in the assumption this will allow them to make informed decisions. The sheer amount of information an organisation has to provide, however, might have the opposite effect as less data subjects will be inclined to read the increasingly longer terms of service.

The EU – US Privacy Shield on the other hand will be less impactful. Although progress has been made to offer additional recourse mechanisms and provide more detailed obligations, the criticism of the EU – US Privacy Shield is abundant. The EU – US Privacy Shield is criticised to be too complex and at times inconsistent. Additionally, tome key principles, such as data retention, are not guaranteed. The concept of an ombudsperson might be a good one, lest it not be as complex as it is now. Lastly, the EU – US Privacy Shield does nothing to prevent the mass surveillance of EU data subjects' data. Unless the European Commission renegotiates the EU – US Privacy Shield to include the recommendations made by the Article 29 Working Party, it will most likely be contested immediately. Unless the European Commission is able to ensure an adequate level of protection by US organisations, the protest to its adequacy decisions will persist.

Overall, data subjects' right to data protection will become more enforceable. As long as data subjects and DPA's make it a priority to actually enforce these rights, the GDPR will offer them the effective mechanisms to do so. People who value their privacy will be able to demand a high standard of data protection, while others who do not mind giving up a part of their right to privacy, in exchange for services, can opt-in to these practices. This dissertation can therefore be concluded fittingly with the words of Niels Ole Finnemann[498]:

"The citizens will divide between those who prefer convenience and those who prefer privacy."[499]

---

[498] *"Niels Ole Finnemann is a professor and director of Netlab, DigHumLab in Denmark."* Rainie, L. and Anderson, J. (2014). *The Future of Privacy - Elaborations: More Expert Responses*. [online] Pew Research Center: Internet, Science & Tech. Available at: http://www.pewinternet.org/2014/12/18/future-of-privacy/ [Accessed 16 May 2016].

[499] Rainie, L. and Anderson, J. (2014). *The Future of Privacy - Elaborations: More Expert Responses*. [online] Pew Research Center: Internet, Science & Tech. Available at: http://www.pewinternet.org/2014/12/18/future-of-privacy/ [Accessed 16 May 2016].

BIBLIOGRAPHY

I. Legislation

UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, *UN Doc.* A/6316 (1966).

UN General Assembly, *International Convention on the Protection of the Rights of all Migrant Workers and Members of Their Families*, 18 December 1990, *UN Doc.* A/RES/45/158 (1990).

UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, *UN Doc.* A/RES/44/25 (1989).

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, *O.J.* C 306, 17 December 2007, pp. 1–271.

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *O.J.* L-95, 21 April 1993, pp.29-34.

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, *O.J.* L-215, 25 August 2000, pp.7-47.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *O.J.* L-178, 17 July 2000, pp.1-16.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *O.J.* L-201, 31 July 2002, 37-47, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and

Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, *O.J.* L-337, 18 December 2009, pp.11-36.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L-281, 23 November 1995, pp.31–50.

EU-US Privacy Shield Agreement, *Annex II EU-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce*, pp.4-7, 9-10, 14-18, 20-21.

European Commission, (2016). *Draft Adequacy Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, pp. 3-5.

European Commission, Proposal for a Directive on the protection of individuals with regards to processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25 January 2012, COM 2012/0010 (COD).

European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM 2012/0011 (COD).

European Parliament, Legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Ordinary legislative procedure: first reading, 12 March 2014, C7-0025/2012 – COM 2012/0011(COD).

European Council, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 15 June 2015, COM 2012/0011 (COD).

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the

free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* L-119, 4 May 2016, pp. 1-88.

Consolidated version of the Treaty on the Functioning of the European Union, *O.J.* C-326, 26 October 2012, pp. 47–390.

Charter of Fundamental Rights of the European Union, *O.J.* C-326, 26 October 2012, pp. 391–407.

Regulation No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), *O.J.* L-177, 4 July 2008, pp. 6–16.

Gerechtelijk Wetboek, *BS* 31 oktober 1967, p.11360. (Belgian Judicial Code).

Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 13 maart 1993. (Belgian Privacy Act).

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *Journal officiel* du 7 janvier 1978 et rectificatif au *J.O.* du 25 janvier 1978. (French Data Protection Act)

Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (*BGBl*. I S. 2954), neugefasst durch Bekanntmachung vom 14. Januar 2003 (*BGBl*. I S. 66), zuletzt geändert durch Gesetz vom 29.07.2009 (*BGBl*. I, S. 2254), durch Artikel 5 des Gesetzes vom 29.07.2009 (*BGBl*. I, S. 2355 [2384] und durch Gesetz vom 14.08.2009 (*BGBl*. I, S. 2814). (German Federal Data Protection Act).

Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das durch Artikel 7 des Gesetzes vom 4. April 2016 (BGBl. I S. 558) geändert worden ist. (German Copyright Act).

Data Protection Act 1998. (UK Data Protection Act).

II. Case Law

ECHR

Klass and others v Federal Republic of Germany [1979]5029/71 Series A No. 28 (ECHR).

Leander v. Sweden [1987]9248/81 (ECHR).

Malone v. The United Kingdom [1984]8691/79 (ECHR).

X. v. Iceland [1976]6825/74 (ECHR).

CJEU

Albako Margarinefabrik Maria von der Linde GmbH & Co. KG v Bundesanstalt für landwirtschaftliche Marktordnung [1987]C-249/85 (CJEU).

Content Services Ltd v. Bundesarbeitskammer [2012]C-49/12 (CJEU).

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González [2014]C-131/12 (CJEU).

Joined cases *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* and *Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado* [2011]C-468/10 and C-469/10 (CJEU).

Joined cases *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Davis and Others,* C-203/25 and C-698/15 (CJEU).

Maximilian Schrems v. Data Protection Commissioner [2016]C-362/14 (CJEU).

Mediaset SpA v. Ministero dello Sviluppo economico [2014]C-69/13 (CJEU).

Opinion of Advocate General Bot, *Maximilian Schrems v. Data Protection Commissioner* [2016] C-362/14 (CJEU), §141.

Parliament v. Council and Commission [2006]*C-317/04 and C-318 04 (CJEU), §56.*

Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011]C-70/10 (CJEU).

NATIONAL COURTS

Court of Cassation, 21 May 1987, *Pas*. 1987, I, 1160.

Belgian Commission For The Protection Of Privacy V. Facebook INC., Facebook Belgium SPRL And Facebook Ireland Limited 15/57/C (Dutch Speaking Court of First Instance Brussels 2015).

Landgericht Berlin, Urtail vom 6. März 2012, (16 O 551/10), available at http://openjur.de/u/269310.html.

The Rachel Affaire [1858] D.P. III 62 (Tribunal civil de la Seine).

III. Policy Documents

Article 29 Working Party, (2007). *Opinion 4/2007 on the concept of personal data.* pp.16-17.

Article 29 Working Party, (2010). *Opinion 2/2010 on online behavioural advertising*. p.15.

Article 29 Working Party, (2010). *Opinion 8/2010 on applicable law*. p.25.

Article 29 Working Party, (2011). *Opinion 13/2011 on Geolocation services on smart mobile devices*. pp.19-20.

Article 29 Working Party, (2011). *Opinion 15/2011 on the definition of consent*. pp.11, 18, 21-25.

Article 29 Working Party, (2012). *Opinion 04/2012 on Cookie Consent Exemption*. p.9.

Article 29 Working Party, (2013). *Opinion 03/2013 on Purpose Limitation*. pp.15-16.

Article 29 Working Party, (2014). *Letter to Larry Page. Google Privacy Policy - Appendix*. p.2.

Article 29 Working Party, (2014). *Opinion 05/2014 on Anonymisation Techniques*. p.23.

Article 29 Working Party, (2016). *Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision*. pp.3, 17, 24-25, 27, 39, 45-57.

Australian Law Reform Commission, (2008). *Report 108 Volume 2*. pp.1132-1134.

CNIL, (2012). *CNIL Review of Google's New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data across Services*. p.2.

College Bescherming Persoonsgegevens, (2013). *Investigation into the Combining of Personal Data by Google - Report of Definitive Findings*. Den Haag, pp.66-68.

Data Protection Commissioner, (2012). *Facebook Ireland Limited – Report of Re-Audit*. pp.22, 42.

Data Protection Commissioner, (n.d.). *Guidance Note on Data Protection in the Electronic Communications Sector*. p.3.

ICO, (2015). *Information Commissioner's guidance about the issue of monetary penalties prepared and issued under Section 55C (1) of the Data Protection Act 1998*. pp.6-8.

OECD, (2013). *Privacy Guidelines*. Available at: http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm [Accessed 20 April 2016].

Office of the Privacy Commissioner of Canada, (2012). *Getting Accountability Right with a Privacy Management Program*.

IV. Legal Doctrine

Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C. and Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins*. [online] pp.2, 6, 12-13, 15, 17-19, 21-23. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf [Accessed 4 May 2016].

Acar, G., Verdoodt, V., Wauters, E., Van Alsenoy, B., Heyman, R. and Ausloos, J. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms v.1.3.* [online] pp.8, 12-17, 38, 55, 61-69, 73-79, 90-93, 98-99, 104-109. Available at: https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms [Accessed 4 May 2016].

Belgian Privacycommission.be. (n.d.). *Ik ben een internetgebruiker, hoe kan ik mij beschermen tegen tracking door social plug-ins? | Privacycommissie*. [online] Available at: https://www.privacycommission.be/nl/ik-ben-een-internetgebruiker-hoe-kan-ik-mij-beschermen-tegen-tracking-door-social-plug-ins [Accessed 18 Apr. 2016].

Burke, K. (1981). Secret Surveillance and the European Convention on Human Rights. *Stanford Law Review*, 33(6), p.1122.

Craig, P. and De Búrca, G. (1998). *EU law*. Oxford: Oxford University Press.

Cropper, L. (2016). *EU-US Privacy Shield: The Article 29 Working Party raises its concerns*. [online] Privacylawblog.fieldfisher.com. Available at:

http://privacylawblog.fieldfisher.com/2016/eu-us-privacy-shield-the-article-29-working-party-raises-its-concerns/ [Accessed 3 May 2016].

Davidson, B. (2016). *Getting to know the General Data Protection Regulation, Part 7 - Accountability Principles = More Paperwork*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-7-accountability-principles-more-paperwork [Accessed 4 May 2016].

DLA Piper, (2016). *Data Protection Law of the World*. pp.137-149, 482-487.

Dunphy-Moriel, M. and Power, L. (2015). *Getting to know the General Data Protection Regulation, Part 3 – If you receive personal data from a third party, you may need to "re-think" your legal justification for processing it*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-general-data-protection-regulation-part-3-if-you-receive-personal-data-from-a-third-party-you-may-need-to-re-think-your-legal-justification-for-processing-it [Accessed 4 May 2016].

Ernst & Young, (2009). *Privacy and Data Protection Law: European Developments*.

European Union Agency for Fundamental Rights, (2014). *Handbook Data Protection*. pp.14, 17-18, 20-21.

Hauch, J. (1994). Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris. *Tulane Law Review*, 68(1219).

Keller, D. (2015). *The Final Draft of Europe's "Right to Be Forgotten" Law*. [online] Center for Internet and Society. Available at: http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law [Accessed 4 May 2016].

Lee, P. (2015). *Getting to know the GDPR, Part 1 - You may be processing more personal information than you think*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-1-you-may-be-processing-more-personal-information-than-you-think [Accessed 4 May 2016].

Lee, P. (2016). *The Privacy Shield – is it any good then?*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/the-privacy-shield-is-it-any-good-then/ [Accessed 4 May 2016].

Mahmood, S. and Power, L. (2016). *Getting to know the General Data Protection Regulation, Part 6 – Designing for compliance*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-6-designing-for-compliance/ [Accessed 4 May 2016].

Maldoff, G. (2016). *Top 10 operational impacts of the GDPR: Part 3 – consent*. [online] The International Association of Privacy Professionals. Available at: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/ [Accessed 4 May 2016].

Paez, M. (2009). *Germany Strengthens Data Protection Act, Introduces Data Breach Notification Requirement*. [online] Jones Day. Available at: http://www.jonesday.com/germany-strengthens-data-protection-act-introduces-data-breach-notification-requirement-10-26-2009/#_edn15 [Accessed 4 May 2016].

Paez, M., von Diemar, U., Little, J., Robertson, E., Bru, P., Haas, O. and De Muyter, L. (2015). *Agreement Reached on the European Reform of Data Protection*. [online] Jones Day. Available at: http://www.jonesday.com/agreement-reached-on-the-european-reform-of-data-protection-12-17-2015/ [Accessed 4 May 2016].

Patrikios, A. (2015). *Getting to know the GDPR, Part 2 – Out-of-scope today, in scope in the future. What is caught?*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-2-out-of-scope-today-in-scope-in-the-future-what-is-caught [Accessed 4 May 2016].

Power, L. (2016). *Getting to know the GDPR, Part 9 – Data transfer restrictions are here to stay, but so are BCR*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-9-data-transfer-restrictions-are-here-to-stay-but-so-are-bcr/ [Accessed 4 May 2016].

Privacylawblog.fieldfisher.com. (2016). *Getting to know the General Data Protection Regulation - Part 8*. [online] Available at: http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-8-you-may-need-to-appoint-a-data-protection-officer/ [Accessed 4 May 2016].

Proust, O. (2015). *Getting to know the GDPR, Part 5: Your big data analytics and profiling activities may be seriously curtailed*. [online] Privacylawblog.fieldfisher.com. Available at:

http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-5-your-big-data-analytics-and-profiling-activities-may-be-seriously-curtailed [Accessed 4 May 2016].

Ragno, F. (2009). The Law Applicable to Consumer Contracts under the Rome I Regulation. In: F. Ferrari and S. Leible, ed., *Rome I Regulation: The Law Applicable to Contractual Obligations in Europe*, 1st ed. Munich: sellier. european law publishers, pp.147-149.

Ryssdal, R. (1991). Data Protection and the European Convention on Human Rights in Council of Europe Data protection, human rights and democratic values. In: *XIII Conference of the Data Protection Commissioners*. pp.41-43.

Sartor, G. (2013). *Providers' liabilities and the right to be forgotten*. European University Institute, p.9.

Strossen, N. (1990). Recent US and International Judicial Protection of Individual Rights: A comparative Legal Process Analysis and Proposed Synthesis. *Hastings Law Journal*, 41, p.805.

Swire, P. and Lagos, Y. (2013). Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. *Maryland Law Review*, 72, pp.335-380.

Van Canneyt, T. and Power, L. (2015). *Getting to know the GDPR, Part 4 – "Souped-up" individual rights*. [online] Privacylawblog.fieldfisher.com. Available at: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-4-souped-up-individual-rights/ [Accessed 4 May 2016].

Van Eecke, P. and Truyens, M. (2010). Privacy and social networks. *Computer Law & Security Review*, 26(5), pp.535-546.

Warren, S. and Brandeis, L. (1980). The Right to Privacy. *Harvard Law Review*, IV(5).

V. Press Releases

OECD

OECD, (2011). *Thirty years after the OECD Privacy Guidelines*. [online] Available at: http://www.oecd.org/sti/ieconomy/49710223.pdf [Accessed 4 May 2016].

EUROPEAN COMMISSION

European Commission, (2012). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*. [online] Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en [Accessed 4 May 2016].

European Commission, (2015). *Agreement on Commission's EU data protection reform will boost Digital Single Market*. [online] Available at: http://europa.eu/rapid/press-release_IP-15-6321_en.htm [Accessed 4 May 2016].

European Commission, (2016). *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*. [online] Available at: http://europa.eu/rapid/press-release_IP-16-216_en.htm [Accessed 4 May 2016].

European Commission, (2016). *EU-U.S. Privacy Shield: Frequently Asked Questions*. [online] Available at: http://europa.eu/rapid/press-release_MEMO-16-434_en.htm [Accessed 6 May 2016].

European Commission, (2016). *Joint Statement on the final adoption of the new EU rules for personal data protection*. [online] Available at: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm [Accessed 15 May 2016].

European Commission, (2016). *Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield*. [online] Available at: http://europa.eu/rapid/press-release_IP-16-433_en.htm [Accessed 6 May 2016].

BELGIAN PRIVACY COMMISSION

Belgian Privacy Commission, (2015). *On 13 May the Belgian Privacy Commission adopted a first recommendation of principle on Facebook*. [online] Available at: https://www.privacycommission.be/en/news/13-may-belgian-privacy-commission-adopted-first-recommendation-principle-facebook [Accessed 15 May 2016].

Belgian Privacy Commission, (2015). *The judgment in the Facebook case*. [online] Available at: https://www.privacycommission.be/en/news/judgment-facebook-case [Accessed 4 May 2016].

CNIL

CNIL, (2015). *Un nouveau label CNIL gouvernance Informatique et Libertés*. [online] Available at: https://www.cnil.fr/fr/un-nouveau-label-cnil-gouvernance-informatique-et-libertes [Accessed 4 May 2016].

VI. Media Coverage

Bracy, J. (2016). *CNIL gives Facebook three months to comply with privacy order*. [online] International Association of Privacy Professionals. Available at: https://iapp.org/news/a/cnil-gives-facebook-three-months-to-comply-with-privacy-order/ [Accessed 10 May 2016].

Drozdiak, N. (2015). Belgian Privacy Watchdog Hails Facebook Court Ruling. *Wall Street Journal*. [online] Available at http://www.wsj.com/articles/belgian-privacy-watchdog-hails-facebook-court-ruling-1447162169 [Accessed 4 May 2016].

Fioretti, J. (2015). *EU can suspend new data transfer pact with U.S. if worried about privacy: Official*. [online] Reuters. Available at: http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKBN0TT1FG20151210?feedType=RSS&feedName=technologyNews#ZPodROJISjvM0iwL.97 [Accessed 4 May 2016].

Fioretti, J. (2015). Max Schrems: the law student who took on Facebook. *Reuters*. [online] Available at: http://www.reuters.com/article/us-eu-ireland-privacy-schrems-idUSKCN0S124020151007 [Accessed 15 May 2016].

Fioretti, J. (2016). French data privacy regulator cracks down on Facebook. *Reuters*. [online] Available at: http://www.reuters.com/article/us-facebook-france-privacy-idUSKCN0VH1U1 [Accessed 14 May 2016].

Johnson, B. (2010). Privacy no longer a social norm, says Facebook founder. *The Guardian*. [online] Available at: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [Accessed 15 May 2016].

Meyer, D. (2016). Facebook Hit With German Antitrust Investigation Over User Terms. *Fortune*. [online] Available at: http://fortune.com/2016/03/02/facebook-germany-antitrust/ [Accessed 14 May 2016].

Perez, M. (2008). T-Mobile Lost 17 Million Subscribers' Personal Data. *InformationWeek*. [online] Available at: http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210700232 [Accessed 4 May 2016].

Schechner, S. (2014). Max Schrems Vs. Facebook: Activist Takes Aim at U.S.-EU Safe Harbor. *Wall Street Journal*. [online] Available at: http://blogs.wsj.com/digits/2014/11/20/max-schrems-vs-facebook-activist-takes-aim-at-u-s-eu-safe-harbor/ [Accessed 4 May 2016].

VII. Facebook

Facebook Ad Settings. (n.d.). *Facebook*. [online] Available at: https://www.facebook.com/settings?tab=ads [Accessed 14 May 2016].

Facebook Developers. (n.d.). *Social Plugins - Documentation - Facebook for Developers*. [online] Available at: https://developers.facebook.com/docs/plugins [Accessed 18 April 2016].

Facebook Investor Relations. (2015). *Facebook Reports Third Quarter 2015 Results - Facebook*. [online] Available at: http://investor.fb.com/releasedetail.cfm?ReleaseID=940609 [Accessed 5 May 2016].

Facebook Newsroom. (2015). *Setting the Record Straight on a Belgian Academic Report*. [online] Available at: http://newsroom.fb.com/news/h/setting-the-record-straight-on-a-belgian-academic-report/ [Accessed 16 May 2016].

Facebook Newsroom. (n.d.). *Company Info*. [online] Available at: http://newsroom.fb.com/company-info/ [Accessed 5 May 2016].

Facebook. (2015). *Data Policy*. [online] Available at: https://www.facebook.com/policy.php [Accessed 5 May 2016].

Facebook. (2016). *Terms of Service*. [online] Available at: https://www.facebook.com/terms [Accessed 5 May 2016]. (Terms of Service)

Facebook. (n.d.). *Audience Targeting Options - Help Center*. [online] Available at: https://www.facebook.com/help/633474486707199 [Accessed 21 April 2016].

Facebook. (n.d.). *Can I target my ad to people based on their age and gender? - Help Center*. [online] Available at: https://www.facebook.com/help/813939365351532 [Accessed 21 April 2016].

Facebook. (n.d.). *Control the ads you see - About Advertising on Facebook*. [online] Available at: http://facebook.com/about/ads [Accessed 18 April 2016].

Facebook. (n.d.). *Cookies, Pixels & Similar Technologies*. [online] Available at: https://www.facebook.com/help/cookies/update [Accessed 5 May 2016].

Facebook. (n.d.). *Does Facebook use my name or photo in ads? - About Facebook Ads | Facebook Help Center*. [online] Available at: https://www.facebook.com/help/769828729705201/ [Accessed 5 April 2016].

Facebook. (n.d.). *How can I download my information from Facebook? | Facebook Help Center | Facebook*. [online] Available at: https://www.facebook.com/help/212802592074644 [Accessed 30 April 2016].

Facebook. (n.d.). *How do I target education levels, specific schools, fields of study or specific graduation years? - Help Center*. [online] Available at: https://www.facebook.com/help/227971680551772 [Accessed 21 April 2016].

Facebook. (n.d.). *How does Facebook know when people are in the locations I am targeting? - Help Center*. [online] Available at: https://www.facebook.com/business/help/133609753380850 [Accessed 19 April 2016].

Facebook. (n.d.). *Nearby Friends | Facebook Help Center | Facebook*. [online] Available at: https://www.facebook.com/help/629537553762715/ [Accessed 19 April 2016].

Facebook. (n.d.). *What are audience behaviours? - Help Center*. [online] Available at: https://www.facebook.com/help/243268465859743 [Accessed 21 April 2016].

Facebook. (n.d.). *What is a custom audience? - Help Center*. [online] Available at: https://www.facebook.com/help/341425252616329 [Accessed 5 May 2016].

Facebook. (n.d.). *What is connections targeting? - Help Center*. [online] Available at: https://www.facebook.com/help/186282224754628 [Accessed 21 April 2016].

Facebook. (n.d.). *What is interests targeting? - Help Center*. [online] Available at: https://www.facebook.com/help/188888021162119 [Accessed 21 April 2016].

Facebook. (n.d.). *What options do I have when selecting people within a location? - Help Center*. [online] Available at: https://www.facebook.com/help/755086584528141 [Accessed 21 April 2016].

VIII. Other

Biography. (2016). *Edward Snowden*. [online] Available at: http://www.biography.com/people/edward-snowden-21262897 [Accessed 15 May 2016].

Biography. (2016). *Mark Zuckerberg*. [online] Available at: http://www.biography.com/people/mark-zuckerberg-507402 [Accessed 15 May 2016].

Europe versus facebook. (n.d.). *Get Your Data*. [online] Available at: http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html [Accessed 14 May 2016].

European Commission, (2015). *Special Eurobarometer 431 "Data protection"*. [online] European Union, p.115. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf [Accessed 14 May 2016].

International Telecommunication Union (ITU). (2015). *Statistics - Global ICT Developments*. [online] Available at: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx [Accessed 14 May 2016].

Lee, Phil, and Mark Webber. "GDPR 1.0 - Top 10 Things You Need To Know!". Presentation, SanDisk Corporation, 2016.

Lobbyplag. (n.d.). *LobbyPlag: Amendments*. [online] Available at: http://lobbyplag.eu/map/article/17 [Accessed 9 May 2016].

Mashable. (n.d.). *Pete Cashmore*. [online] Available at: http://mashable.com/people/petecashmore/ [Accessed 15 May 2016].

Mozilla Support. (n.d.). *Disable third-party cookies in Firefox to stop some types of tracking by advertisers | Firefox Help*. [online] Available at: https://support.mozilla.org/en-US/kb/disable-third-party-cookies. [Accessed 7 May 2016].

Rainie, L. and Anderson, J. (2014). *The Future of Privacy - Elaborations: More Expert Responses*. [online] Pew Research Center: Internet, Science & Tech. Available at: http://www.pewinternet.org/2014/12/18/future-of-privacy/ [Accessed 16 May 2016].

Snowden, E. (2015). *Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLU's Jameel Jaffer. AUA. • /r/IAmA*. [online] reddit. Available at: https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/crglgh2 [Accessed 15 May 2016].

Snowden, E. (2016). *Edward Snowden on Twitter*. [online] Twitter. Available at: https://twitter.com/Snowden/status/694571566990921728 [Accessed 6 May 2016].

The Center for Internet and Society. (n.d.). *Stanford Law School - Daphne Keller*. [online] Available at: http://cyberlaw.stanford.edu/about/people/daphne-keller [Accessed 14 May 2016].