HAW University of Applied Sciences
Faculty of Economics and Social Sciences
Department of Economics

Post Safe Harbor: Regulatory Changes and Economic Consequences

Bachelor Thesis

Submitted by Stephanie Harringer

Course of study: Foreign Trade and International Management

[redacted]

Submission date: March 14th 2016

Supervising professer: Prof. Dr. Michael Gille

Second examiner: Prof. Dr. Natalia Ribberink

List of Contents

List of Figures

List of Abbreviations

BCR	Binding Corporate Rules
CFREU	Charta of the Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DAE	Digital Agenda for Europe
DPA	Data Protection Agency
ECB	European Central Bank
EEA	European economic area
EU	European Union
EUR	Euro
FDI	Foreign Direct Investment
FTC	Federal Trade Commission
GDP	Gross domestic product
GDPR	General Data Protection Regulation
ICT	Information and communication technology
MMS	Multimedia Messaging Service
MNE	Multinational enterprises
OECD	Organization of Economic Cooperation and Development
PRISM	Planning Tool for Resource Integration, Synchronization, and Management
R&D	Research and Development
SC	Standard Clauses
SIP	Social Investment Package
SME	Small and medium-sized enterprises
SMS	Short Message Service

TISA	Transatlantic Information and Service Agreement
TTIP	Transatlantic Trade and Investment Partnership
UAE	United Arab Emirates
UK	United Kingdom
US	United States of America
WP133	Working Paper 133
WTO	World Trade Organization

1. Introduction

As a business area generating billions of dollars p.a. in trade[1], legal developments that concern the data flow business between Europe (EU) and the US are a highly controversial subject among political as well as business entities. Nevertheless, the e-business is of fast-moving nature and the currently available regulatory framework, still being in its fledgling stage, does not seem to be able to keep pace.

With the Safe Harbor Agreement being declared invalid by the Court of Justice of the European Union (CJEU) on October 6th 2015, the legal foundation for personal data transfer from Europe into the US has been deprived. This is due to the difference in prevailing perceptions of jurisdictional importance in privacy matters within the economies. Despite a granted grace period until the end of January 2016[2], companies and political authorities now depend on a fast development of a new regulatory framework and adjustments of accompanied tools to continue and to retain international business as well as economic and political interests.[3]

Yet, jurisprudence for data protection and privacy in the US and EU are fundamentally disparate. Data protection is valued very highly and cautiously by EU citizens[4] and is also privileged by legislation in the Charter of Fundamental Rights of the European Union[5]. Although US citizens share the importance of being in control over their data[6], US companies “do not see privacy as a normal cost of doing business”[7] and the US Congress avoided putting up a comprehensive privacy law in the past.

Therefore, the European Commission occurs to be the driving force in the regulatory development[8] and already agreed on the new General Data Protection Regulation (GDPR) on December 15th 2015 whilst constantly negotiating new draft laws and agreements. However, it is conspicuous that

[1] OECD, 2015
[2] Piltz, 2013
[3] Mester, 2015; also: Fuchs 2015
[4] European Commission, Data Protection Eurobarometer – Factssheet, 2015
[5] European Commission, Charter of the Fundamental Rights of the European Union (2000(C 364/01) 2000, Articel 7, 8 and 47; also: European Commission, 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 1995, Article 25
[6] Madden and Rainie, 2015
[7] Schriver, 2002, p. 2779
[8] Svantesson, 2014, p. 62

the changes made have a cause-effect relationship which might comprise unforeseeable repercussions. Hence it is important to screen the current development and evaluate its possible future impact in order to assess where the prospective data privacy regulation should be navigated.

1.1 Objective

The aim of this paper is to ascertain possible consequences of upcoming law decision making on the affected economy and companies in particular bearing in mind the initial drift of motivation being achieved.

1.2 Course of Investigation

First the importance of the Safe Harbor Decision C-362/14 for the data privacy development will be explained. Then the meaning of current and negotiated future regulatory changes in law, which concern data transfer from Europe into the US, will be examined with regards to the needs and deliberate goals of the European Commission as the prevailing law-making authority. After that, possible consequences depriving from the ongoing development in the data flow business as well as impacts on the EU and US economy as a consequence thereof will be evaluated.

2. The Importance of the Safe Harbor Decision

The reason to attune the Safe Harbor Agreement in 2000 was to provide a legal basis for data trade between the European Union and the US. Five years earlier, on October 25th 1995, the Data Protection Directive 95/46/EC had been adopted by the European Parliament and Council. The intention was to provide a legal framework for the concerns of elicitation, transfer and processing of data from EU-citizens in international matters within and beyond the European Union. Directive 95/46/EC is part of the EU privacy and human rights law aiming to protect the fundamental rights and highlights the importance of data protection even beyond European borders. Hence it states in Article 25 that data-importing entities should provide an "adequate level of protection"[9] that complies with the European standards. The concomitant Safe Harbor Agreement has served as the legal fundament for the U.S. as a data-importing non-EU country, covering the requirements of Article 25. [10]

In Case C-362/14 the CJEU came to focus on the derogation in the Safe Harbor framework.[11] First trigger was the scale of infringement on personal data by the US government, which was brought to light by Edward Snowden in 2013. On July 24th 2013 the federal agency as well as privacy officials adverted to "the eligibility of national officials to intermit data transfer to non-EU countries if a high possibility exists, that Safe Harbor principles or standard clauses are breached"[12]. A few weeks later, on August 13th 2013, the European Article 29 Working Party made similar implications.

Following this, the Austrian law student Maximilian Schrems demanded a control assessment by the European Data Commissioner and prohibition for facebook Ireland Inc. to send its data to the US. With his enquiry, Schrems indirectly questioned the validity of the Safe Harbor Agreement itself.[13] The case proceeded to the Irish Court and thereon further to the CJEU where the complaints within the Safe Harbor framework were found to be unlawful in terms of Article 7, 8 and 47 of the Charta of Fundamental Rights of the

[9] European Commission, Directive 95/46/EG of the European Parliament and of the Council 1995, Article 25
[10] Ibid.
[11] CJEU, Judgment of the Court in Case C-362/14, 2015
[12] Götz, 2013, p.636
[13] CJEU, Judgment of the Court in Case C-362/14, 2015

European Union.[14] Subsequently, the adequacy of the level of protection provided by Safe Harbor was ruled to be insufficient. Hence the Safe Harbor Agreement was declared invalid on October 6th 2015, abrogating the legal basis for data trade between the EU and US.[15]

The ruling can be seen as the presentation of current bias points within the market. It is not to be understood as a judgment of the data protection scale in the US but rather, as a statement in the decision which declares, that the ”lawful action of the EU commissioner is not enough to obey the needed regulation for protection under European data protection law“.[16] It also criticizes several other loopholes and the way of handling operational needs. Therefore the circumstances described in Decision C-362/46 are a statement on some key points that need to be in the focus of discussion when thinking of designing future data protection laws.

One important hurdle for the assertion of EU data protection law is that national law of third countries acts out superior to international agreements.[17] Mass surveillance has been achieved by the U.S. National Security Agency (NSA), demanding personal data information from PRISM-entities like Google, Facebook or Microsoft. These companies have been self-certified under Safe Harbor criteria but were at the same time obliged to U.S. law. European law cannot forbid U.S. law but the dependability of compliance with EU-standards in non-EU countries needs to be assured by an appropriate system of monitoring and control mechanisms, to be able to protect personal data and restrict the issuance of those if needed.[18] The absence of appropriate operational mechanisms and the lack of effective restriction of infringement by the U.S. authorities[19] undermine the national level of protection.

The Safe Harbor investigation has also shown how restricted data protection authorities are in their action. Schrems’ enquiry only had to be pushed further in the legislative latter because the data protection commissioner was

[14] European Commission, Charter of the Fundamental Rights of the European Union (2000(C 364/01), 2000
[15] Manich und Assion, 2015; also: CJEU, Judgment of the Court in Case C-362/14, 2015
[16] Manich und Assion, 2015
[17] Judgment of the Court in Case C-362/14, 2015, recital no. 85
[18] Judgment of the Court in Case C-362/14, 2015, recitals no. 81 - 83
[19] Ibid., recitals no. 84-88

abrogated by the means of the Safe Harbor Agreement itself. The correct application of operational tools as well as already established mechanisms for a safe data transfer (e.g. the Article 29 Working Party “Standard Clauses”) need to enable authorities to intervene in a timely manner and should be equipped with a set of tools to engage flexibly in accordance to new risks of advanced technological development.

There is a strong need of a harmonized regulatory system to provide transparency in action for both companies as well as authorities and to strengthen citizen rights of remedy. Questionable in the prevailing regulatory system was who to hold responsible for these systematic loopholes. Directive 95/46 in its nature gave EU Member States the freedom of integrating the rules into their national law in their own tenor which lead to the creation of patchwork law within the EU.[20] This made it non-transparent for businesses and authorities to understand and cope with the legal basis they were working on. Furthermore the CJEU found a lack of administrative and jurisdictional remedy for EU-citizens whose data has been breached by the NSA surveillance system.[21] EU citizens are unable to demand legal action due to a lack of assigned accountabilities and legal procedures which should be a protected fundamental human right.[22]

With data trade being such an important factor for the gross domestic product (GDP) revenue between Europe and the U.S., those key issues resulting from the Safe Harbor Decision will be of much importance for the future jurisdictional development and need to be considered in both the short and long term regulatory solutions.

Considering that the flaws in the current regulations regard highly operational and Citizen-involving issues, the change of regulations will have a definite impact on how companies will operate in the future which in turn will have an effect on business practices and opportunities. Therefore this could also mean a shift in competition and economic power.

[20] Gilbert, European Data Protection 2.0: New Compliance Requirements In Sight - What The Proposed EU Data Protection Regulation Means for U.S. Companies, 2012
[21] Judgment of the Court in Case C-362/14, 2015, recital no. 89 and recital no. 90
[22] European Commission, Charter of the Fundamental Rights of the European Union (2000(C 364/01), 2000, Article 47

3. The Impact of Current Regulatory Changes and Outstanding Legal Decisions on E-Business

3.1 The General Data Protection Regulation

On December 15th 2015 the European Commission agreed on the new General Data Protection Regulation as the new legal framework. It includes a regulation to protect individuals with regard to the processing and movement of private data as well as a Police and Criminal Justice Data Protection Directive to make sure incident response will be facilitated. The new GDPR seeks to replace Directive 95/46/EC.[23] It will be applicable in two years from the day of adoption, which is predicted for 2016.[24]

The GDPR will foster a harmonized way of jurisprudence throughout Europe in terms of data protection and therefore strengthen the ability of enforcement for authorities. With a Regulation as the new form of law, no further inclusion of or interpretation into national law will be needed[25] because it will be equally and promptly applicable to all EU Member States.[26] Therefore the Commission assumes a regulation to be a more suitable instrument of clearing uncertainty for data controllers[27] as well as authorities.[28] It will not matter where in the EU a complaint is drawn, the rules and processes will be similar and Member States are encouraged to learn quickly from each other to improve their legal action and surveillance in this matter. This will ensure process clarification for all entities involved in doing e-business but not yet a cut in administrative expenditures for the economy.

---

[23] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, Article 88 and Article 98

[24] European Commission, European Commission: Questions and Answers - Data protection reform, 2015

[25] Gilbert, European Data Protection 2.0: New Compliance Requirements In Sight - What The Proposed EU Data Protection Regulation Means for U.S. Companies, 2012; also: European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, pp. 5-6

[26] Gilbert, European Data Protection 2.0: New Compliance Requirements In Sight - What The Proposed EU Data Protection Regulation Means for U.S. Companies, 2012, pp. 817 and 823

[27] de Hert and Papakonstantinou, The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals, 2012, p. 132

[28] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012

It is also approaching an extraterritorial reach to ensure the GDPR to be eligible and actionable for data controlling and processing of EU-citizens that are conducted outside the EU. The GDPR Proposal claims that the Regulation shall also apply, if the collector of personal data processes data of EU-citizens beyond EU/EEA borders[29] which extends the reach of accountability of internationally acting organizations in the EU. Furthermore, controllers not established in the EU are obliged to designate a representative in the EU.[30] If several Member States are affected by the collector's work, only the Data Protection Authority (DPA) in the country of the Headquarters is responsible.[31] Involving organizations of non-EU countries into the definitions of the European Regulation and incorporating their approachability into the EU targets to be able to hold them accountable for their actions. The DPA-Headquarter-Rule again simplifies responsibility of jurisdiction for authorities and business entities.

On the one hand, the companies' obligations in terms of demonstrating their level of protection will extend. Controllers as well as processors will have to carry out a data protection impact assessment prior to risky processing operations.[32] They will need to perform upon individual requests to exercise, for example, their "right to be forgotten"[33] by providing written procedures and processes that they actually use, and to be able to show that they comply with the applicable legal requirements - "principle of accountability".[34] There will be an obligation to inform citizens and authorities about possible data breach[35] as well as the need to show transparency by communicating companies' actions clearly, as the "principle of transparency" states.[36] It is

[29] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, recitals no 20, 21 and Article 3, also: Verheijden, 2015, p. 192; also: Bull, 2015, 104-105

[30] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, recital 63, Article 25; also: Verheijden, 2015, p. 192

[31] Ibid., recital 97, 98, Article 51.2

[32] Ibid., Article 33

[33] Gilbert, European Data Protection 2.0: New Compliance Requirements In Sight - What The Proposed EU Data Protection Regulation Means for U.S. Companies, 2012, p. 819

[34] Ibid., p. 819; also: European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, Article 22

[35] Ibid., Article 5

[36] Ibid., recital 46

easy to see how this creates great internal and external operational needs for companies. To comply with the new regulation, businesses will have to invest mostly into administration, educated workforce and legal expertise.

On the other hand, other bureaucratic burdens will be eliminated. As already mentioned, the legal harmonization and extraterritorial reach of rules also simplifies procedures for companies. The "one-stop-shop"[37] approach is supposed to save an estimated expense of EUR 2.3 billion per year[38] by limiting supervisory accountability down to one, who will be approached by the headquarters. In addition, "data protection by design"[39] and the installation of privacy-friendly mechanisms and techniques will be encouraged from an early stage of development to ensure prompt compliance for innovative products.[40] Although this can also be seen as extra expenditure for companies, it secures long-term adherence to legal expectations and thus can be used as an image-boost for created trust in new technology.

The new regulation intends to give EU-citizens an extended influence on and control over the data collected about them. The data subjects' right of access to their personal data[41] will be extended by the new elements of the right to be informed about the data's storage period, the right of rectification and the right of erasure.[42] The right of erasure also refers to the "right to be forgotten".[43] As mentioned before, information on how personal data is stored shall be available and understandable. In addition, the data subject will be able to require a data transfer from one service provider to another under the "principle of data portability"[44]. Citizens have the right to be informed when their data has been breached which falls under the obligations of the data

[37] European Commission, Europe 2020 - A strategy for smart, sustainable and inclusive growth, 2010
[38] European Commission, European Commission - Agreement on Commission's EU data protection reform will boost Digital Single Market, 2015
[39] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, Article 23
[40] European Commission, European Commission - Agreement on Commission's EU data protection reform will boost Digital Single Market, 2015
[41] European Commission, 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, 1995, Article 12(a)
[42] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, Article 15
[43] Ibid., Article 17
[44] Ibid., Article 18

controller.[45] The clarification of circumstances on data storage and processing in the complex e-business environment can help raise the awareness of EU-citizens. Knowledge leads to a confident use of one's rights. Hence, if the execution of rights claimed increases, this will create an excessive legal burden for companies that are not yet fully compliant. Nevertheless, engaging consumers also creates trust and consent and feedback will help to find a company's legal needs to be able to approve them.

Furthermore, improved administrative and juridical remedies will be provided.[46] Citizens will be able to directly refer to the DPA in their country, even when their data are processed by a company based in a different Member State or even outside the EU/EEA area.[47] Next to the direct ability for citizens to lodge a complaint, also organizations and associations receive the right to issue complaints on behalf of one or more data subjects.[48] To condense complaints under the legal action of an association can be a great administrative relief. The result of such attempts tends to be more successful than that of individuals which should encourage citizens to take advantage of these remedies. Rectifications imply high financial risk for businesses, especially small and medium-sized enterprises (SMEs). This holds true especially in the US, where legal complaints and compensation are acted out stronger than in the EU. Companies might suffer severe financial damage if legal conflicts start evolving under U.S. law. In terms of the GDPR, companies not complying can be sentenced with "up to 0.5% of (their) annual worldwide turnover".[49]

[45] European Commission, European Commission - Agreement on Commission's EU data protection reform will boost Digital Single Market, 2015

[46] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, Article 15

[47] Gilbert, European Data Protection 2.0: New Compliance Requirements In Sight - What The Proposed EU Data Protection Regulation Means for U.S. Companies, 2012, p. 818; also: Verheijden, 2015, p. 193

[48] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, recital 112, Article 73; also: Verheijden, 2015, p. 192

[49] Ibid., Article 79.4

3.2 Regulatory Exceptions

To ease the process of consent and control, contractual alternatives are commonly used in business environments with a very complex regulatory system. To keep the data transfer an easier endeavor in the concept of Safe Harbor, alternatives to the invalid agreement could now derive from other contractual solutions, consent, other derogations or a Safe Harbor 2.0.[50] In general, Binding Corporate Rules (BCR) and Standard Clauses (SC) are already in use. Furthermore special agreements can be attuned in bilateral agreements such as the currently negotiated Transatlantic Trade and Investment Partnership (TTIP) or Trade in Services Agreement (TiSA).

3.2.1 Standard Clauses and Binding Corporate Rules

SCs and BCRs help to provide applicability of European Law beyond EU/EEA borders. The purpose of Standard Clauses is to bring business execution matters in cooperation or within non-EU countries that are not yet certified with adequate level of protection, into the context of "order data processing"[51] with EU data to make the GDPR applicable to these cases.[52] BCRs carry the same objective in the scope of Multinational Enterprises (MNEs) and assure compliance with legal expectations for the entire company to avoid contracts for each single transfer.[53] Both tools have been established by the Article 29 Working Party, different versions of the SCs are in use since 2001.[54] In context of the GDPR, the three types of clauses and BCRs have been inherited without change for now. Thus processes will be bound to provide data protection to the standard of the new regulation.

However, some authorities see the same flaws of undermining authorities' action and impracticable consumer dispute as in the Safe Harbor Agreement.[55] Certain clauses show equal self-certifying characteristics of

[50] Schrems, 2015
[51] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, Article 41 f.)
[52] Datenschutz, 2011
[53] European Commission, Overview of Binding Corporate Rules 2015; information on the procedure of approval under: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm
[54] European Commission, Model Contracts for the transfer of personal data to third countries, 2015
[55] CJEU, Judgment of the Court in Case C-362/14, 2015

operations hard to verify.[56] For BCRs, the European Commission makes sure companies throughout all EU member states are able to apply correctly.[57] Sometimes even an authorization fee is needed.[58] WP133 states that effectiveness of BCR shall be demonstrated by typically used mechanisms, such as regular audits. These are assumed to be conducted by the DPA.[59] Yet the necessity to prove compliance of written BCR with the actual operational business by an external authority is nowhere mentioned as conditional for approval. This leads to the assumption that both approval and operational control, audits, are rather an act of bureaucracy than an actual execution by authority.

Furthermore, once a SC is approved, Member States are obliged to acknowledge that organizations which use SCs provide an adequate level of data protection.[60] Also, the approved BCR will assure authorization of transfer of data into non-EU/EEA countries with no adequate level of protection.[61] This could again, like the Safe Harbor Agreement, make it difficult, if not impossible, for authorities to question and revise their decision.[62]

If companies are still able to meet law criteria with exceptional agreements that allow them to hide business practices that do not correlate with the actual legal security standards, the entire protective purpose of the GDPR will be put out of order. Therefore both tools need to be questioned for applicability and be revised accordingly.

[56] European Commission, Commission Decision C(2010)593 - Standard Contractual Clauses (processors), 2010, Clauses 4 (f), 4 (e), 5 (a) 2, ; also: European Commission, Commission Decision C(2010)593 - Standard Contractual Clauses (processors), 2010, Clause 12 (1)
[57] Article 29 Working Party, ec.europa.eu - National filing requirements for controller BCR ("BCR-C"), 2015
[58] Ibid., p. 7
[59] Ibid., Section 5: Effectiveness
[60] Weniger, 2005, p. 471
[61] European Commission, Overview of Binding Corporate Rules, 2015; information on the procedure of approval under: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm
[62] CJEU, Judgment of the Court in Case C-362/14, 2015

3.2.2 The EU-US Privacy Shield

As foretold by experts, on February 2nd 2016 the European Commission and US agreed on an attempt of a Safe Harbor 2.0[63], the now called EU-U.S. Privacy Shield.[64]

The intention, beside the ease of data trade, is to make EU standards enforceable under U.S. law and give EU-citizens several options to claim for compensation. The fact that companies publish their commitments shall enable legal action of the U.S. Federal Trade Commission (FTC). A communication mechanism for complaints will be installed between EU and U.S. authorities and companies will be obliged to react upon a deadline. Additionally, "Alternative Dispute resolution will be free of charge".[65]

This agreement shows the promising potential to become an arrangement that is supportive of European standard needs and encouraging extraterritorial legal enforcement. It could imply an attempt to literally condense U.S. and EU company practices under the same legal expectations. As much as that would seem a drawback for U.S. MNEs, it could also generate chances for all companies in both the U.S. and the EU. Whether this becomes reality or if it will rather provide another easy way around legal burdens, remains to be seen with the first published draft.

3.2.3 Bilateral Agreements TTIP and TiSA

Since the start of negotiation, TTIP and TiSA have been discussed and criticized for endangering European standards and human rights in various ways, including data privacy.[66] Both agreements include sections that deal explicitly with the transfer of data deriving from electronic commerce between the U.S. and EU.

Although co-operation and accompanying negotiation on issues related to future developments are being promoted[67] and there are sections included

[63] Schrems, 2015
[64] European Commission, European Commission - EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, 2016
[65] Ibid.
[66] Israel 2015, pp. 14-17
[67] Transatlantic Trade and Investment Partnership - Trade in Services, Investment and E-commerce, 2015, Article 6-1

that give an understanding for the importance of data protection[68], at least two major concerns arise from the current drafts.

First, the agreements reflect that there is a serious possibility that GDPR protective measures are going to be constrained. TiSA Article 2 states that "no Party may prevent the transfer, access, processing or storing of information outside that Party's territory if conducted in connection with a business. Article 2 sub-clause 5 further holds that Parties should not prevent foreign suppliers of services from transferring information across borders within internal networks."[69] In the TTIP section of "trade in services, investment and e-commerce"[70], article 6-4 sub-clause1 states that "parties shall ensure that the provision of services by electronic means may not be subject to prior authorization or any other requirement having equivalent effect"[71]. It also states that this shall be "without prejudice to authorization schemes which are not specifically and exclusively targeted at services provided by electronic means".[72] In the GDPR basically every data collection and transfer targets services provided by electronic means. Therefore, surveillance and control mechanisms developed by the European Commission and the ability to intervene when European citizens' rights are breached.

Second, measures to ensure accountability for non-EU companies are being eliminated. TiSA article 9 holds, that "no party may require a service provider to use territorially localized computer facilities for processing and storage of data as a condition of supplying service to that country."[73] Taking legal action in Europe under harmonized law is obviously easier than filing complaints across borders. If U.S. companies draw back their premises from EU territory, it makes them harder to account to European privacy standards that are still not included in any way under U.S. national law. Although the GDPR attempts an extraterritorial reach and the EU-U.S. Privacy Shield intends to

[68] Transatlantic Trade and Investment Partnership - Trade in Services, Investment and E-commerce, 2015, Article 6-7
[69] Israel, 2015; also: Wikileaks - Trade in Services Agreement - Annex on [Electronic Commerce], 2015, p.3
[70] TTIP
[71] Ibid.
[72] Transatlantic Trade and Investment Partnership - Trade in Services, Investment and E-commerce, 2015
[73] Ibid., p. 8

make standards applicable under U.S. law, the U.S. FTC is only able to enforce protective measures to companies if they voluntarily agree to adopt them.[74]

3.2.4 The US approach towards Data Privacy

Although there is no data protection law in the US jurisdiction, the federal government seems to become aware of the importance of the consideration of consumer rights. In spring 2015, a second draft for a new act, supporting consumer rights, has been released. The Consumer Bill of Rights does not seem to include an individual right of action but seeks to provide penalties and includes additional consumer rights when enforced.[75]

Some market areas in the US already included precautious actions into their legal system. States like Vermont and California have introduced bills that enable them to introduce privacy laws into their constitution. It has not happened yet, but in a case of increased importance for US companies to comply with European standards, it will be easier to introduce necessary regulations for the US business environment.[76] This can be seen as an important step towards the acceptance of European privacy interests as a global standard.

Furthermore, experts see the major difference to European prospective in the given opt-out option rather than opt-in. This is conceived as a learning process on the issue of understanding of the nature of privacy protection for US consumers.[77] The US industry will experiences the possible change in consumer interest towards data protective entities once European legislation becomes effective. Non-compliant companies then have to expect greater expenses to adjust to a new global standard and to sustain their image.

[74] Israel, 2015, pp. 13-14
[75] Marshall, 2015, p. 614
[76] Ibid., pp. 616-617
[77] Ibid., p. 628

3.3 Conclusion

The most important objectives for future data protection law were ascertained in the Safe Harbor Ruling. Taking those into account, the aim of the new regulatory changes is to harmonize jurisdiction throughout the EU, enable claims to be enforced extraterritorially, strengthen user rights and hold organizations and companies accountable for their actions by assuring data protection through evidenced procedures and authorization.

The GDPR provides the fundament to these objectives. Yet, corresponding law and regulations such as SCs and BCRs should be reviewed and adjusted accordingly to interact with new law instead of bypassing important measures of protection.

Furthermore, currently discussed bilateral agreements such as TTIP, TiSA and the EU-US Privacy Shield contain debatable portions. It is possible that they endanger the fundamental objective of data protection by outlawing the GDPR as the superior regulation.

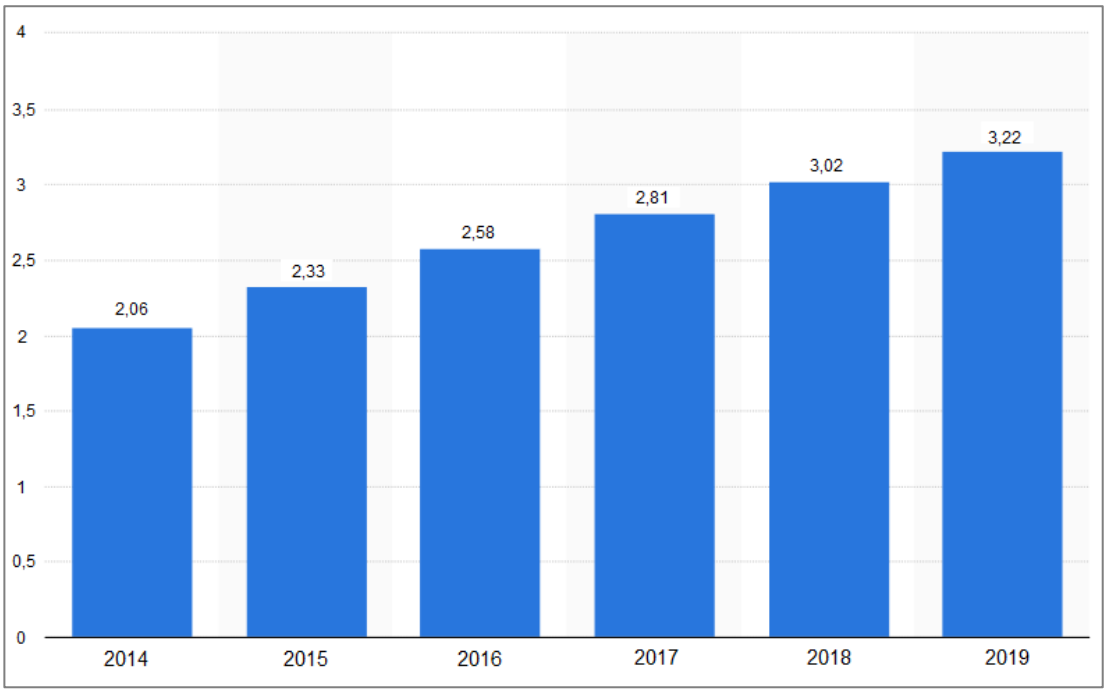
The US started paying closer attention to the enhancement of consumer rights and the awareness of privacy issues increases. However, definite data protection law is still absent in US jurisdiction. This has been and continues to be the greatest challenge in negotiations between the US and EU.

4. Consequences for the EU and US Economy

4.1 The Relevance of Data Privacy Law for Economic Development

From third world countries to developed economies, the electronic connectedness and involvement has developed rapidly. To illustrate this, Figure 1 shows the consistent growth of mobile internet users, with the

Figure 1: Number of mobile internet users from 2014 until 2019



X: time in years; Y: Number of users in billions

Source:(Statista, 2016

mobile connection being only one option of all possible e-connections, with a prognosis until 2019. [78] The worlds' population currently amounts to an estimated 7.3 billion.[79] From 2012 to 2013, the average adoption of smartphones in OECD countries reached an average of almost 50% in 2013. Consumers use mobile devices for a multitude of activities. Not only emailing and social networking account to the scope of mobile activities, but also more sophisticated operations such as online banking or online purchases are increasingly pursued through mobile connectedness. Besides the increased usage of mobile devices, also the frequency of usage has grown. 40% of

[78] Statista, 2016
[79] United States Census Bureau, 2016

consumers in OECD countries have used their smartphones several times per day for social networking and browsing purposes in 2013. [80] Within this development, the importance of social interaction through digital inclusiveness increased. Therefore, electronic inclusiveness became a profound business component to encourage social interaction with business entities. [81]

Following this, the importance of information and communication technologies (ICTs) and the internet in business models and strategies is expanding rapidly. Rates for adoption and using ICTs among OECD countries show that almost all businesses rely on ICTs. In 2014, nearly 100% of large companies were connected to broadband, while 95% of all business entities with more than ten employees had a broadband connection.[82] "National digital strategies are cross-sectoral by nature and in many instances are designed explicitly to boost countries' competitiveness, economic growth and social well[-]being."[83] Since the increased connectedness has become such an integral part throughout the society, the consequences of policy changes for the economy are extensive. "[The] impact is so profound that no sector remains unaffected." [84]

Detecting the financial profit behind this progress, whole economies developed a digital dependency to "reap economic benefit".[85] The US already holds the biggest players in the digital market. Companies like Microsoft, Google, Facebook, SAP, etc. are global actors and hold most of the market shares in their segment.[86] At European level, there is one vital policy framework seeking to increase Europe's economic share: The Digital Agenda for Europe (DAE).[87] The aim is to increase and sustain market power and welfare by entering further into the promising digital market.[88] In the DAE one of the objectives is "to speed up the roll-out of high-speed Internet and reap

[80] OECD, 2015, p. 54
[81] Andreasson, 2015, p. xxi
[82] OECD, 2015, p. 47
[83] Ibid., p. 21
[84] Ibid., p. 20
[85] Andreasson, 2015, p. xxi
[86] Windows: Global makret share for operational system Windows7: 53.71% : netmarketshare - Desktop Operating System Market Share, 2016; Google: Global market share of search engines January 2016: 88.36%: Statista - Worldwide desktop market share of leading search engines from January 2010 to January 2016, 2016
[87] Helsper and van Deursen, 2015, p. 137
[88] Ibid., p. 138

the benefits of a digital single market for […] firms"[89] and additionally, the "circulation of content with high level of trust for consumers and companies on digital platforms as regulated by national legislation"[90]. Furthermore, citizen rights, assurance of training in skills regarding information technology (IT) and the access to personalized services is backed up by the Social Investment Package (SIP).[91] Hence, there is a clear aim from the European side to oppose to the influence of US companies by investing into enhanced strength on the own market.

With the increase of global digital dependency, more companies are affected by international data protection law. Most firms rely on the outsourcing of IT functions or choose to buy IT services instead of investing into it themselves. However, the use of information technology in businesses, mainly from the secondary and tertiary economic sector, is very common.[92] Still, the companies, as the collecting and processing entities, are liable under the law. Additionally, the definition of what constitutes personal data has been expanded to include pretty much any possible identifier, especially if profiling of data is carried out.[93] As mentioned before, the GDPR promotes the implementation of security mechanisms into new tools in a very early stage of development. Thus, suppliers that incorporate European standards into their devices have an increased chance to profit in the European market. The affect digresses to all companies associated with digital services, ranging from the tool user to the producers of digital devices and eventually their suppliers.

Despite the rapid progression, the digital economy already faced two vigorous challenges, the dot-com bubble from 1997 to 2000 and the Double-Dip crisis from 2007-2009. Although recovering from these major set-backs, "the digital economy has not yet reached full potential". [94]

The digital economy of the US has developed significantly faster in comparison to that in the EU. Starting in the 1990s, the US has spotted the

[89] European Commission, Europe 2020 - A strategy for smart, sustainable and inclusive growth, 2010, p. 6
[90] Ibid., p. 21
[91] Helsper and van Deursen, 2015, p. 138
[92] Peukert, 2013, pp. 1-3
[93] Heureux, 2015, p. 309
[94] OECD, 2015, p. 17

opportunities given by the newly arising digital market and started investing heavily into its development. Throughout the 1990s the US spent about three times more of their nominal GDP shares into IT and six times more into the IT market in total.[95] The US investment into venture capital is at its highest level now and important business industries like the semiconductor market are growing.[96] As a result the market in the US was able to grow fast and establish strong positioning. The biggest players, such as Google, Facebook, Microsoft, were all founded in the US[97] and have gained an almost monopoly-like ambassadorship by providing omnipresent products throughout the world. "Moreover, sixteen US companies and only three European companies were ranked among the twenty largest big data vendors in 2013."[98]

For the upcoming economic evaluation, the following assumption on the jurisdictional future is made: The GDPR will be adopted by the European Parliament and European Council in 2016 and will therefore be effective in 2 years from now. Standard Clauses and Binding Corporate Rules will be reviewed and adjusted according to GDPR needs. As other non-EU countries already started adopting the European approach in data protection, the enforcement of legal consequences will increase. The awareness of extraterritorial means will also increase globally.

4.2 Economic Consequences due to the Outcome of Regulatory Changes

4.2.1 Harmonization of European Law

Through the new regulation government and non-government jobs will be created throughout Europe. Harmonized interpretation of law will strengthen penalty and enforcement. In the prevailing jurisdictional framework, the penalties as well as enforcement vary strongly in the different member states. In some member states, e.g. Spain and France, the interpretation of the law is stricter than in others, e.g. the United Kingdom (UK). Therefore, the

[95] Welfens und Jungmittag, 2003, p. 16
[96] OECD, 2015, p. 36
[97] Google, 2016; The Guardian, 2007; Microsoft, 2016
[98] Ciriani, 2015, p. 44

chances for companies to face law enforcement are higher in those member states where law is taken more serious and executed stricter. The new regulatory framework follows the rather strict approach and is imminently and uniformly applied in all EU/EEA countries.[99] Hence, the level of enforcement will increase throughout the EU. To ensure the execution of law, DPAs have to increasingly engage into audits and check-ups throughout the market. Also, companies need to invest into experts to control data control and processing internally to receive authorization. This can be seen as a great expense for the government and business entities. However, it is also supporting the industry behind the legal system. To execute the surveillance of the new mechanisms, the demand for skilled labor will increase which creates jobs. Positive effects on the economy therefore are increased tax income for the government, increased demand of goods and therefore increased trade in goods, growing GDP and an overall increase in welfare.

By harmonizing data privacy law, Europe will reach a better positioning by investing into digital trust within their economic area. An OECD survey from 2014 on priority areas in the digital economy revealed that *security* and *privacy* range among the top three in their importance. Furthermore, in several other surveys a rise in trust concerns was pointed out. They ascertained that out of all the participants, 91% felt that they were not in control over their personal data anymore and overall concerns about privacy have risen by 64% within one year. Therefore, providing trust in the digital economy seems to become an inevitable success factor to exploit economic opportunities.[100] The EU attempts to enhance the digital market by creating trust and competence for European products through legislative backup. As explained by Viviane Reding, the Vice-President of the European Commission: “Trust in a coherent EU regulatory regime will be a key asset for service providers and an incentive for investors looking for optimal conditions when locating services”[101]

Therefore, through the increase in created trust the EU economy might benefit from an increase of Foreign Direct Investments (FDIs) into the EU. Implementing coherent law throughout Europe demands expenditures on

[99] Heureux, 2015, p. 309; also: Svantesson, 2014, p. 71
[100] OECD, 2015, pp. 62-63
[101] Svantesson, 2014, p. 57

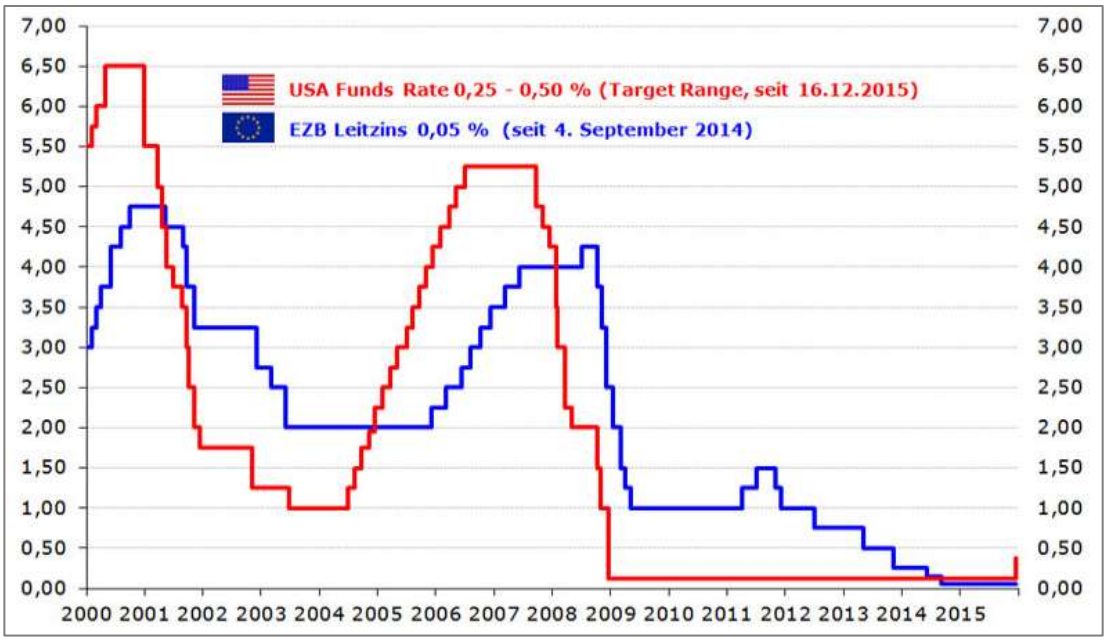
human resource, job training and administration.[102] The changes relate mostly to new tasks that "concern the implementation of the new consistency mechanism which will ensure coherent application of harmoni[z]ed data protection law, the adequacy assessment of third countries for which the Commission will have sole responsibility, and the preparation of implementing measures and delegated acts".[103] For this, the GDPR proposal states an estimated expenditure for the period of 2014-2020 of approximately 40 billion Euros in total.[104] This amounts to roughly ¼ of the available means of payment estimated for the financial framework of the EU.[105] Despite the given willingness to invest into the legal framework, further government investments into the economy by, for example, supporting market relevant education or providing subsidies are limited. Nevertheless, companies or investors might want to seize future risks by complying with upcoming law and therefore reason to evolve directly within the necessary legal environment. Companies would also benefit by exploiting upcoming economic support in that area and the created image of trust on digital products from the EU which will overspill to the brands of entities situated in the EU. Therefore, an increase of FDIs into Europe for the digital market is most likely to occur. For the European economy this will have several positive effects. One of them is the potential of job creation through an increased number of companies that demand labor. The overall unemployment rate will decrease, which will lead to an increase of government income through taxes, less spending on social services and a total increase in welfare. The government income then can be spent to further boost the economy by, for example, investing into the needed fields of education.

The increased demand for investment gives Europe the opportunity to strengthen its inner-market. As well as FDIs may flow from non-EU countries, also investors within the EU will be interested to exploit the benefits of a trustworthy economic environment. As Figure 2 shows the development of th

[102] Gilbert, European Data Protection 2.0: New Compliance Requirements In Sight - What The Proposed EU Data Protection Regulation Means for U.S. Companies, 2012, p. 819
[103] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, pp. 113 f.
[104] Ibid.
[105] Bundefinanzministerium, 2014

funds rate of the US and European Central Bank (ECB) since 2000. IT is obvious, that the ECB funds rate has reached a significant low of 0,05% since September 2014.[106] Hence, banks are able to loan money on a simultaneously low rate which attracts entities to lend money for their endeavor.[107] Not only powerful enterprises will be attracted, but especially entrepreneurs or SMEs will be triggered to invest heavier into their businesses ideas as loans are cheap. Flourishing small enterprises will provide an increased variety in supply on the market. The growing market mix will support inner-EU trade which will generally lead to a gain in profit for the trading countries.[108]

Figure 2: US and EU Funds Rates from 2000 - 2016



X: Time in years; Y: Funds Rate in percent

Source: Kerbler, 2015

Following this, the EU, as a compound of different countries, is able to benefit from comparative advantage. Despite the goal of the EU to create a uniform economic area with equally developed member states[109], the different stages of economic development still vary between countries. As already said, the digital market combines all business areas. By investing into pools of

[106] Kerbler, 2015
[107] Bofinger, 2015, pp. 378 f.
[108] Bofinger, 2015
[109] European Commission, Die Grundprinzipien der Union, 2016

specialization in the different member states, the full potential of skills and labor can be achieved and inter-European trade increases to ensure a distribution of benefits in the EU.[110]

Moreover, the GDPR will support the establishment of genuine competition within the EU digital economy. The new legal framework "does not address the asymmetry resulting from the classification of digital services"[111]. Therefore, all business service providers have to obey the same rules when controlling and processing data of EU-citizens. This also leads to the conclusion that transatlantic data flows will not be forged by the execution of the GDPR due to the uniform exertion and impact for both, EU and US business entities.[112]

The US economy will also benefit from investing into the EU area. As Figure 2 shows, the fund rate in the US has almost developed simultaneously to the EU and is ranging between 0.25% - 0.5% since December 2015. This gives US investors the chance to either invest directly into the EU market through FDIs or to loan money inexpensively in the US and invest indirectly into the European market through subsidiaries. Both ways give US companies the chance to increase their market power and share across borders. Powerful business entities have a higher demand in their products than products than others. Hence, they profit from high revenues. Sustaining US businesses in the EU rewards them with increased influence in the market. The demand for innovative and brand products is there. Since US businesses inherit better market positioning, the European market depends on products originating in non-EU countries.

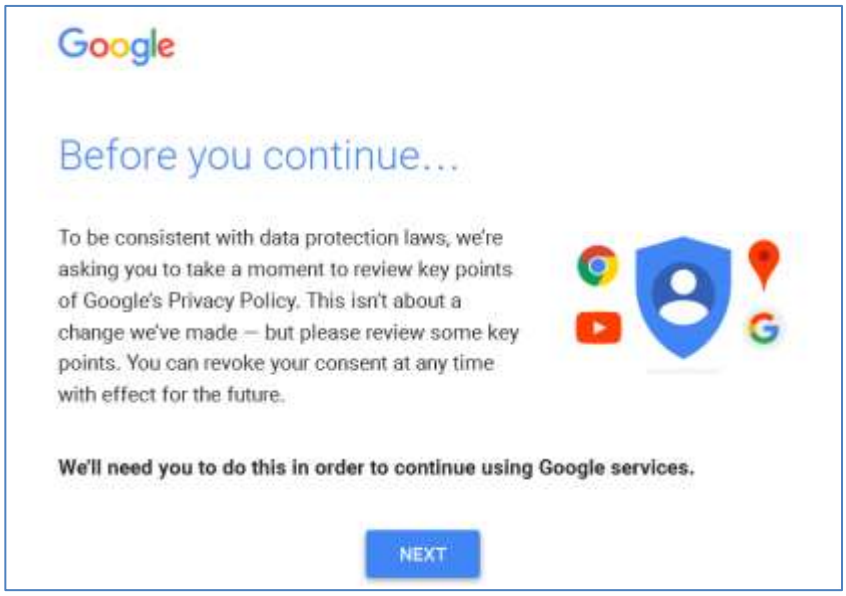
Overall, the harmonization of European law seems to profit the EU economy more than the US by generating trust as an important economic asset. Increased investments into the European market will boost the economy. US competition only has the chance to hop on the boat by complying with EU legal standards as well as by investing into European economy themselves.

[110] Bofinger, 2015
[111] Ciriani, 2015, p. 49
[112] Ibid.

4.2.2 Extraterritoriality

It is without doubt mandatory for US businesses to comply with European law when they attempt to do business in the EU. In Germany, companies already started to take proactive actions towards the new regulatory needs and made consumers opt-in on their unchanged data policy before using their products. Since the beginning of March 2016, on the Google website, as well as Google-product websites like YouTube, the business confronts the consumer with their data policy and asks for acceptance as seen in Figure 3. The information includes links to the several topics of their data policy as well as giving other options of using the product if the user is concerned data will be breached.[113]

Figure 3: Google Privacy Policy Awareness



Source: Google, 2016

Moreover, on-site audits by the DPA have already been executed since the late 1990s. The first audit with extraterritorial background has been carried out on Citibank in 1996. This serves as an example of why foreign policy with extraterritorial claim matter to US companies.[114]

As for now, the EU compensated the absence of extraterritorial jurisdiction by making it mandatory for non-EU enterprises to locate servers within the

[113] further screenshots enclosed in Appendix
[114] Svantesson, 2014, pp. 74-75

EEA.[115] This way, enterprises could be hold responsible for data breach happening since their servers were located within an area where European jurisdiction avails. As mentioned before, this approach might be neglected through bilateral agreements.

Then again, one good reason to support trans-border data flows is that it can also imply the protection of privacy in itself. In 2010, the United Arab Emirates (UAE) was about to ban BlackBerry messaging services due to their encryption during a transmission process happening on Canadian ground. For the UAE this meant that data could not be accessed and surveilled by their government agencies.[116] As much as accessed data can be breached, the location of data processing enterprises is an important factor of controlling and protecting it.

Handling privacy issues globally will eliminate trade barriers. The inducement for SMEs to participate in the e-commerce industry has been moderate, especially across borders. One reason is "consumer resistance to cross-border-purchases"[117] due to the concern that consumer rights are not protected. Ensuring data privacy protection through global standards eliminates a part of such trade barriers. Therefore, Start-Ups and SMEs are liberated from another obstacle for their business development.

As mentioned before, parts of the US economy also insinuated a development towards EU privacy standards.[118] Yet, the extraterritoriality of European jurisdiction has great potential to harm the economic relationship between the US and EU. The internet and development of digital tools has made it easier to access comprehensive data flows beyond geographic restrictions. Due to this, an extraterritorial reach of EU-law is necessary to efficiently protect citizens from data breach "and to have an effective remedy against those responsible".[119] In a matter of companies expanding into non-EU areas or areas that are not declared to offer an "adequate level of

[115] European Commission, 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, 1995
[116] Kuner, 2011, p. 24
[117] OECD, 2015, p. 55
[118] Marshall, 2015
[119] Svantesson, 2014, p. 77

protection"[120] they remain liable for. Since the awareness of data protection and associated concerns are increasing among OECD (Organization for Economic Cooperation and Development) countries[121], interests of all affected citizens will be supported by this endeavor. Even if the enforcement of European standards remains difficult in non-EU countries, data breaching will reflect negatively on the company's image.

From another perspective, it could also be seen as an approach that heavily influences the market by forcing European interests as a new global standard upon it. The assertive attempt to provide law with an extraterritorial reach that regards data privacy issues embeds the interest to standardize global solutions based on European interests. Even if it turns out that the law cannot be enforced as easily in the US, the enforceability will leave US companies with the risk of possible sanctions for non-compliance or economic disadvantages if they support European law.[122] Besides, the US government and jurisdiction do not share the European opinion on the need of data protection. This could lead to severe political and economic reactions in a dispute over market power with negative effects on both parties.

The US, for example, could decide to enact legislation that will block the execution of European policies. Such "blocking legislation"[123] seeks to prohibit the supply of evidence in foreign cases, attempts to hinder legal enforcement and forbids compliance on orders from foreign authorities.[124] As a result, European authorities and citizens will be unable to make use of their right to fair remedy when the responsible collector or processor of their data is situated in the US. This could lead to the following example settings that will decrease trade between the two economies and generate a loss in trust, comparative advantage and welfare.

US companies will realize that they cannot be hold legally accountable for data breach when located in the US. Hence, they will withdraw their subsidiaries from the European area to solely provide their business activities

[120] European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, Article 41
[121] OECD, 2015
[122] Svantesson, 2014, pp. 59 and 101
[123] Svantesson, 2014, p. 94
[124] Ibid., pp. 94 f.

from US headquarters. The US companies that provide online services are still able to do business in Europe since these are geographically independent. There might be a loss in trust in US products which may lead to a decreased demand. This would incorporate a total decrease in trade between the US and EU which will have a direct negative effect on the GDP in both economies.

The newly gained trust-image through European law will suffer if it turns out to be inefficient. Other companies may see a chance in relocating their businesses to non-EU countries to bypass European policies. A loss of market power for the European economy will be inevitable. Although the EU owns a strong market share in the digital industry now, the economy will suffer from the loss of incoming tax, work places and the consistent demand in goods that will require import expenditures.

In order to protect the rights of EU-citizens, the EU could react by not giving authorization to foreign companies. The non-authorization of specific firms is not a direct trade barrier but can have a limiting effect to the economy which will again harm the overall trade with a negative effect on GDP and welfare for both economies. Despite this, it could lead to a possible dispute under the World Trade Organization (WTO). Issues in this regard are lying in ambush since the Safe Harbor Decision from 2000.[125]

Besides the non-authorization of businesses, also the GDPR itself is seen as "protection policy"[126] with negative influences on the world's most competitive business entities from the US.[127] Increased production costs and entry barriers are argued to affect US companies disproportionately due to their strong positioning in the European market. Whereas TTIP is supposed to raise bilateral trade by 0.7%, higher costs in production through the GDPR could decrease bilateral trade by over 0.5%.[128]

Whether foreign claims should be supported by the national government surely depends on the limiting effect they have on their economy. Being the less developed economy in terms of accepting privacy matters as a natural

[125] Shapiro, 2003
[126] Ciriani, 2015, p. 46
[127] Ibid.
[128] Ibid., page 47

business cost, US entities are not supported by the government to enhance their privacy standards. Thus, economic consequences of the extraterritorial reach of European law will affect US businesses heavier since their risk of non-compliance is higher. After all, an "aggressively pushed approach has the potential to become the dominant one, or even the only viable one"[129]. The European approach is certainly supported by other countries, such as China, Australia and Russia, which also seek to implement data protection law.[130] A future trend towards stricter data privacy matters will be a setback for the US economy through proportionately higher business expenses and the need to reconstruct business strategy and products, while the EU can exploit the benefits of a growing market by investment and gain in trust. The EU governments might additionally take the opportunity to fasten the development process with subsidies.

4.2.3 Increased Consumer Rights

The scope of companies exposed to data privacy law increases with the new regulation. The most famous companies in this industry are already known for their unlawful business practices and legal actions have been successful in the past. In 2009, a class action lawsuit has been carried out against Facebook because information on consumer action on associated websites like Ebay have been collected and stored without the consent of users and without an explanatory use of the data. The, for this action, introduced "Beacon"[131] tool has been out of order since.[132] In 2013, the synchronization of smartphones with network platforms caused concerns due to an intrusion into consumers' privacy. Facebook wanted to process information from Android short message services (SMS) and multimedia messaging services (MMS) to create user calendar appointments, update appointments and sending notice to email addresses without the user's being noticed upfront.[133] Another example for consumer surveillance is Google, whose front website has more than 100 million visitors daily. Google works with promotional partners that pay for products to be published for certain search criteria of the

[129] Svantesson, 2014, p. 101
[130] Marshall, 2015, p. 624 f.
[131] Verheijden, 2015, p. 88
[132] Ibid.
[133] Ibid., pp. 91 f.

consumer. The consumer will only be confronted with promotions linked to their search and therefore perceive advertisement as an enrichment rather than disturbance. The advertising entities are even able to follow the interests of potential clients, the consumers. Companies are able to access the consumers' data through cookies and synchronize with or possibly store them in their own big data pool.[134] However, the law does not only affect powerful businesses like Facebook or Google. More and more businesses work with an online presence or IT-tools to control and process consumer data. "Most websites track the 'click stream data' of their visitors to make an inventory of their interests and requirements."[135] Therefore, all businesses that cooperate in the digital market are exposed to the legal framework.

US companies may experience the legal effects heavier than EU companies. The most famous digital products that are used on a daily basis by worldwide consumers are product from US companies. Google is dominating the global market of search engines with 88% market share in 2014. In 2013, Facebook and Google together were responsible for 70% of the overall revenue.[136] Consumers use search engines and social networks on a daily basis. Through the increased awareness of data privacy concerns the consumer will reflect and question the most popular and frequently used products. Hence, not only will the litigants' focus be on the MNEs, also the quantity of possible claims is much higher than for products coming from SMEs and Start-Ups.

Stronger consumer rights and their ability to claim for compensation imply a rise in compliance costs for businesses. A survey from Ovum, where IT decision makers have been questioned, highlights, that "over 70% of respondents expect to increase spending in order to meet data sovereignty requirements, and over 30% expect budgets to rise by more than 10% over the next two years."[137] „The new Regulation includes a purpose limitation and data minimization will harm study outcomes. Companies are regulated more strictly and even have to conduct Privacy Assessments before launching a new product."[138] These expenses will affect EU and non-EU products equally

[134] Clasen, 2015, pp. 249-258
[135] Svantesson, 2014, p. 73
[136] Ciriani, 2015, p. 44
[137] Loshin, 2015
[138] Heureux, 2015, pp. 309-310

and could lead to a short-term decrease in overall compliant supply and increase of product prices.

The “one-size-fits-all” approach on sanctions incorporates an unproportioned risk for companies. The sanction on data breach can reach up to 2% of the annual worldwide turnover and is defined without a definition that considers a level of severity in unlawful behavior.[139] Sanctions upon non-compliance as well as the obligations of purpose limitation and earmarking of data controlling and processing activities[140] may lead to companies being “more reluctant to take risks and [being] more cautious before rolling out new innovations.”[141]

Almost like the extraterritoriality, stronger consumer rights have the potential to effect US business to a greater extent than those in the EU. Nevertheless, it bares great risks for all business entities in the digital industry and may lower innovation rates. This will effect both economies by slowing down product life-cycles and overall competition in the market.

4.3 Impact of Related Economic Circumstances

To specialize on European standards it makes most sense for investors to locate their business entities within the EU, where they can closely follow the jurisdictional development and be in direct exchange with experts. Not only the variety of digital business will increase but also the industry sector of consulting businesses has the opportunity to grow due to increased demand in legal expertise. In the long-term, the quantity and quality of specialized businesses will increase within Europe. Thus, the demand for skilled labor will increase as well.

One of the biggest problems for the European economy is the lack of skilled labor. “European policy emphasizes training (entrepreneurs) to work in IT industries, while there is still clearly a lack of knowledge of the basic skills

[139] Svantesson, 2014, pp. 74-75
[140] von Grafenstein, 2015, p. 790; also: European Commission, 2012/0011 (COD) - 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 Privacy Regulation), 2012, Article 6
[141] Heureux, 2015, pp. 309-310

needed for “everyday” jobs for volunteer intermediaries helping others to get online.”[142] “The evaluation of policy effectiveness beyond infrastructure provision, related to digital skills and engagement, is poor. This is problematic because individuals’ skills and motivation seem more important than infrastructure, especially in northern and western European countries where diffusion rates are reaching saturation.” Policies focus on supply rather than on demand.[143]

The European economy is at risk to harm economic growth due to non-employability of labor. E-skills are mandatory to support and sustain competitiveness, employability and growth. In the EU, e-skills are not yet visualized as a long-term policy need. Additionally, the number of graduates from computer science from the EU seems to decline. [144] Low labor productivity points out the weakness of technology enterprises and inefficient subsidization on Research and Development (R&D).[145] In order to provide for the demand of labor in the rapidly growing market, the EU needs to include a long-term policy for needed education into their agenda. Meanwhile the growth of the economy throughout Europe is at risk due to non-employability of labor.

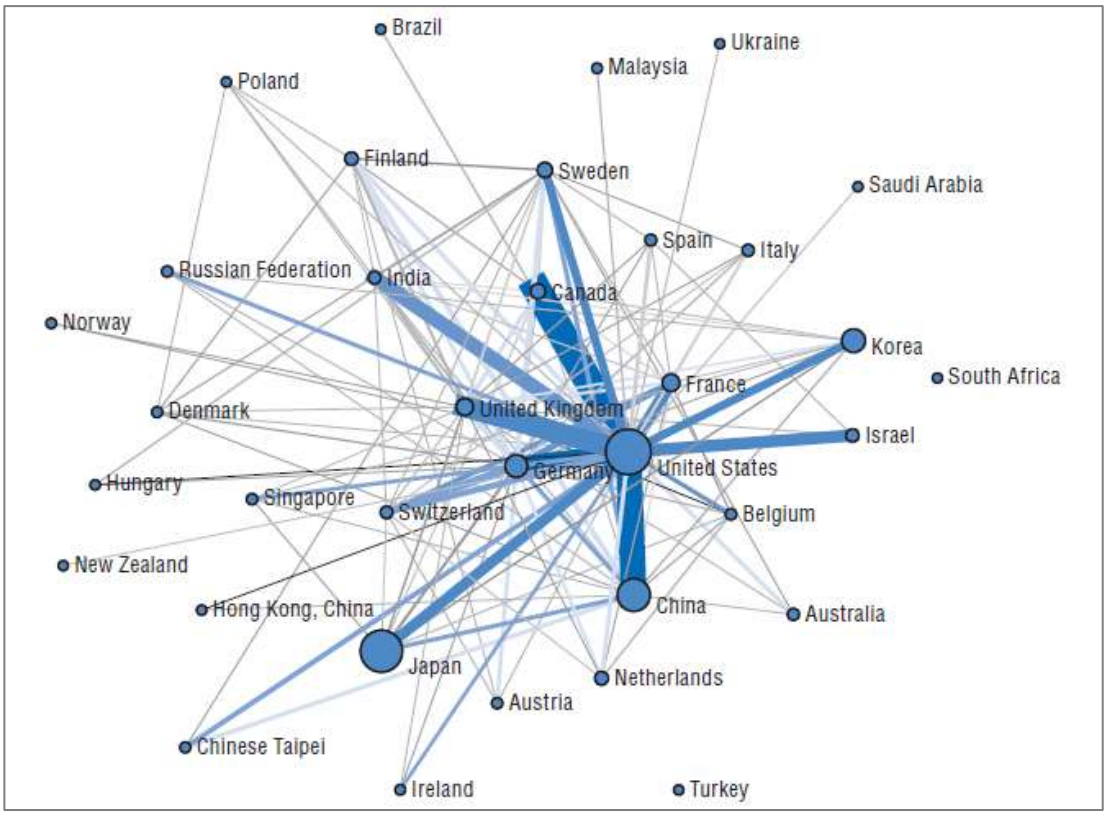
Therefore, European businesses are left with greater expenses on the economic development than US competitors. The US remains in a superior positioning on the market. In the US, labor productivity growth increased considerably faster than in the EU. [146] US productivity growth has benefited from growing trade due to rising import penetration and heavy investment since the 1990s.[147] In a situation of high demand and low supply, European companies are forced to pay extensive salaries to engaging experts. [148] Furthermore, competitiveness through market knowledge and innovation expertise can only grow slowly for EU businesses because they need to rely on less experienced employees than required. [149]

[142] Helsper and van Deursen, 2015, p.143
[143] Helsper and van Deursen, 2015, p. 142
[144] E-skills gap a concern for EU, 2013
[145] Welfens und Jungmittag, 2003, p. 51
[146] Ibid., p. 16
[147] Ibid., page 51
[148] E-skills gap a concern for EU, 2013
[149] Ibid.

Moreover, this makes the European economy partially dependent on the US competitors. The European economy will profit from US companies investing into the market as their businesses incorporate knowledge and skills in products and the required labor. If in any case US companies decide to leave the European area due to privacy policies, this could have negative effects on labor productivity and the supply of skilled labor in Europe.

Another important factor is the power over already invented ICT products. "Registered designs can be used to proxy innovation in relation to the aesthetic feature of products. They can also provide information about product differentiation and customi[z]ation and, more generally, about the role played by design to shape competition in the marketplace." [150]

Figure 4: International cooperation networks in ICT-related patents, 2010-2012



Whole counts of internationally co-invented patents

Source: OECD, 2015

The US retains a superior deployment when it comes to registration of innovation in the EU. Besides Korea, the US accounts to one of the most

[150] OECD, 2015, p. 97

active economies who register ICT and audio-visual related products. US business entities subsequently gain market share and enhance their power and influence on the European market. Figure 4 highlights international cooperation networks in ICT-related patents from 2010-2012. The illustration underlines the influence of US companies in this regard. Meanwhile countries like Germany are losing market share.[151]

A high number of patented products in the EU resembles a positive development in the European economy. Increased innovation stands for a certain involvement in the economy, regardless of whether it is skilled or unskilled entrepreneurs who come up with new ideas. It means that the awareness of opportunities in the market increases and attracts people to follow their chances to pursue prosperity. Therefore, it can be assumed that the rise of interest in the market would fit perfectly with investments into R&D as well as market relevant education.

Again, the US has the opportunity to lead the digital market further by investing into the European market. Good inventions tend to be bought by MNEs quickly after their introduction on the market. Due to the high connectedness the potential of increased the use of a product can spread extraordinarily. Subsequently, innovative products are able to gain market share quickly. Therefore, the value of the brand or product will increase rapidly if accepted by the consumers. If the presence of US companies increases through investments in the European economy, not only MNEs like Google and Facebook but also smaller enterprises will profit from increased influence on the market. Thus, they are able to attract start-ups with their market power and brand image and sustain their influence by buying innovative business or by supporting business mergers of all kinds.

[151] OECD, 2015

5. Conclusion

The legal interests of the EU are introduced globally step by step. New regulations and policies implemented in this regard appear to increasingly influence global thinking and economic decision making. Even strong economies that do not or only slowly approach data privacy issues are affected by this development – like the US.

From an experts point of view, the market will increase in its international complexity and the location of business or data servers should not be an obstacle for business practices in the future.[152] Subsequently, this "new era of […] law"[153] provides reason for international negotiations on how trans-border data trade will be handled in the future. International dispute is a possible outcome, while

The European economy will certainly benefit from the enforcement of the new regulation. Gained trust is a strong asset when it comes to consumer protection with which the EU can exploit economic opportunities. The EU has the chance to increase their involvement in the digital market through an increase in businesses that supply corresponding products and support innovation and entrepreneurs as well as SMEs.

Increased competitiveness of the European economy by regulation gives incentives to other non-EU countries to apply the same standards. Countries like Australia and China start to approach data privacy issues and plan to implement them in their own jurisdiction. This could lead to more countries becoming competitive in the digital field and enhances the global market.

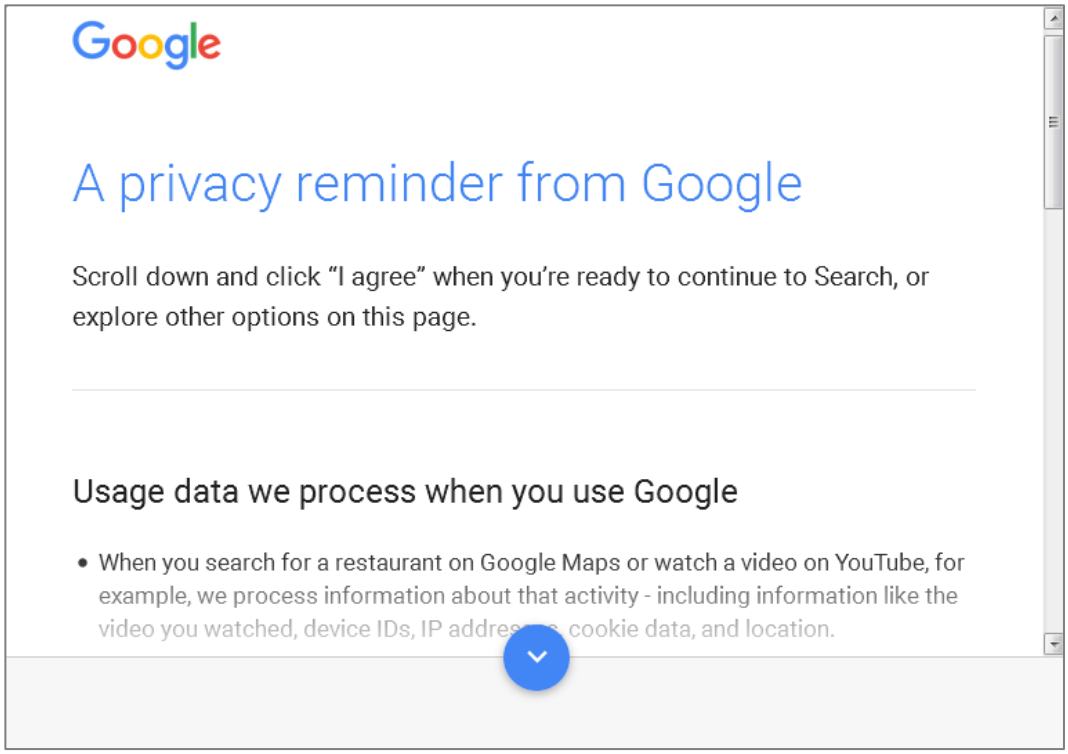
Yet, the US remains to be a strong competitor in the global market. Through their intense investments in the past, US enterprises have reached significant influence and power in the international market. Some even argue, that "Europe tries to compete with the US in an area where it cannot win."[154] To become stronger as an economic competitor, the EU has to take further measures to improve their positioning in the market. The lack of e-skills in labor and low investment into R&D are two major objectives to work on.

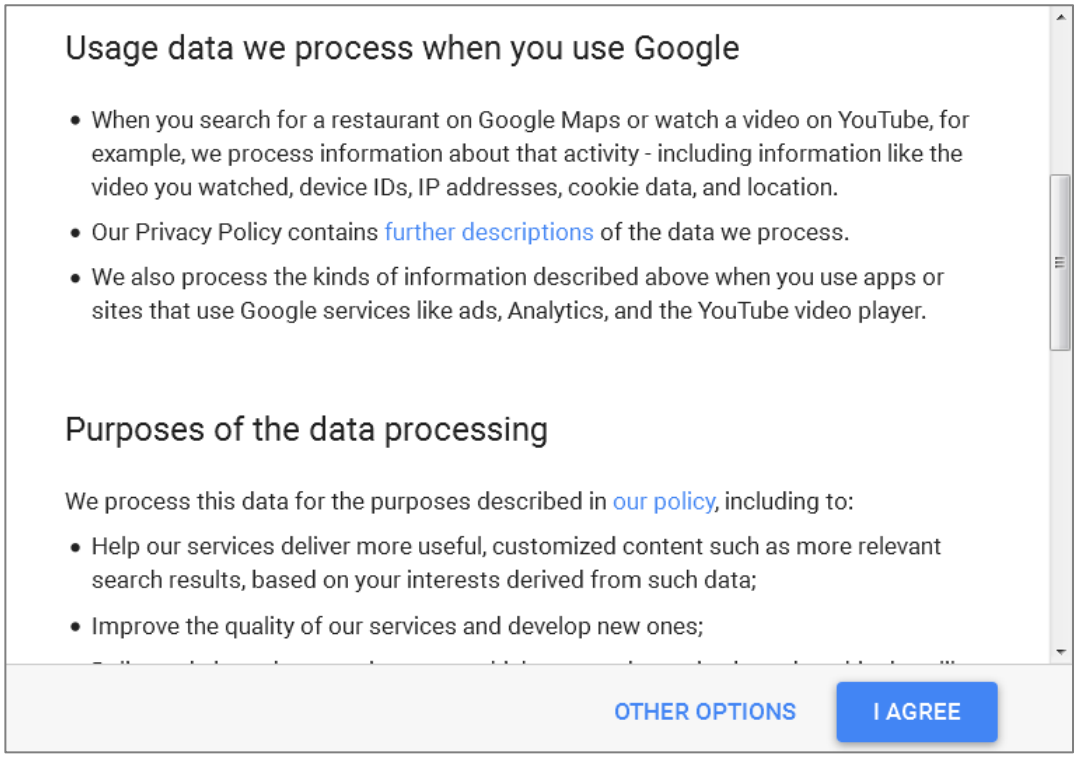
[152] Marshall, 2015
[153] Svantesson, 2014, p. 102
[154] Ibid.

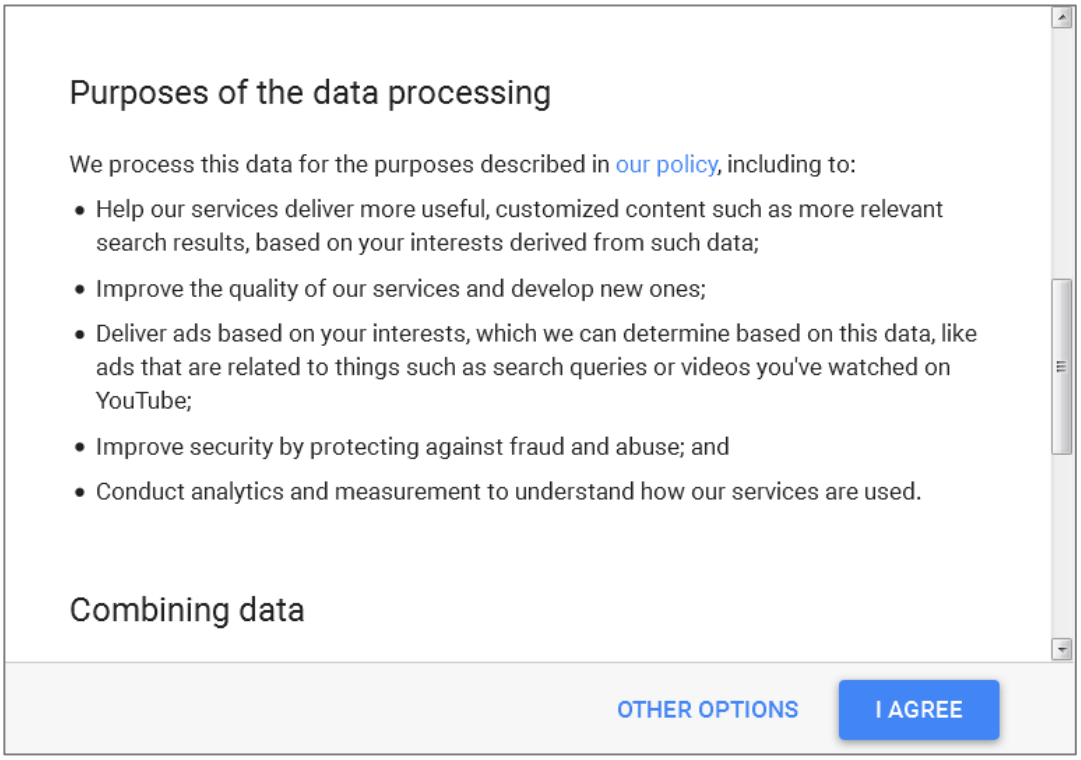
Appendix

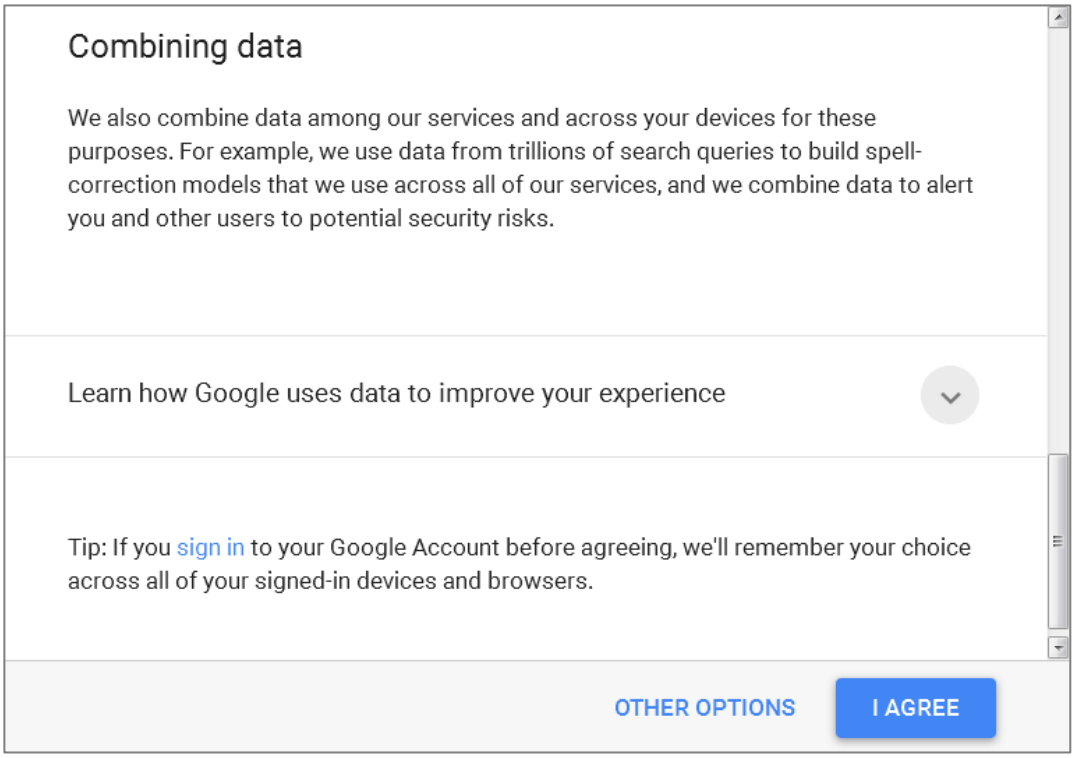
Google Data Privacy Policy Awareness

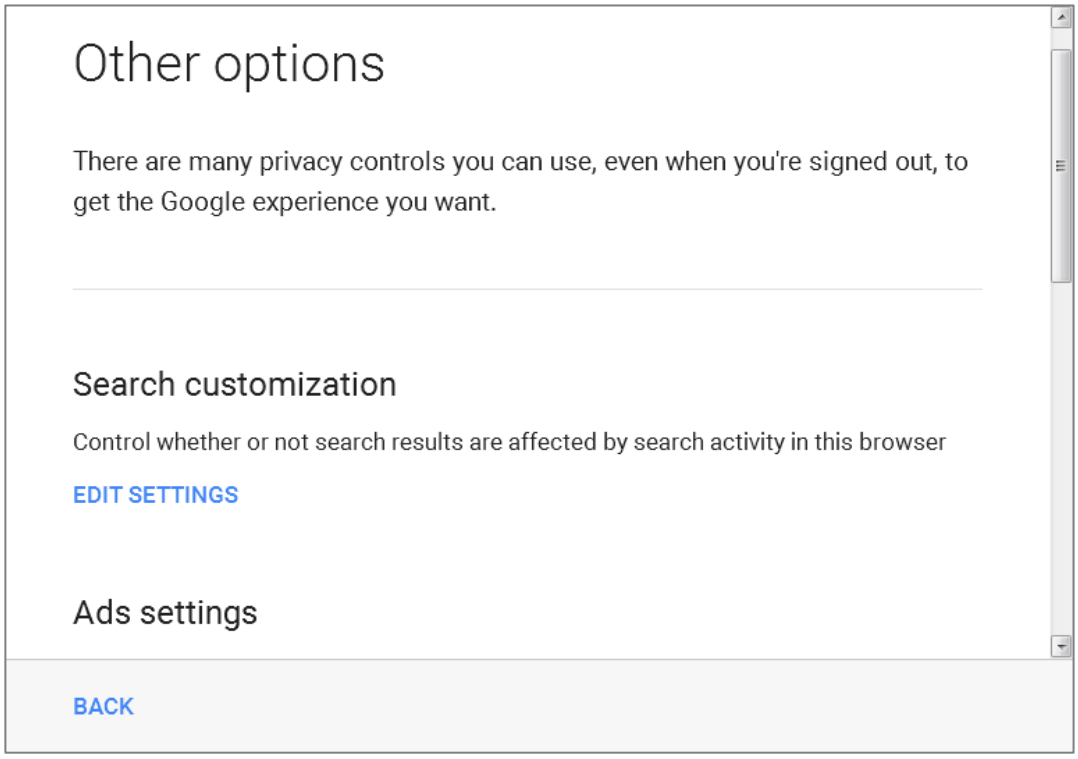
Source: (Google 2016)






Purposes of the data processing
We process this data for the purposes described in our policy, including to:
• Help our services deliver more useful, customized content such as more relevant search results, based on your interests derived from such data;
• Improve the quality of our services and develop new ones;
• Deliver ads based on your interests, which we can determine based on this data, like ads that are related to things such as search queries or videos you've watched on YouTube;
• Improve security by protecting against fraud and abuse; and
• Conduct analytics and measurement to understand how our services are used.
Combining data
OTHER OPTIONS
I AGREE


Combining data
We also combine data among our services and across your devices for these purposes. For example, we use data from trillions of search queries to build spell-correction models that we use across all of our services, and we combine data to alert you and other users to potential security risks.
Learn how Google uses data to improve your experience
Tip: If you sign in to your Google Account before agreeing, we'll remember your choice across all of your signed-in devices and browsers.
OTHER OPTIONS
I AGREE



YouTube Privacy Policy Awareness

Source: (Youtube 2016)

List of References

Andreasson, Kim. *Digital Divides - The New Challenges and Opportunities of e-Inclusion.* Boca Raton: CRC Press, 2015.

Article 29 Working Party. „ec.europa.eu - National filing requirements for controller BCR ("BCR-C").“ July 2015. http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf (Zugriff am 2nd. February 2016).

—. „ec.europe.eu - WP133: Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data.“ 10th. January 2007. http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/tools/index_en.htm (Zugriff am 2nd. February 2016).

Bofinger, Peter. *Grundzüge der Volkswirtschaftslehre.* Hallbergmoos: Pearson, 2015.

Bull, Hans Peter. *Sinn und Unsinn des Datenschutzes.* Tübingen: Mohr Siebeck, 2015.

Bundefinanzministerium. *Bundesministerium der Finanzen - Der Mehrjährige Finanzrahmen der EU 2014-2020.* January 29th, 2014. http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Europa/EU_auf_einen_Blick/EU_Haushalt/2012-02-26-mehrjaehriger-finanzrahmen-der-eu-2014-2020.html (accessed February 10th, 2016).

Ciriani, Stéphane. „The Economic Impact of the European Reform of Data Protection.“ *Digiworld Economic Journal* no. 97, Nr. 1st Q 2015 (2015): 41 - 58.

Clasen, Nicolas. „Data Driven Advertising bei Google und Facebook.“ In *Big Data im Marketing*, Herausgeber: Torsten Schwartz, 249 - 269. Freiburg: Haufe-Lexware GmbH & Co. KG, 2015.

Datenschutz, Dr. *Auftragsdatenverarbeitung - Was sind EU-Standardvertragsklauseln?* 2011.

https://www.datenschutzbeauftragter-info.de/auftragsdatenverarbeitung-was-sind-eu-standardvertragsklauseln/ (Zugriff am 2nd. February 2016).

de Hert, Paul, und Vagelis Papakonstantinou. „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals.“ *Computer Law & Security Review* 28 (2012): 130 - 142.

Dutton, William H., und Elizabeth Dubois. *Politics and the Internet.* New York: Routledge, 2014.

„E-skills gap a concern for EU.“ *Human Research Management International Digest*, 2013: 9-11.

European Commission. "2012/0011 (COD) - 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 Privacy Regulation)." 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed February 10th, 2016).

European Commission. "Charter of the Fundamental Rights of the European Union (2000(C 364/01)." *Official Journal of the European Union*, no. C 364 (2000): 1 - 22.

—. „Commission Decision C(2010)593 - Standard Contractual Clauses (processors).“ 2010. http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (Zugriff am 8th. February 2016).

—. "Data Protection Eurobarometer - Factssheet." June 24th, 2015. http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf (accessed December 20th, 2015).

—. *Die Grundprinzipien der Union.* 2016. http://europa.eu/scadplus/constitution/objectives_de.htm (Zugriff am 3rd. March 2016).

European Commission. „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.“ *Official Journal* L 281 (1995): 0031 - 0050.

European Commission. "Directive 95/46/EG of the European Parliament and of the Council." *Official Journal of the European Communities*, no. L 281 (1995): 31 - 50.

—. "Europe 2020 - A strategy for smart, sustainable and inclusive growth." *EUR-Lex.* March 3rd, 2010. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:em0028 (accessed February 15th, 2016).

—. *European Commission - Agreement on Commission's EU data protection reform will boost Digital Single Market.* 2015. http://europa.eu/rapid/press-release_IP-15-6321_en.htm (accessed December 16th, 2015).

—. *European Commission - EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield.* 2016. http://europa.eu/rapid/press-release_IP-16-216_en.htm (accessed February 10th, 2016).

—. „European Commission: Questions and Answers - Data protection reform.“ 21.. December 2015. http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (Zugriff am 28.. December 2015).

—. *Model Contracts for the transfer of personal data to third countries.* 2015. http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (accessed February 2nd, 2016).

—. *Overview of Binding Corporate Rules.* 2015. http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm (accessed February 2nd, 2016).

Fuchs, Jana C. "Personenbezogene Daten zwischen der EU und den USA." *Betriebs-Berater*, no. 51/52.2015 (2015): 3074 - 3079.

Gilbert, Francoise. „European Data Protection 2.0: New Compliance Requirements In Sight - What The Proposed EU Data Protection Regulation Means for U.S. Companies.“ *Santa Clara Computer and High - Technology Law Journal* 28, Nr. 4 (2012): 815 - 863.

Gilbert, Francoise. "Proposed EU Data Protection Regulation: The Good, The Bad, And The Unknown." *Internt Law* 15, no. 10 (2015): 20 - 34.

Google. 2016. https://www.google.com/about/company/history/ (Zugriff am 10th. February 2016).

Google. March 3rd, 2016. https://www.google.de?gfe_rd=cr&ei=YfvZVp-JFKu[8Qfe1p7QBw&gws_rd=ssl (accessed March 3rd, 2016).

Götz, Christopher. "Grenzüberschreitende Datenübermittlung im Konzern." *DuD - Datenschutz und Datensicherheit* 10, no. 2013 (2013): 631 - 638.

Helsper, Ellen Johanna, and Alexander J.A.M. van Deursen. "Digital Skills in Europe: Research and Policy." In *Digital Divides - The New Challenges and Opportunities of e-Inclusion*, by Kim Andreasson, 125-146. Boca Raton: CRC Press, 2015.

Heureux, Alain. "Regulatory Challenges for Big Data." In *Big Data im Marketing*, edited by Torsten Schwartz, 308 - 311. Freiburg: Haufe-Lexware GmbH & Co. KG, 2015.

Israel, Tamir. "Wikileaks - TISA Annex on Electronic Commerce: A preliminary analysis by the Canadian Internet Policy & Public Interest Clinic (CIPPIC)." June 3rd, 2015. https://wikileaks.org/tisa/ecommerce/analysis/page-11.html (accessed February 17th, 2016).

Judgment of the Court in Case C-362/14. (2015).

Kerbler, Gabriele. *Leitzinsen.* 2015. http://www.leitzinsen.info/ (Zugriff am 20th. February 2016).

Kuner, Christopher. *Regulation of Transborder Data Flows und Data Protection and Privacy Law: Past, Present and Future.* OECD Digital Economy Papers, No. 187, http://dx.doi.org/10.1787/5kg0s2fk315f-en: OECD Publishing, 2011.

Loshin, Peter. *TechTarget.* December 18th, 2015. http://searchsecurity.techtarget.com/news/4500267248/Compliance-costs-expected-to-rise-as-EU-GDPR-advances (accessed February 20th, 2016).

Madden, Mary, and Lee Rainie. "PEW Internet - Americans' Attitude About Privacy, Security and Surveillance." May 20th, 2015. http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (accessed December 20th, 2015).

Manich, Marlene, und Simon Assion. *Telemdicus - 5 Fragen zum Safe Harbor-Urteil des EuGH.* 2015. http://www.telemedicus.info/article/3001-5-Fragen-zum-Safe-Harbor-Urteil-des-EuGH.html (Zugriff am 20. November 2015).

Marshall, J. „Legal Problems in Data Management: The Impact of International Data Restriction Laws on U.S. Companies.“ *The John Marshall Journal of Information Technology & Privacy Law*, 2015: 609-632.

Mester, Britta Alexandra. "EU-Datenschutzgrundverordnung." *DuD - Datenschutz und Datenscherheit* 2015, no. 12 (2015): 822.

Microsoft. 2016. http://news.microsoft.com/facts-about-microsoft/ (Zugriff am 11th. February 2016).

netmarketshare - Desktop Operating System Market Share. 2016. https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qpsp=2015&qpnp=2&qptimeframe=Y (accessed February 20th, 2016).

OECD. *OECD Digital Economy Outlook 2015.* http://dx.doi.org/10.1787/9789264232440-en, Paris: OECD Publishing, 2015.

Petri, Thomas. „Die Safe-Harbor-Entscheidung - Erste Anmerkungen.“ *DuD Datenschutz und Datensicherheit*, December 2015: 801 - 805.

Peukert, Christian. *Essays on the Economics of Information Technology and Media.* München: Ludwig-Maximilians-Universität Mänchen, 2013.

Piltz, Carlo. *De Lege Data.* 2013. https://www.delegedata.de/ (Zugriff am December 2015).

Schrems, Max. *europe-v-facebook.org, First Thoughts on Decision C-362/14.* 2015. http://www.europe-v-facebook.org/EN/Complaints/PRISM/Response/response.html (Zugriff am 8.. November 2015).

Schriver, Robert R. "You cheated, you lied: The Safe Harbor Agreement and its enforcement by the Federal Trade Commission." *Fordham Law Review* 70 (2002): 2777 - 2818.

Shapiro, Eric. „All Is Not Fair In The Privacy Trade: The Safe Harbor Agreement And The World Trade Organization.“ *Fordham Law Review* 71, Nr. 6 (2003): 2781 - 2821.

Statista - Worldwide desktop market share of leading search engines from January 2010 to January 2016 . 2016. http://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/ (accessed February 20th, 2016).

Statista. 2016. http://de.statista.com/statistik/daten/studie/502548/umfrage/anzahl-der-nutzer-des-mobilen-internets-weltweit/ (accessed February 10th, 2016).

Svantesson, Dan Jerker B. „The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Business.“ *Stanford Journal of International Law* 50:1 (2014): 53 - 102.

The Guardian. 25th. July 2007. http://www.theguardian.com/technology/2007/jul/25/media.newmedia (Zugriff am 10th. February 2016).

"Transatlantic Trade and Investment Partnership - Trade in Services, Investment and E-commerce." *European Commission.* December 2015. http://trade.ec.europa.eu/doclib/press/index.cfm?id=1230 (accessed February 10th, 2016).

United States Census Bureau. 2016. http://www.census.gov/popclock/ (accessed February 28th, 2016).

Verheijden, Josina. *Rechtsverletzungen auf YouTube und Facebook.* Schriftenreihe - Recht der Neuen Medien - Band 67. Hamburg: Verlag Dr. Kovac, 2015.

von Grafenstein, Maximilian. "Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit." *DuD - Datenschutz und Datensicherheit* 12, no. 2015 (2015): 789 - 795.

Voßbein, Reinhard. *Datenschutz - Best Practice.* 5. Heidelberg: DATAKONTEXT, 2010.

Welfens, Paul J.J., und Andre Jungmittag. „Internet, Economic Growth and Globalization.“ In *Internet, Economic Growth and Globalization*, von Claude E. Barfield, Günter Heiduk, & Paul J.J. Welfens, 9-65. Heidelberg: Springer-Verlag Berlin, 2003.

Weniger, Robert. *Grenzüberschreitende Datenübermittlungen international tätiger Unternehmen.* Hamburg: Kovac, 2005.

„Wikileaks - Trade in Services Agreement - Annex on [Electronic Commerce].“ *www.Wikileaks.org.* May 2015. https://wikileaks.org/tisa/ (Zugriff am 10th. February 2016).

Youtube. 3rd. March 2016. https://www.youtube.com (Zugriff am 3rd. March 2016).

Declaration of Originality

I hereby confirm that

- I was the sole author of the written work.
- I have compiled it in my own words.
- I have documented all methods, data and processes truthfully.
- I have not manipulated any data.
- I am aware that the work may be screened electronically for plagiarism.

Hamburg, 14th of March 2016

_____

Stephanie Harringer[redacted]