Westfälische Wilhelms-Universität Münster
Institut für Politikwissenschaft
Supervisor: Dr. Matthias Freise

School of Management & Governance
Department of Political Science and Research Methods
Supervisor: Dr. Andreas Warntjen

Bachelor Thesis

The Challenges of European Data Protection Policy –

An Analysis of Supranational Decision-Making Processes

Julia Nickenig
Am Grafenbusch 70
46047 Oberhausen
Phone: (0208) 800752
E-Mail 1: j.nickenig@student.utwente.nl
E-Mail 2: julianickenig@uni-muenster.de
Student number: s1122193 (UT)
356470 (WWU)

Double degree program: Public Administration (B.A) / European Studies (B.Sc.)

Date of submission: 20.04.2011

Table of Contents

1 Introduction

'Everyone has the right to the protection of personal data concerning him or her.'

This right of privacy is codified in Article 8 (1) of the Charta of Fundamental Rights of the European Union. A broad definition is given in the second paragraph, stating that personal data can only be used in specified cases and with the agreement of the person concerned or some other legitimate aim.

Until the mid 1990s each Member State of the European Union had its own legislation on data protection policy. However, this was considered to be a hindrance for the internal market and its 'free flow of data'. Thus, in 1995 a first Directive was passed laying down the basic principles of European data protection policy. Subsequently, further legislative acts were passed in order to regulate more specific issues.

The circumstances in which data protection policy takes place are changing constantly. In an era of rapid technological advancement, new developments and inventions are becoming increasingly popular. The last decade has seen, by way of example, an exponentially increasing popularity of online shopping and social networking. While facilitating communication and the provision of goods and services, those developments also entail new possibilities for the collection and processing of data. Besides this, a growing fear of terror attacks stimulates the debate about the future of data protection policy. The question discussed in this context is to what extent data protection rights can be restricted to prevent such serious and organized crime as terrorism. This short outline indicates that data protection policy is a topic of steady relevance.

In the last two decades the European Union has realized the importance of harmonized European regulations on consumer protection policies – including data protection - for the establishment of the internal market and passed various acts of law. Yet, a view on the decision-making processes reveals that different and to some extent opposing opinions exist on how to regulate the field of data protection policy. This has lead to controversial and protracted debates in the past. Taking into account the contexts in which former decision procedures took place, this paper examines the European Union's ability to cope with the aforementioned new challenges of the policy field. Thus, the following research question shall be analyzed:

What are the possibilities and limits of European decision-making in the field of data protection policy?

The paper focuses on the political limits and possibilities. It elaborates contemporary challenges of data protection policy and analyses what conclusions can be drawn from former legislative procedures about the European Union's potential to meet these challenges. Therefore, it refers to the actors involved in the decision-making process and scrutinizes their ability to cooperate and adopt legislation which on the one hand ensures the protection of personal data and on the other hand enhances the internal market by allowing a free flow of data. In doing so, it first analyzes the procedural capacity: Were the actors able to find a

common position and react rapidly to the contemporary challenges or was the decision-making procedure difficult and drawn-out because the positions were too contrary? Information about the different positions and steps of discussion can be gained by a review of protocols and documents of the different EU institutions about the decision-making procedures. Yet, the paper goes further and takes into account the consequences of contestation and cooperation for the substance of adopted legislation. This is necessary because the pure procedural analysis does not give information about the degree to which the challenges are efficiently met. Could the actors adopt stringent regulation or do they leave wide scope for the Member States to employ differing national rules that still hinder the free movement of data? Therefore, the provisions of existing regulations will be reviewed. The scope of this paper allows only a review of the most important European regulations in the policy field of data protection that entailed substantial changes of the status quo. Consequently, a broader analysis would be necessary to ultimately answer the research question. Yet, the subsequent discussion leads to the formulation of well-founded hypotheses about the challenges of European data protection policy. These could serve as the basis for further research that evaluates more closely the possibilities and limits of data protection policy and propose practical recommendations to deal with these limits. This is, however, not possible in the current state of analysis. Therefore, the paper should be seen as the starting point for an empirical research project.

Focusing on the developments in this field on the European level, this work can be assigned into the wider context of European policy analysis. This field of research has undergone an extensive growth over the last years. Simon Hix (2005; 2010) as well as Wallace, Pollack and Young (2010) have written main works in this context to which this paper will refer to.

The paper is structured in three parts. In the first part, data protection policy will be embedded in a theoretical context. Different aspects of the policy field and its integration process will be presented. As in most fields the EU makes use of regulatory policies regarding data protection. At this point, reference is especially made to Giandomenico Majone, whose work 'Regulating Europe' (1996) is one of the most insightful and most cited analyses of regulatory policy. Further, the actors involved in decision-making and theoretical approaches of possible limits of European decision-making will be presented. Subsequently, the second part presents the achievements of the main legislative acts on data protection and some points of critique. This overview serves as the basis for the analytical part. First, two challenges of data protection policy, namely (1) *new possibilities for data abuse due to new technological developments* and (2) *threats of terrorism causing a necessity to intervene in people's privacy to prevent such crime* will be further examined. Afterwards, evidence will be provided for each of the challenges with regard to the question of the possibilities and limits of European data protection policy. Finally, hypotheses will be developed taking those findings into account. In the conclusion possibilities and limits will be contrasted and the finding will be applied to the theoretical considerations regarding the limits of European decision-making processes.

2 Embedding data protection policy in European policy making

Until 1995 data protection was regulated on the national level. Since then, a harmonization of this policy field on the European level has taken place with *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data* being the first European legislative act in this field. A definition of 'personal data' is given in Article 2 of the Directive, stating that the term implies 'any information relating to an identified or identifiable natural person ("data subject")'. Hereby, 'identifiable' means that a person can be identified according to certain information about this person, such as an identification number. The term 'data protection policy' includes all measures taken to regulate the scope within which those personal data can be legally used. In the following section the theoretical framework of data protection policies will be presented.

2.1 Characteristics of data protection rights

In many daily situations people divulge personal data - the registration at a communal office, the closure of a contract with a mobile phone provider or the purchase of a plane ticket are just exemplary situations in which people give away private information. European legislation on data protection policy forces Member States to secure that those personal data do not get abused but are treated confidentially. Data owners shall still possess control over the extent to which their data are used. As citizens of an EU Member State, the data owners obtain a number of rights from this state. Those rights can be divided into positive and negative rights. Positive rights signify that people have a claim to certain benefits, such as education or asylum. On the contrary, negative rights ensure that they enjoy a right of non state interference in private affairs. The right to protection of personal data falls under the positive rights since states are responsible for taking measures ensuring that their citizen's data are protected.

The examples above indicate that data are collected and processed in different contexts. On the one hand data can be accessed by national or European authorities. This is, for example, the case in criminal cooperation. On the other hand, people need to be protected in their role as consumers. Providers of services or goods typically ask for personal information of their clients and process this data. Personal data are very valuable for advertising purposes. They do not only make it possible to detect new consumers and create personalized offers, but can also be used for calculation of businesses to gain more information about their clients. Hence, further use of data for purposes different from the original one and trade of collected data are profitable. Considering this, data protection policies can be embedded in the broader field of consumer protection policy because the consumer needs to be protected from a misuse of personal data. Although these two sides of data protection are not distinguished in the European legislative acts that will be discussed, this work will focus on data protection as consumer protection. In this context, the topic falls within the scope of civil rights.

2.2. Integration of the policy field

Over many years policies on the use of personal data were made on the national level. However, the creation of the internal market within the European Union changed this conception. Different rules in every Member State had shown to be a constraint for trade. Economic troubles in the late 1970s and 1980s and an increasing interdependence of the Member States strengthened their effort to find common responses. The Single European Act included the aim to complete the single market by the end of 1992.

Regarding integration processes it is again possible to distinguish between the two sides 'negative' and 'positive'. Negative integration means the abolition of differing national rules whose existence is not compatible with the treaties. This abolition of dissimilar national rules finally results in market liberalization improving the free movement of goods, services, workers and capital - a goal that was already stated in the Treaty of Rome in 1957. On the contrary, positive integration implies that the Union adopts new common rules to replace national ones. Those new rules deal mainly with social matters, such as consumer safety. The Member States agree on a certain set of standards that need to be maintained. (c.f. Wallace et al. 2010, pp. 118-119).

The Commission issued a first legislative proposal for common action in data protection policy in 1990, which was passed five years later. The harmonization allowed a 'free flow of data' within the internal market, fostering the aims of the internal market. Neo-functionalists like Haas would explain this harmonization with the fact that once a framework for the internal market was achieved, spill-over effects took place including social questions, such as how to protect privacy within this common area (c.f. Chalmer, Davies, Monti, 2010, p. 676). On the contrary, intergovernmentalists like Moravcsik focus on the role of Member States arguing that integration is pushed forward by national interests and ideas while supranational actors only play a minor role. A review on the historic developments of harmonization shows that both of these major theories cannot explain many characteristics of the integration process. Hence, Stone Sweet and Sandholtz (1997) came up with a theory combining these two approaches. According to them it is costly for Member States to maintain different national rules in an economy where transnational exchange increases steadily. Governments are therefore anxious to 'adjust their policy positions in ways that favor the expansion of supranational governance' (p. 299). The result of this adjustment is that governments' power to control the outcomes is weakened while the power of supranational actors rises. Once this process has started, the integration in one sector deepens and can have spillover effects to other sectors. Thus, the theory takes as a starting point the intergovernmentalist idea of powerful Member States initiating the integration process. Yet, it further argues in a neo-functionalist way that supranational action with spillover effects to other sectors is the most appropriate answer to overcome diverging trade restrictive national legislation. Indeed, as pointed out above, divergent national rules concerning data protection in a common market hindered intra-community trade, so that decision-making bodies favored harmonization of this field on the European level.

This fact is observed by Pollack (2005) who thinks that 'the creation of the single market has put pressure on member states to adopt common or harmonized EU-wide regulations' (p.30).

2.3 Decision-making on the European level

The basic legislation on data protection policy, the aforementioned Data Protection Directive (95/46/EC), as well as Directive 97/66/EC, which was focused on telecommunication and replaced by the Directive 2002/58/EC on Privacy and Electronic Communications, were passed in the middle 1990s and the beginning 2000s. At this time the structure of the European Union was described with the famous three-pillar structure, established in the Maastricht Treaty in 1993 and abandoned by the Lisbon Treaty in 2009. The first pillar, the 'European Community', was organized supranationally, while the second pillar, 'Common Foreign and Security Policy', and the third one, 'Justice and Home Affairs' were characterized by intergovernmental principles. As mentioned above, the common regulations concerning data protection policy were regarded as significant for the functioning of the internal market. Due to the fact that internal market matters were part of the first pillar, supranational procedures were used in the field of data protection policy. However, data protection policies that do not mainly contain an internal market matter belonged instead to the third pillar.[1] This distinction was important because the power of the actors involved in the decision-making process differed greatly between intergovernmental and supranational principles. Regarding the Data retention Directive (2006/24/EC) the main point of discussion was whether it belongs to the first or third pillar. With the entry into force of the Lisbon Treaty the pillar structure was replaced by a single framework. The new treaty enhanced supranationalism, so that all measures previously only used in the supranational first pillar now apply - with a period of transition - also to former third-pillar activities (c.f. Chalmer, Davies, Monti, 2010, p.46).

2.4 Policy modes

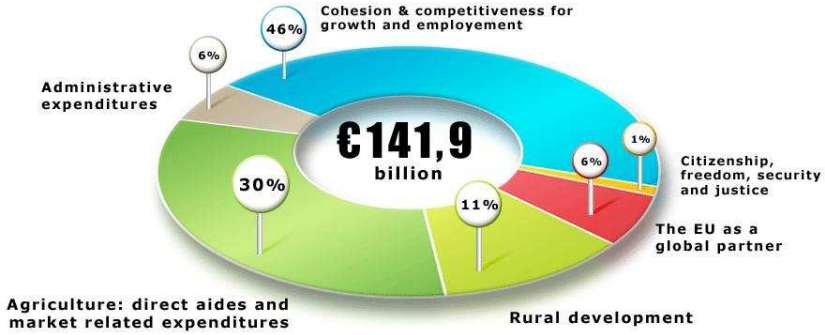
Policy makers possess various kinds of instruments to govern a certain policy field. Against this background, 'instruments' can be defined as the concrete actions which are taken to influence the behavior of actors to achieve a desired political aim (c.f. Jann, 1981, p.60). To get an overview of the policy instruments, efforts have been made to categorize them. The choice of policy instruments depends on the kind of policy. Following Lowi (1979), a widely accepted distinction is made between distributive, redistributive and regulatory policies. Distributive policy means that goods or state benefits are just distributed among citizens, an example of this is public infrastructure. On the contrary, redistributive policies indicate that one group is better off at the expense of a second group because it benefits from the burdens imposed on the latter one. Since consequently redistributive policies entail winners and losers, they are much more controversial than distributive policies. However, they are by far more frequently used nowadays because only a few things remain that can just be distri-

[1] Since this paper focuses only on data of consumers within the internal market, those matters fall outside the scope of this paper.

buted. Most resources are already distributed and can therefore only be *re*-distributed among people. The main instruments used are progressive taxation, subsidies or structural funds. The third category, regulation, is defined by Majone (1996) as 'rules issued for the purpose of controlling the manner in which private and public enterprises conduct their operation' (p.9). According to him regulation is necessary to meet market failures such as monopoly power, negative externalities, inadequate provision of public goods and information failures (ibid, p. 28-29). The policy instruments used are mainly prohibitions, requirements and obligations, persuasion, creation of incentives and role models. Having a look at the history of policy making, it becomes obvious that the kind of policy and the use of instruments prevailing depends on actual political trends. In times of reconstruction after World War II, redistribution in favor of weak groups in society was at the top of the list in many European countries. State intervention in economic matters and nationalization of strategic industries allowed the states to influence the reconstruction of the economy, granting subsidies, providing special infrastructure and offering support programs in research and vocational training. Since states were moreover concerned with questions regarding labor conditions and wages, a mixture of the different policy modes existed (c.f. Braun, Giraud, 2009, p.30-31). However, in the early 1980s neoliberal ideas became popular, enhancing liberalization and privatization first in the U.S., but later also in European countries. According to this, the market is responsible for the distribution of resources while the state has the task to rule out market failures. This implied a change in the use of policy instruments. As Majone (1996) has pointed out, regulatory policies are an appropriate measure to overcome market failures. Indeed, regulatory policies did not only grow in number in liberalized economic sectors but also in social and environmental ones.

How do these ideas focused on the nation state apply to the European Union? The creation of the internal market in the European Union aimed to enhance free trade and liberalization. As in each single nation state, market failures arose, which could be met by regulatory measures. Therefore, the development of a common European market strengthened regulatory policy. However, there is second reason the European Union is often described as a 'regulatory state': the budget of the European Union is small, and out of this small amount great parts are already destined for other purposes, as Figure 2.1 makes clear.

Figure 2.1 The EU Budget 2011



source: http://ec.europa.eu/budget/budget_detail/current_year_en.htm

Since not much has changed over the last decades concerning the amount and allocation of the EU's budget, Majone's conclusion that '(b)ecause the Community budget is too small to allow large-scale initiatives in the core areas of welfare-state activities – redistributive social policy and macroeconomic stabilization – the EC executive could increase its influence only by expanding the scope of its regulatory programmes (…)' (1998, p.1) is still valid. This is true because distributive and redistributive policies are constrained by the budget, while regulatory policies are only slightly influenced by this. Thus, to increase their powers, the actors on the European level have no other possibility than making use of regulatory policies. (Majone, 1996, p. 63-65). Consequently, this is also true for policies concerning data protection. Because the free market encourages providers of goods and services to abuse or resell personal data, the risk exists that the privacy of data owners - secured in the Charta of Fundamental Rights - is disregarded if no measures are taken to protect it. Hence, to secure the entitled right of privacy, the European Union makes use of regulatory policies in this field. Regulatory policies can have different characteristics. Héritier (1987) distinguishes between three kinds of regulatory policies: (1) social regulative policies dealing primarily with norms of human interaction, (2) competitive regulative policies dealing with conceptions of the internal market, especially market entrances, and (3) protective regulative policies aiming to protect special groups from negative consequences of economic action. Policies on data protection fall under the scope of the third category because the special group of 'data owners' shall be protected from misuse of their personal information.

The next question to be considered is which concrete policy instruments are employed by the European Union. The policy field of data protection is regulated by law-making. Yet, different sources of law can be distinguished. The first is primary law, which is the supreme source of European law and consists of the founding Treaties, their amendments and protocols as well as the Treaties on the accession of new Member States. They determine the general principles of European law. Next comes secondary law, distinguishing between unilateral acts on one hand and Convention and Agreements on the other. Unilateral acts according to Article 288 (1) TFEU are Regulations, Directives, Recommendations and Opinions. Further, some 'atypical' acts not mentioned in Article 288 (1) TFEU are considered as unilateral acts, including recommendations and communications, as well as green and white papers. Conventions and Agreements comprise agreements between Member States, international agreements and agreements between institutions including those between purely EU institutions. Finally, supplementary law, including international law and general principles of law, is applied by the Court of Justice when neither primary nor secondary law entails provision to decide a case.

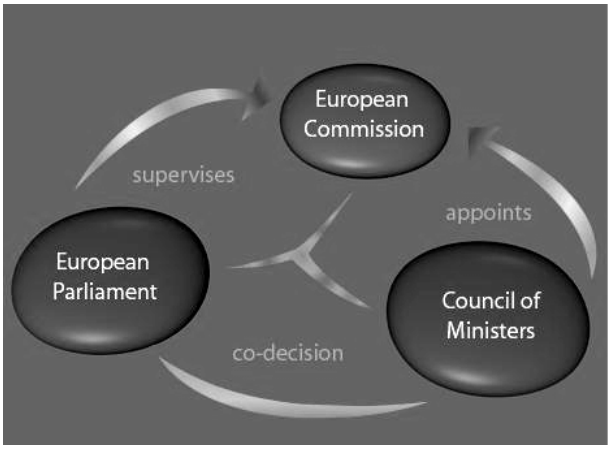
The policy instrument most frequently used in supranational regulation of data protection is the one of Directives. Just like Regulations, Directives are 'hard-law', meaning that they are binding to the Member States. However, while Regulations are binding in their entity and directly applicable, Directives are only binding as to the result to be achieved. In contrast, soft-law, like Recommendations, Opinions, Communications or action programs, has no le-

gally binding force. Yet, it entails positions and perceptions of actors that can have an influence on decisions on the national and European level.
In sum, the field of data protection policy is mainly governed by a regulatory policy mode of law making, mainly in the form of Directives.

2.5 Actors

In the following section, the actors participating in the decision-making procedure shall be presented.[2] An overview of the general positions and organization of the institutions in this policy field will give an impression of the institutional structure in which data protection policy takes place. With this background information, the consequences of cooperation or non-cooperation between the different actors regarding the possibilities and limits of data protection can be evaluated in the analytical part (c.f. chapter 4.2).
This paper focuses only on the supranational legislative actions. In all cases the ordinary legislative procedure (known before the entrance into force of the Lisbon Treaty as the co-decision procedure) was employed. This implies that the European Parliament had important decision-making power in the legislative process besides the European Commission and the Council of Ministers. Since no new legislative act can be adopted without initiation of the Commission and consent of the Council and the Parliament, they are often referred to as the *institutional triangle*. Each part of the triangle will be presented below. Furthermore, some additional actors play a role in the decision-making process that have no decisive power but are consulted for their opinion or make efforts on their own to push through their interests. A detailed description of these actors would go beyond the scope of this work. Thus, their positions are outlined in a tabular overview.

Figure 2.2 The institutional triangle



source: http://www.euandyou.eu/decisions.html

[2] The presentation of the actors involved in the decision-making process is based on information retrieved from PreLex and the websites of the actors itself.

European Commission

The supranationally organized European Commission consists of 27 commissioners, each of whom is responsible for one portfolio and leading at least one of the forty Directorate-Generals (DGs). In case of all four Directives discussed in this paper the DG Information Society and Media (only named DG Information Society until 2005) was designated as 'primarily responsible' during the decision-making processes. It prepared the legislative texts and contacted those DGs that dealt with the topic in a broader sense, asking them to give their opinion. This applied, for example, to the DG Internal Market, DG Competition or DG Health and Consumer Protection. Currently, the Commissioner for the Digital Agenda is responsible, but due to the fact that the allocation of the portfolios varies over time, the Commissioner for the Internal Market and Industrial Affairs and the Commissioner for Internal Market, Financial Services and Financial Integration, Customs, and Taxation were formerly primarily responsible for this DG and, consequently, the topic of data protection.

However, concerning the topic of data retention, a second DG was jointly responsible besides the DG Information Technology, that is the DG Justice, Freedom and Security. This was agreed because the topic fell in equal measure into both portfolios. The citizens' right of data protection was restricted for reasons of security.

The drafts formulated in the DG were discussed and adopted during the weekly meeting of the Commissioners, making use of the oral procedure as decision-making mode. Yet, in the further process, like the adoption of amended proposals, the Commission employed the empowerment procedure (delegation of decision-making power to one or more responsible Commissioners) or the written procedure (automatic adoption if no Commissioner writes reservation) in all cases. Consequently, no Directive was further discussed in the plenary after the initial text had been adopted.

Council of Ministers

The intergovernmental Council of Ministers is composed of ministers from each Member State who meet in different configurations depending on the topic to be discussed. Issues concerning data protection are mainly debateded in the Council of Telecommunication and Transport. However, since the topic has an impact on different subject areas, it has for example also been on the agenda of the Council of General Affairs and the Council of the Internal Market.

The topic of data retention was again treated in a different way than the former Directives: It was only discussed in the Justice and Home Affairs Council because of its emphasis on security matters.

A Committee of Permanent Representatives prepares meetings and divides matters in categories 'A' (not contentious) and 'B' (controversial issues that need to be discussed in the Council). In most cases, early agreement is found and topics are categorized as 'A' matters (c.f. Hix, 2005, p.83). Yet, data protection issues have in most cases been recognized as 'B' items and were discussed more extensively by the ministers themselves to rule out conten-

tious questions. Issues on which no agreement could be found were also sent back to the Committee for further discussion.

The presidency of the Council rotates in half-year terms among the Member States. In this time the presidency has the chance to give special emphasis to issues it considers to be important. As the analytical part of this paper will show, the presidency of Great Britain in 2005 had a strong influence on the decision-making process regarding data retention because the country had a strong intention to reach a fast decision on this topic.

The first two Directives, passed in 1995 and 1997, were adopted under the decision mode of unanimity, while the other two Directives were adopted in 2002 and 2005 under the procedure of qualified majority voting. Although this voting procedure is nowadays the prevailing principle, empirical evident shows that regarding all European decision-making processes most matters are still decided unanimously and entail no contestation (c.f. Hix, 2005, p. 87; Scharpf, 2003, p.263). Yet, in 2002 Luxembourg voted against Directive 2002/58/EC, just like Ireland and Slovakia did regarding Directive 2006/24/EC.

European Parliament

The European Parliament is the second legislative body besides the Council of Ministers. Its members are organized in party groupings. Seven of those party groupings currently exist (April 2011) with the European People's party (EPP, 265 seats) and the Progressive Alliance of Socialists and Democrats[3] (S&D, 184 seats) being the largest and most influential ones.

Much preparatory work is done in committees to coordinate positions and accelerate final voting in the Parliament's plenum. In case of data protection policies the committee of Legal affairs and the committee of Civil Liberties, Justice and Home affairs have been responsible for adopting an opinion on the Commission's proposal and referring it to the plenum. As in the case of DGs involved in the decision-making process, committees in whose broader subject area the topic of data protection falls give an opinion that shall be taken into account by the primarily responsible committee. Those affected committees are, amongst others, the Internal Market and Consumer Protection Committee, the Budgets Committee and the Industry, Research and Energy Committee.

Regarding all four Directives discussed in this paper the responsible committees have made many amendments to the Commission's proposals. In those cases where no agreement was found in the first reading, compromises were again debated in the responsible committee. No permanent coalitions exist between the different party groups. Yet, the decision-making processes are mainly influenced by the two large party groups, EPP and S&D. This general pattern can also be observed concerning data protection policies. In all cases the two groups could agree on a common position while the Greens–European Free Alliance and the Alliance of Liberals and Democrats for Europe argued in favor of stronger rules and a higher level of data protection, especially concerning data retention issues.

[3] The name of the group has changed various times. From 1993 to 2009 it was called the Group of the Party of European Socialists (PES).

Since the Parliament is a supranational actor, its members shall represent the interests of all European citizens instead of single country positions. Yet, a look at protocols of committee meetings shows that members try to enforce national interests when proposing amendments. By way of example a Swedish member of Parliament aimed to preserve the nation's principle of public scrutiny and argued that 'the Directive should not make it more difficult to gain access to registers which are now public' (European Parliament, 1995), thus trying to maintain easy public access to personal data as is usual in Sweden.

Further actors involved in the decision-making process

	Working Party on the Protection of Individuals with regard to the processing of Personal Data	***Social and Economic Committee***	***Interest groups***
Short characterization of the actors	- established in Article 29 of Directive 95/46 - composition: representatives of supervisory authorities from Member States, representatives of the Commission and the European Data Protection Supervisor. - tasks: control the implementation to secure uniform application, observe the level of data protection within the EU, give advice to the Commission on any measure related to data protection. - acts independently from the European institutions	- consultative body composed of members of economic and social interest groups - gives opinion on topics concerning the internal market and social regulation → includes data protection issues: free movement of data and protection of a fundamental right - opinions are forwarded to Commission, Council and Parliament	- represent special interests and try to influence the decision-making process - registered interest groups engaged in consumer protection: BEUC - The European Consumers' Organisation; EDP -European Digital Rights - Registered interest groups of telecommunication sector: ETNO - European Telecommunications Network Operators′ Association ECTA - European Competitive Telecommunication Association
Role in decision making-process	- issued opinions concerning Directive 2002/58/EC and Directive 2006/24/EC - argues for a high level of protection of personal data - opinions are not binding	- mandatory consultation of the Committee in cases of all four Directives after Commission's proposal - strive for more harmonization and transparency	- issued opinions, open letters, press releases and position papers on proposed legislation concerning data protection - interest group engaged in consumer protection argue for higher standards and transparency - interest groups of telecommunication sector aim to achieve same standards in all countries, low administrative burdens and more self-regulation

2.6 Limits of European decision-making

Although, as showed above, actors aim to find a consent on controversial issues, the question arises if supranational decision-making can come to a point where no further agreement can be achieved.

Scharpf (2003) argues that decision-making is 'limited in policy areas where conflicts of interest have high political salience in the constituencies of member governments (…)' (p. 253) He points out that substantial changes regarding salient and contested topics are unlikely because the European institutional structure provides many possibilities to veto a legislative act. In the co-decision procedure the Member States in the Council and the supranational Parliament can prevent the adoption of new legislation by voting against it. Consequently, policy outcomes are often close to the status quo instead of striking for decisions implying substantial modification. Moreover, he explains that the process to find a consensus for sensitive topics is slowly. (c.f. Scharpf, 2003, p.252).

Data protection can be considered such a sensitive topic because data often involve intimate information and people want their political environment to ensure a high level of protection. However, contesting opinions exist about the level of protection, public inspection of data and the degree of interference for reasons of public security.

Whether data protection policies are indeed lowest common denominator policies and are the result of a drawn-out decision-making process allowing significant specific national provisions shall be analyzed in the fourth part. Yet, before being able to draw conclusions about the possibilities and limits of data protection policies the historical lines of development have to be taken into account. This is essential because the analysis on the future challenges of data protection policy refers to the context in which existing legislative acts have been passed.

3 Historical lines of development

The following section presents the most crucial regulatory measures of the European Union in the field of data protection policy. All those measures exist in the form of Directives passed under the ordinary legislation procedure. This paper focuses on data protection as consumer protection policy, meaning that only those cases are discussed in which people have given their data as a consumer of a provider of goods or services. Therefore, all regulations falling in the former third pillar as well as *Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data* are not considered because they are not concerned with the protection of consumer data. The overview of the Directives shall give an impression of the lines of developments in data protection policy.

3.1 Main legislative acts of data protection policy

Directive 95/46/EC

Although the European Parliament had already sent a request to the Commission to initiate common legislation on data protection in 1976, it was only in 1990 that the Commission came up with a proposal on this topic. Up to then, each Member State had its own regulations. Although some common standards on the protection of privacy had been set for example in the Declaration of Human Rights in 1948, the European Convention on Human Rights in 1950 and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the legislation in each Member States differed significantly. This is due to the fact that the mentioned agreements focused on the aim to be pursued but not on the process of how to achieve it. The varying standards and restrictions to transfer of data across borders was considered to be a hindrance for the internal market. To establish a well functioning internal market, the free movement of data within the Member States was necessary. In order to achieve this aim and harmonize data protection policy Directive 95/46/EC was passed establishing a basic framework of European data protection. The Directive includes general definitions of vocabulary used in the context of data protection policy such as 'personal data', 'processing of personal data' or 'controller'. Further, it entails obligations for the Member States to ensure that personal data are handled trustfully and the consumer gets sufficient information on the subject holding the data and the purposes of its use. Transparency of processing is one of the main principles. Particular attention in this context is given to sensitive data which can only be processed under specific circumstances and with explicit consent of the data owner. Moreover, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data was established whose mission was explained before (c.f. 2.5 actors). The Commission had issued the proposal for the Directive in 1990. However, the decision-making process was protracted and thus, the Directive was passed five years later in the second reading. The average time for a proposal made in 1991[4] under the co-decision procedure was 882 days (c.f. Maurer, 2003, p.241). In case of Directive 95/46/EC the decision-making process took 1857 days and lasted consequently much longer than the average process.

Directive 97/66/EC

The Directive is a complement to Directive 95/46/EC and regulates data protection in the telecommunication sector, a topic which was not mentioned in the former one. New technological developments, especially the widespread use of ISDN and digital mobile networks, required this new piece of legislation because they entailed new possibilities for the processing of consumer data. Again, the aim of the Directive was to overcome different national regulations hampering free movement within the internal market. The Directive

[4] No data could be found for proposals made in 1990. Yet, since the proposal for Directive 95/46/EC was made in September 1990 and no changes in the legislative procedure took take place between this date and 1991, it can be assumed that the average duration for a proposal made at this time was approximately the same.

introduces some new definitions and imposes on the Member States the responsibility to ensure that communication data are only listened, tapped or stored with consent of the data subject. Moreover, traffic data shall not be stored longer than necessary for the service and subscribers shall have the chance to receive non-itemized bills. It does not require any specific technical features since this would be against the principles of the internal market idea. Although the Directive is only a complement to Directive 95/46/EC and most questions concerning data protection had already been solved in the discussion of the former, the legislative process was again complicated. An agreement could only be found after the establishment of a conciliation committee. Thus, the decision-making procedure was again protracted and lasted with more than seven years even longer than the one regarding Directive 95/46/EC.

Directive 2002/58/EC

Although the decision-making process for passing Directive 97/66/EC was drawn-out, it was replaced only five years later by Directive 2002/58/EC. This new piece of legislation had become indispensable because 'the development of the information society is characterised by the introduction of new electronic communications services' (Recital 5). Spyware, computer viruses and hidden identifiers are some examples that made it easily possible to gain access to private information of consumers. Moreover, digital mobile networks enabled data processors to get more detailed information about location data than necessary for the fulfillment for their service. Those new developments entailed new risks for data protection that ought to be regulated on the European level.

The Directive intends to determine that features of these new technologies are not misused for purposes other than the provision of the desired service. Therefore, traffic data may not be stored longer than necessary for the transmission of a communication (c.f. Article 5) and location data can only be processed anonymously (c.f. Article 9). However, many provisions are equal or similar to those in the replaced Directive 97/66/EC, like the articles concerning the right to receive non-itemized bills or the requirement not to use specific technical features. The legislative procedure was again characterized by many amending and opposing provisions of the European Parliament and the Council.

Directive 2006/24/EC

This Directive is an amendment to Directive 2002/58/EC and is concerned with the retention of data. The previous Directives stated that data may only be stored as long as they are needed to provide the service. However, they granted Member States the right to restrict this principle when

> *'such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system (…)'* (c.f. Article 15, Directive 2002/58/EC).

Directive 2006/24/EC underlines the threats of terrorism, especially after the attacks in London in 2005, and the possibilities to prevent such crime through a more extensive analysis of personal data. Due to the fact that no common legal basis existed for this, each Member State had made its own regulations which were again considered to hinder the internal market. Thus, common European solutions were desired. It is stated that only traffic and location data are relevant while the provisions do not apply to the content of communications (c.f. Article 1 (2)). The Member States are responsible for ensuring that only the competent national authorities get access to those information. The data must be stored for a minimum of six months and a maximum of 2 years, with each Member State allowed to decide on the exact time in between those two extremes. In contrast to the previous Directives, the decision-making process proceeded rapidly. Although the average time from the proposal to the adoption of a legislation under the co-decision procedure amounted to 15.7 months between 2004 and 2006 (c.f. European Commission 2007, p.2) the Directive was passed in the first reading after only 7 months.

Table 3.1 Overview of the historical lines of development in the field of European data protection policy

	object of regulation	***Time between first proposal and adoption***	***Stage in which agreement was found***	***specifics***
Directive 95/46/EC	Basic principles for data protection	5 years and 1 month	2nd reading	First legislative act in the field of data protection
Directive 97/66/EC	Regulations for the telecommunication sector	7 years and 3 months	3rd reading	
Directive 2002/58/EC	Regulation of new developments in the telecommunication sector, especially through widespread use of the internet	2 years	2nd reading	Part of a package of five Directives concerning the telecommunication sector → last of the five Directives to be passed
Directive 2006/24/EC	Data retention	6 months	1st reading	Initial proposal to regulate the topic under the third pillar but opposed by Parliament and Commission

3.2 Evaluation of existing law

An Eurobarometer survey gives an impression of the feelings of individuals and organizations toward the degree of data protection. 68% of the individual consumers within the European Union indicate that they are concerned about the way their data are treated. Notably, in 1996, when the first Directive on data protection policy had only been passed a few month ago, the number of people concerned was 58%. Since then, a steady increase of wor-

ries can be observed, signifying that harmonization of data protection policy could not create a feeling of protection among consumers. (c.f. Eurobarometer, 2008 a, pp. 7-8). On the contrary, organizations evaluate the level of protection to be on a medium level whereas no changes in this attitude can be observed to the opinions stated in a previous analysis in 2003. However, organizations raised complaints about the fact that although common European legislation exists different implementation in the Member States hindered intra-community trade. This malfunction has also been recognized by the Commission. Since many formulations in the Directives are very broad, Member States enjoy a large freedom of action in the implementation process. One example mentioned is that 'the way in these rights [the rights to be able to access, rectify, delete or block data] can be exercised is not harmonised, and therefore exercising them is actually easier in some Member States than in others (c.f. European Commission, 2010b, p.7). Differing national legislation can also be observed, inter alia, concerning the period of data retention, remedies and sanctions for non-compliance with legislation and requirements for adequacy assessment of third countries' level of data protection.

3.3 Consideration of new legislative acts

In 2009, the Commission started to initiate new legislation for data protection in 2011. Although it still judges Directive 95/46/EC to be 'good legislation' (Reding, 2010), it came to the conclusion that a revision of the existing legal framework is needed to face the aforementioned problem of inconsistent national legislation and meet the challenges of new trends and developments of modern technology. To review actual shortcomings and arising challenges, the Commission published a Communication with the title *'A comprehensive approach on personal data protection in the European Union'*. To receive input from the public, the Commission further launched a public consultation and invited citizens, organizations and public authorities to comment on the current and desired future European data protection policy. It has been announced that a proposal for legislation will be made by the Commission by the end of 2011.

4 Analysis – possibilities and limits of European data protection policy

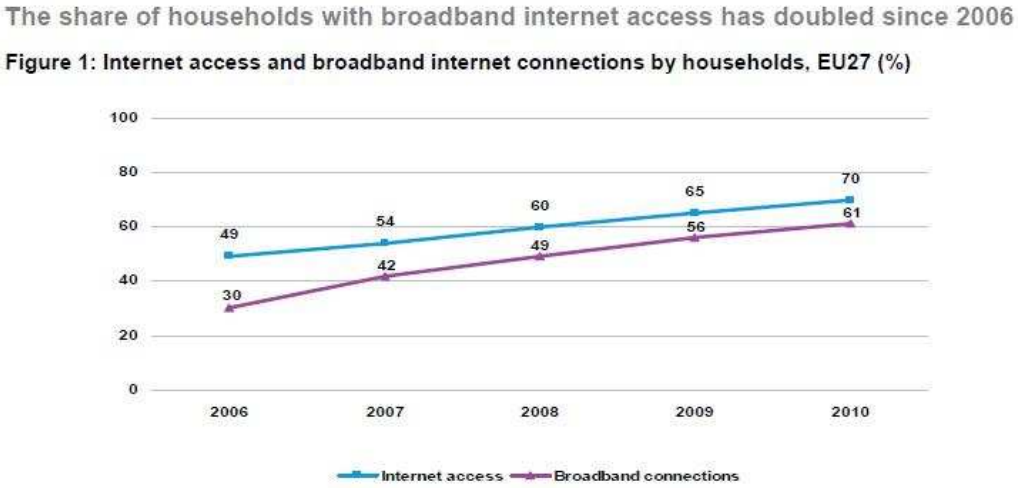
The circumstances in which data protection policy takes place are continually changing due to technological developments and current political affairs. Consequently, new legislative actions are regularly required to deal with the arising challenges. This part of the paper focuses on the European Union's ability to deal with these challenges.

4.1 The challenges of European data protection policy

Two current challenges of data protection policy will be addressed: (1) new possibilities for data abuse due to technological developments and (2) threats of terrorism causing a necessity to intervene in people's privacy to prevent such crime.

New possibilities for data abuse due to technological developments

Although the basic piece of legislation in data protection policy, Directive 95/46/EC, is formulated technologically neutral and presents basic long-lasting principles for security of data, it is acknowledged that new technical inventions involve possibilities for the processing of data that were not known when the Directive was passed in 1995. Thus, the Commission acknowledged in its newest Communication on this topic in 2010 that there is a 'need to clarify and specify the application of data protection principles to new technologies, in order to ensure that individuals' personal data are actually effectively protected (…)' (p. 3). Most changes in current years can be observed in the usage of the internet. The table below shows that only within the last four years the number of users has grown considerably from 49% to 70%, with the number of broadband internet connections by household increasing from 30% to 61%.



Source: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF

But not only the number of people using the internet has increased, their activities in the online world have also altered. Recent years have shown a rising popularity of social network sites such as Facebook, Myspace or LinkedIn where users publish personal information, communicate with other users and upload photographs and videos. According to a survey, nearly every second internet user nowadays posts massages to chat sites, blogs and social networking sites (c.f. Seybert & Lööf, 2010, p.3). It has been argued that 'risks typically associated with the potential misuse of personal data exchanged on SNS (Social Network Services) range from exposure to direct marketing, re-identification, profiling, identity theft, online and physical stalking, blackmailing and embarrassment' (Gross and Acquisti, 2005, p.73). Moreover, some raise the fear that security aspects are neglected for the benefit of functionality and that Web 2.0 applications can easily be exploited by hackers (c.f. Lawton, 2010, p.15).

Besides an increased use of Social Network services, a growing number of people buys and orders goods or services online. Today, nearly 60% of EU citizens are active in these online activities (c.f. Seybert & Lööf, 2010, p.4). Online shopping necessarily entails that personal

data need to be indicated, such as the buyer's address or bank data. Furthermore, it can be observed which kind of goods and services people are interested in, enabling providers to create personal profiles of consumers. As a result, people feel a loss of control over their own data (c.f. European Commission, 2010a, p.2). In particular, concerns are caused by the fact that children and teenagers are often active on online platforms without being aware of the risks of data misuse.

In addition, it is problematic for the effectiveness of European policy making that the internet is a global network where European citizens are not only in contact with providers of goods or services within the internal market but worldwide. Therefore, most consumer data are processed outside the European Union. Since globalization has increased the outsourcing of processing acts it has become even more difficult to detect the accountable data processors and make adequate regulations that ensure people's privacy and confidence in European regulatory actions. However, the Union has stated that the citizen's right of protection of personal data shall not be affected by the fact that data processing takes place outside its territory (c.f. European Commission, 2010b, p. 11). Besides changes in the online environment, automated data collection of mobile device users through techniques such as electronic ticketing or road toll collection simplified the exact location of individuals (ibid, p.2). Thus, it is easily possible to collect and process more information than necessary for the provision of the service. The additional data can be misused for other purposes.

Threats of terrorism causing a necessity to intervene in people's privacy to prevent such crime

In the last decade Member States of the European Union have repeatedly become the target of terroristic attacks. Although the RAF, ETA and other terroristic groups carried out attacks within Europe some decades ago, recent threats of terrorism are regarded as more incalculable and inconceivable because they do not have a regional focus anymore but can happen at any time at any place. Most of them are connected with Islamic fundamentalism (c.f. Bonnici, 2007, p. 163). In 2004 and 2005, attacks in Madrid and London reached a death toll of nearly 250 people while more than 2000 people were injured. Those were the two biggest attacks during the last decade within the territory of the European Union, but terrorism has been present beyond that. In 2006 terrorists had planned a train bombing in Germany that failed because the bombs, situated in suitcases, did not go off. Recently, parcel bombs were found in various embassies in Italy and Greece. Those are only some events which have raised fear among Europe's population.

The European Union took common actions against these threats. The Tampere Programme adopted in 1999 and the Hague Programme adopted in 2004 underlined that the fight against terrorism is on the European agenda focusing on the exchange of information between law enforcement services, cooperation with third countries and prevention of terrorism financing. For the period 2010 – 2014 the Stockholm Programme was passed which states that 'we [the European Union] must not lower our guard against these heinous criminals'. Yet, it is claimed

that in this fight fundamental rights - one of which is the right to protection of personal data according to Article 8 of the Charta of Fundamental Rights - should always be respected. The fulfillment of this principle presents a difficult challenge for the European Union because most considerations to prevent terrorism include an extensive interference in people's private data. Those considerations are in particular about the use of biometric identification techniques such as face, voice or iris recognition software or digital fingerprints as entrance identification. Collected information can then be stored in databases containing and connecting personal information of the citizens. An area of particular sensibility since the terror attacks of 9/11 is air travel, and passenger data are inspected thoroughly. It is important to note that this stored information often contains sensitive data about the racial background or the state of health of the individual. These measures are a restriction to the right of protection of privacy. The question asked by data protectionists is to what extent such techniques are useful and necessary to prevent terrorism.

In a nutshell, European decision-making in the field of data protection is challenged to take place within an area of tension: On the one hand it promises to offer its citizens an area of physical security, but on the other hand it has to secure their fundamental rights, including the right to protection of personal data.

4.2 Assessment of the European Union's ability to meet the challenges

The following part aims to answer the question whether the European Union is able to set regulations that meet the challenges presented above. Therefore, the context in which former legislative acts have been passed and the positions of the actors will be analyzed in order to draw conclusions from this process for the challenges presented above.[5] Furthermore, it will be discussed whether decision-making in form of Directives is still an appropriate instrument in this policy field. The two challenges of (1) data misuse due to new technological developments and (2) threats of terrorism will be regarded separately due to the fact that they might provide different findings for the possibilities and limits of data protection policy.

New possibilities for data abuse due to technological developments

As the descriptive part has shown Directive 95/46 EC laid down the basic principles of data protection, while Directive 97/66 EC and Directive 2002/58 EC were passed to find answers to the challenges of new technological developments such as ISDN and a widespread use of internet services. It is notable that in all three cases decision-making was difficult and took at least two readings. A long decision-making process concerning the first legislative act in a harmonization process of a policy field might be explained by the fact that a whole new framework has to be created. Formerly, each Member State had its own regulations which now have to be aligned with the positions of all Member States in the Council as well as with those of the Commission and the European Parliament. In such a process each actor has a

[5] The information about the procedure and position of the actors are originate from PreLex and the European Parliament Legislative Observatory

basic position and idea of common regulation on the European level. It can be assumed that they have a special interest to enforce their positions in the first legislative act because following the concept of path dependency this basic piece of legislation indicates the direction for future policies and therefore influences the starting point for further decision-making processes. Therefore, an explanation suggests itself for the fact that it took five years from the initial proposal of the Commission to the final adoption of Directive 95/46 EC. Both the European Parliament and the Council had amendments to the submitted proposals. However, their amendments were rather supplementing than opposing. The Council agreed to the European Parliament's concept to apply the rules laid down for the private sector to the public sector as well and to imply less strict rules on media fulfilling their duty of public information. The amendment to extend the scope of the Directive to the processing of data by non-profit organizations was made more concrete by the provision to allow special derogation for nonprofit organizations dealing with sensitive data. The Council's own ambition was to introduce the rule that the purpose of data collection should be disclosed before the collection process and to specify the individuals' rights, for example extending the right to be kept informed to the origin of data or extending the rights to appeal. Four countries within the Council found the provisions to be too detailed. This indicates that the degree to which Member States aimed to have common legislation differed within the Council. The Commission could agree on all the amendments made by the European Parliament and Council so that finally both actors were able to pass the legislative act. According to Bähr et al. (2008) it is common that new legislation is more momentous than amending legislation which only deepens the scope of an existing set of rules. Thus, it can be expected to observe a less problematic decision-making process regarding amending acts. However, this is not the case in the field of data protection policy. Although Directive 97/66/EC and Directive 2002/58/EC only extended the scope of Directive 95/46/EC to the field of telecommunication and the basic principles laid down in this Directive were not called into question, the decision-making process was intricate. Directive 97/66/EC could only be passed after a Conciliation Committee had negotiated an agreement. In contrast to the first Directive, where the Commission was able to accept all the amendments made by the legislative bodies, this time it was only able to agree on seven out of eleven amendments of the Parliament in the second reading. What made it more complicated was the fact that there were long time spans between the discussion of the proposals of the different actors. The proposal handed to the European Parliament for a second reading in 1996 differed a lot from the first one it had received in 1990 because many technological changes had happened. Therefore, many new points had to be discussed to which amendments were made. As in the decision-making process of the first Directive, Parliament and Council did not have contradicting opinions but introduced many new completing points to the proposals. However, the pattern of not contradicting but supplementing opinions cannot be found in the decision-making process of Directive 2002/58/EC. One example is the discussion about the handling of unsolicited e-mails for purposes of marketing: While the Commission and the Council preferred an opt-in approach,

meaning that marketing e-mails can only be received after the addressee's consent, the European Parliament wanted to leave decision power to the Member States. They should de-decide independently whether they want to follow the opt-in approach or an opt-out approach which implies that subscribers only have the right to be removed from a mailing list after receiving marketing emails. Controversy about this topic could also be observed within the Parliament since, in the first reading, it voted with 204 to 129 with 155 abstentions against the draft made by the Committee on Citizen's Freedoms and Rights, Justice and Home Affairs and referred it back for further discussion. Although the European Parliament and the Council had contrasting opinions on some points and were not able to pass the Directive in the first reading, they were willing to find a compromise without implementation of a Conciliation Committee. Thus, the two big parties in the European Parliament, the EPP and the PES, worked out a compromise close to the Council's conceptions. Moreover, the Commission did not oppose any of the amendments made by the European Parliament or the Council. An explanation for this harmonious behavior is that the Directive was part of a package of five Directives concerning the telecommunication sector, and it was the last of the five Directives to be passed. Since a whole set of legislation depended on a decision in this case, the actors were willing to find a common solution.

What conclusions can be drawn from this processes for the challenge of new technological developments that entail new possibilities for data abuse? The starting point is similar to those of Directive 97/66/EC and Directive 2002/58/EC: The fundamental principles for data protection policy are already established and shall not be changed. Yet, some provisions need to be updated to meet the technological progress (c.f. Reding, 2010). The analysis has shown that although uncomplicated decision-making process could be expected where amendments are made to existing legislation, this supposition had to be refuted. Since the legislative framework in which decisions in the field of data protection policy take place has not changed over time, there are no indications that in an upcoming legislative process the actors will struggle to find an early agreement.

As presented above, the efforts to find an acceptable agreement for all actors resulted in broad formulations of the Directives which were interpreted differently by the Member States.

Thus, regarding the current challenges it can be argued that it is not possible to adopt more concrete Directives in this policy field because the actors already needed a long time - and in one case even established a Conciliation Committee - to pass Directives with only broad formulations.

The question arises whether other regulative instruments could overcome these problems. The attempt to solve the problem of diverse national regulations through directly binding Regulations is not feasible. Regulations need concrete provisions that are directly binding upon every Member State. Yet, the Directives could only be passed because the compromises between the actors left some decision-making power to the Member States for their own specific regulations. Regulations do not leave any scope for differing national provisions. The other two legislative instrument mentioned in Article 288, Recommendations and Opi-

nions, are also no appropriate measures to meet these challenges. Although fast decisions might be expected because all actors generally agree on the protection of fundamental rights, they are no appropriate solution because they have no binding force. This would result in even more contrasting national legislation. Consequently, Directives seem to be the only suitable possibility with respect to the challenges.

Thus, it is likely that the current problems of differing national legislation and long decision-making processes remain. Although the problems have been recognized and the Commission emphasizes its will to overcome this problem, the preconditions make it unlikely that this will happen. A possible point of conflict in future debates might be to (re-)define the concepts of data controller and data subject because in the world of social networks, data subjects are often also data controllers when putting information and pictures of themselves and other subjects online. Besides, it might be problematic to agree on the point at which the absolute private domain not covered by data protection policies ends in social networks. If someone uploads a photograph of a party, this can be seen as private sphere. However, if it is accessible to everyone, it cannot be considered to be solely 'private'. Children and teenagers are often not aware of the consequences of their online activities. Adults are usually aware, but often do not care very much about them (c.f. European Commission, 2010b, p.6; Goldie, 2006, pp. 150-153).

Furthermore, Directives are not the only way to meet the challenges of widespread internet usage. This is due to the fact that the internet is a global sphere and many European citizens are in contact with providers of goods and services outside the internal market. Directives do not have the scope to regulate the collecting and processing of data outside its territory. The European Union's capacity of action by Directives in this field is therefore limited. To ensure that data are processed 'fairly and lawfully', as stated in Article 3 of Directive 95/46/EC, contracts with third countries are negotiated. But since European standards are strict, it will be impossible to ensure that all countries in the world offer the same degree of protection. Thus, it seems that regulatory action in form of hard-law comes to a limit in this respect. Yet, other regulatory instruments, such as recommendations or awareness campaigns, have no binding force but can provide information about possibilities of data abuse and measures to protect oneself from this.

Threats of terrorism causing a necessity to intervene in people's privacy to prevent such crime

In 2002 Denmark, which held the Council presidency at that time, had proposed a first legislative act recommending a common period of 12 months for the retention of data. However, this proposal was disapproved. The topic of data retention was on the agenda again after the terror attacks in Madrid, and as a result of the discussion, Directive 2006/24/EC was passed. At first glance it might be questionable why data retention is regulated as an internal market topic because the data retained are given to national authorities in order to prevent criminal offences. Indeed, a group of four countries - France, United Kingdom, Ireland and Sweden -

had proposed to regulate this topic under the third pillar. However, this would have meant that the European Parliament would have had no decision-making power. Thus, it strongly opposed this suggestion. The Commission supported this position. The argument was that data are stored by providers within the internal market who have to obey different sets of law in each Member State which poses a hindrance for the free movement of goods and services.

As shown above, national legislation regarding data protection differed in many respects. Yet, only for the conditions and periods of data retention this was the starting point for further legislation. This already indicates that security matters are an important topic the European actors aim to handle efficiently. In contrast to the previous Directives, a common decision was made within a short period of time. Initially, dissension existed between the actors, most notably concerning the time length of data storage. The desired period for retention varied between six months and three years. Nevertheless, the decisive actors found an agreement after the first reading. This was possible because the two major party groups, EPP and PES, neglected the positions of other party groups and struggled to find a compromise with the Council on the aspiration of the British Council presidency. The parliamentary committee of Civil Liberties, Justice and Home Affairs had found a broad agreement also supported by party groupings aiming for a high degree of data protection, such as ALDE. Yet, the EPP and the PES, previously in favor of this solution, disregarded it, because it would have conflicted with the Council's position. Instead, they negotiated a compromise with the Council and incorporated its opinions in the amendments before the final Parliament's vote in the first reading. Accordingly, the Council was able to agree entirely to the submitted proposal. Smaller party groups, the rapporteur Alexander Alvaro as well as the European Data Protection Supervisor and the Article 29 Working Party strongly opposed this agreement, but the votes in the European Parliament (378 in favor, 178 against, 30 abstentions) and the Council (two votes against) were definite.

How is it possible that, especially for such a sensitive topic, the decision-making process proceeded much faster than in all previous legislative acts regarding data protection? To answer this question the contemporary background needs to be taken into account. While the events in Madrid had already shown that terror attacks as seen in the USA in 2001 could also happen in Europe, the bombings in London only one year later confirmed this anxiety and presented a further argument for those in favor of preventive measures. At the same time, the United Kingdom held the Presidency of the Council, thus having additional power to influence the decision-making process. Because the country was directly affected by the terror attacks, it was strongly in favor of the proposed Directive and put the topic at the top of the agenda repeatedly. Thus, it can be concluded that the visible threats to security and possible fear of new attacks expedited the decision-making process because all actors were anxious to find a common solution. The two big parties in the European Parliament worked together to find a compromise. Critical comments of the Working Party, the European Data Protection Supervisor and smaller parties were disregarded. The quotation of Katalijne Maria

Buitenweg on behalf of the Verts/ALE Group in the parliamentary debate of December, 13, 2005 is representative of the opinion of those who remained unheard:

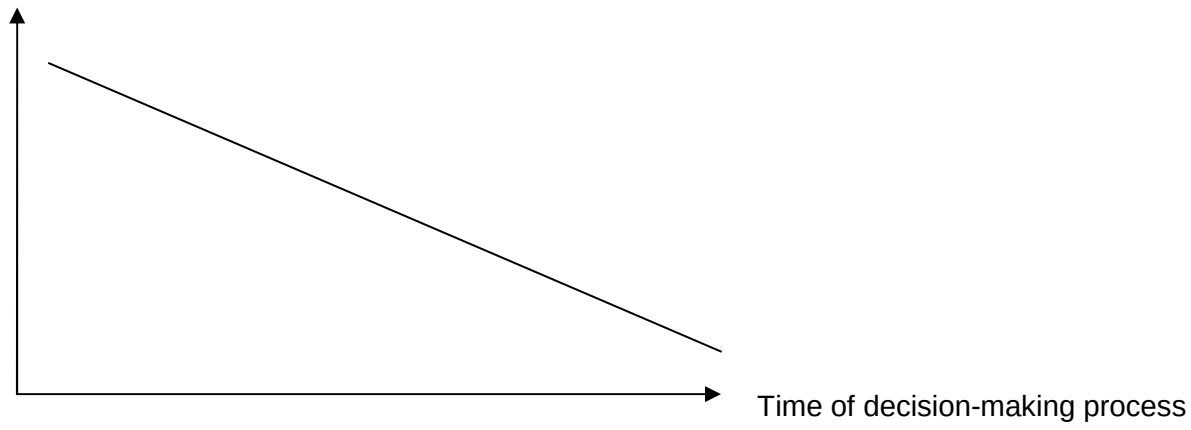
> 'I would now like to turn to the large groups. My group was also in favour of bringing this discussion to a prompt close, namely after first reading in this House, but as you have now done a deal with the British Presidency before Parliament has even adopted a position, we are now faced with a fait accompli.'

Although the initial aim was to harmonize the conditions and periods of data retention, the final legislative act states that Member States can decide to store data between a period of six months to two years (Article 6). Hence, providers of services and goods still have to obey different rules within the Member States. The ambition to find an early agreement existed at the expense of the struggle to make a more concrete provision for the internal market. It appears that the European Union was rather driven by the motivation to regulate a security matter than to face an obstacle of the internal market.

Those findings suggest the conclusion that where security matters are concerned, the decision-making process is dependent on contemporary events. The visible effects of a terror attack provoked intensive cooperation between and within the actors. Following this argumentation, the introduction of biometric identification measures to detect terrorists is most feasible when current developments raise fear of terrorism. Concerns of data protection fade into the background when serious threats to security are present.

In contrast, the problems of data abuse through new technological developments are not that visible and do not raise a feeling of harassment leading to quick decisions. Consequently, Figure 4.1 visualizes the answer to the question why the decision-making process of such a sensitive topic proceeded much faster than in all previous legislative acts regarding data protection. The graph indicates in a simplified manner that the higher the feeling of harassments, the more accelerated is the decision-making process.

Figure 4.1 Influence of a 'feeling of harassment' on the decision-making process



4.3 Hypothesis generation

This paper focuses on the main decisions made in the field of data protection policy and the main lines of development. Thus, the conclusions to be drawn from the analysis are not final. Rather, they can serve as the basis for the generation of well-founded hypotheses which could be verified or falsified in a next step. To do this is beyond the scope of this work, so that the hypotheses can serve as starting points for further research in this policy field.
Since the analysis was divided into two parts - on the one hand the challenges arising from development of new technologies for data abuse and on the other hand threats of terrorist offenses – it is only logical to establish separate hypotheses for each challenge.
Regarding the new technologies it was stated that decision-making processes are difficult because each actor aims to enforce its positions hazarding the consequences of protracted decision-making processes. However, history shows they are willing to find a final agreement since all of them appreciate the advantage of common regulation within the internal market.
With a view to the possibilities and limits the following hypotheses can be made:

If decisions are necessary due to new technological developments, then actors are willing to strike a final agreement but the decision-making process takes a long-time because a low feeling of urgency of an early agreement encourages long and drawn-out debates.

If the actors involved in the decision-making process have dissimilar or even contrasting positions, then the resulting legislative act is broadly formulated and gives so much leeway for differing interpretation that it is still considered a hindrance for a 'free flow of data'.

The conditions concerning the challenge of terrorism are different. Because fear of terrorism is a highly sensitive topic and is discussed emotionally, a feeling of danger to public security strengthens the actors' efforts for goal-orientated cooperation. Following this, the subsequent hypotheses have been developed:

If the fear of terrorist attacks is especially high, due to actual threats or serious warnings, then concessions to restrict the fundamental right of data protection and privacy of personal data are likely.

If the fear of terrorist attacks is especially high, due to actual threats or serious warnings, then the actors strive to strike a rapid agreement willing to compromise with each other.

If the actors strive to find a rapid agreement and compromise with each other on issues where concrete solutions are difficult to reach, then they accept broad formulations and the negative impact of this for the 'free flow of data'.

5 Conclusion

The starting point of this paper was the question which possibilities and limits data protection policy on the European level has. Therefore, the decision-making process has been analyzed with regard to the consequences this can have for future challenges of (1) data abuse possible through development of new technologies and (2) threats of terrorism causing a necessity to intervene in people's privacy to prevent such crime

The conclusions of the in-depth study regarding the **possibilities of data protection policy** are the following:

The European Union is still able to find agreements because all actors share the common will to make decisions on the European level enhancing the 'free flow of data' within the internal market. Although the process concerning regulations on new developments has been protracted, a struggle to find a compromise could finally be observed in all legislative processes. Cooperation is thereby visible not only between, but also within the decision-making bodies. The two big party groupings in the European Parliament, the EPP and the PES, have worked together closely to find common positions. In the Council all legislative acts were approved with a broad majority. The maximum of votes-against was a number of two in the voting of Directive 2006/24/EC. This indicates that the legislative acts had a broad support of the Council. Since the circumstances in which data protection policy takes place have not changed significantly, it is likely to see a similar pattern regarding the current challenges. The development of new technologies was also the starting point for the introduction of Directive 97/66EC and Directive 2002/58/EC. Thus, since an agreement could be found in these cases there is no evidence that the actors could not find a common solution in future legislative acts. The passing of a Directive restricting data protection to prevent threats of terrorism is especially possible when the feeling of harassment is high.

However, **limits of data protection policy** have also been detected:

A long decision-making process, as can be observed concerning the challenge of new technologies, is of particular concern because technologies are quickly outdated and replaced by new inventions entailing unforeseeable challenges for data protection. Thus, a long time span between the widespread usage of new technologies and a common regulation raises the risk of undesired behavior in the processing of data in the meantime. Besides, the Internet facilitates contracting of consumers with providers of goods and services all over the world. The European Union cannot apply the provisions of its Directives to countries outside its territory which offer a lesser degree of data protection. The adoption of legislation regulating the restriction of data protection rights with regard to the prevention of terrorism can come to its limits when the restrictions are felt to be unproportional in comparison to the perceived feeling of danger.

In all Directives the broad formulation of provisions is problematic because the different transposition in national law still imposes the burden to obey varying sets of rules in each Member State. This constitutes a hindrance for the internal market. Since it has already been

difficult to find a agreement on broad formulations, it seems to be unrealistic to expect more concrete formulations in upcoming decisions. For this reason, Regulations, which are directly binding for the Member States, do not seem to be an alternative as policy instrument.

How do these findings apply to the assumption of Scharpf that the decision-making process regarding sensitive topics is slow and produces outcomes on a lowest common denominator? Regarding the procedural capacity to enact legislation it has to be recorded that decision-making procedures were indeed slow when the feeling of harassment was low. Yet, on the highly sensitive topic of data retention the willingness to compromise was high and legislation was adopted only within a few months. In so far, Scharpf's assumption cannot be confirmed.

To examine further whether lowest common denominator results are a consequence of European decision-making, substantive benchmarks were taken into account. In all four cases analyzed in this paper, the actors were not able to formulate stringent regulations. Broad formulations, interpreted differently in each Member State, were the only possible solution to enact legislation. Thus, in this respect, Scharpf's thesis can be confirmed in the field of data protection policy.

To conclude, it can be assumed that the European Union will still be able to enact legislation in this policy field. Yet, no evidence could be found to support expectations of a faster or more stringent process in the future to meet contemporary challenges. To what extent other regulatory policy instruments, such as recommendations or awareness campaigns, might be useful supplementing measures could not be analyzed in this paper. This might be the starting point for further research.

Reference List

Alsenoy, van, B., Ballet, J., Kuczerawy, A. & Dumortier, J. (2009). Social networks and web 2.0: are users also bound by data protection regulations? *Identity in the Information Society, 2 (1),* 65 – 79.

Bähr, H., Treib, O. & Falkner, G. (2008): Von Hierarchie zu Kooperation? Zur Entwicklung von Governance-Formen in zwei regulativen Politikfeldern der EU. In Tömmel, I. (Eds.), Die Europäische Union: Governance und Policy-Making, Politische Vierteljahresschrift, Sonderheft 40/2007. Wiesbaden: VS Verlag für Sozialwissenschaften.

Blum, S. & Schubert, K. (2011). Politikfeldanalyse. 2., aktualisierte Auflage. Wiesbaden: VS Verlag.

Bonnici, J. (2007). Recent European Union developments on data protection ... in the name of Islam or 'Combating Terrorism. *Information & Communications Technology Law, 16 (2).* 161 - 175.

Bulmer S., Dolowitz, D., Humphreys, P. & Padget, S. (2007). Policy Transfer in European Union Governance: Regulating the utilities. Abingdon; New York: Routledge.

Braun, D. & Giraud, O. (2009). Steuerungsinstrumente. In Schubert, K. & Bandelow, N. (Eds.). Lehrbuch der Politikfeldanalyse 2.0. München: Oldenbourg.

Carey, P. (2009). Data Protection. A Practical Guide to UK and EU Law (3rd Edition). New York: Oxford University Press.

Chalmers, D., Davies, G. & Monti, G. (2010). European Union Law: Cases and Materials (2nd Edition). Cambridge; New York: Cambridge University Press.

Council of the EU & European Parliament. (1995). 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 . Retrieved March 22, from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Council of the EU & European Parliament (1997). Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. Retrieved March 22, from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML

Council of the EU & European Parliament (2002). 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. Retrieved March 22, from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

Council of the EU & European Parliament (2006). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Retrieved March 22, from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:EN:HTML

European Commission (2010 a). Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data. Retrieved March 24, 2011, from: http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf

European Commission (2010 b). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union. COM (2010) 609 final. Retrieved March 24, 2010, from: http://ec.europa.eu/justice/news/consulting_public /0006/com_2010_609_en.pdf

European Commission (2008 a). Flash Eurobarometer 225: Data Protection in the European Union. Citizens' perceptions. Analytical report. Retrieved 20 March, 2011, from: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf

European Commission (2008 b). Flash Eurobaroemter 226: Data Protection in the European Union. Data controllers' perception. Analytical report. Retrieved 20 March, 2011, from: http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf

European Commission (2007). Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive. COM(2007) 87 final

European Parliament (1995). Debates of the European Parliament. No 4-464/142.

Falkner G., Hartlapp M., Leiber S. & Treib O. (2004). EG-Richtlinien als soziales Korrektiv im europäischen Mehrebenensystem? Problemskizze und potentielle Wirkungsmuster. In Héritier, A., Stolleis, M., Scharpf, W. (Eds.), European and International Regulation after the Nation State: Different Scopes and Multiple Levels (pp. 115-138). Baden-Baden: Nomos Verlagsgesellschaft.

Goldie, J. (2006). Virtual Communities and the Social Dimension of Privacy. *University of Ottawa Law & Technology Journal, 3(1),* 133-167.

Grimm, R., Löhndorf, N. & Scholz, P. (1999). Datenschutz in Telediensten (DASIT). Am Beispiel von Einkaufen und Bezahlen im Internet. *Datenschutz und Datensicherheit, 23 (5),* 272 – 277.

Gross, R., & A Acquisti (2005). Information Revelation and Privacy in Online Social Networks. In: Proceedings *of the 2005 ACM Workshop on Privacy in the Electronic Society (2005)*, 71-80.

Héritier, A. (2007). Explaining Institutional Change in Europe. New York: Oxford University Press.

Hix S. (2008). What's Wrong with the European Union and How to Fix it. Cambridge: Polity Press.

Hix, S. (2005). The Political System of the European Union (2nd Edition). Basingstoke; New York: Palgrave Macmillan.

Jann, W. (1981). Kategorien der Policy-Forschung. Speyer: Hochschule für Verwaltungswissenschaft Speyer. Speyer Arbeitshefte 45.

Maurer, A. (2003). The Legislative Powers and Impact of the European Parliament. *Journal of Common Market Studies, 41 (2)*, p. 227 – 247.

Lawton, G. (2007). Web 2.0 creates security challenges*. Computer 40(10),* 13–16.

Lowi, T. (1979). Four Systems of Policy, Politics, and Choice. *Public Administration Review, 32 (4),* 298-310.

Majone, G. (1998). The Regulatory State and its Legitimacy Problems. Reihe Politikwissenschaft / Political Science Series No. 56. Vienna: Institute for Advanced Studies.

Majone, G. (1996). Regulation and its modes. In Majone, G. (Eds.), Regulating Europe (pp. 9-27). London; New York: Routledge.

Majone, G. (1996). Theories of regulation. In Majone, G. (Eds.), Regulating Europe (pp. 28 - 46). London; New York: Routledge.

Majone, G. (1996). The rise of statutory regulation in Europe. In Majone, G. (Eds.), Regulating Europe (pp. 47 - 60). London; New York: Routledge.

Polcak, R. (2009). Aims, methods and achievements in European data protection. *International Review of Law, Computers & Technology. 23 (3).* 179 – 188.

Pollack, M. (2005). Theorizing EU Policy-Making. In: Wallace, H,. Pollack, M. & Young, A. (Eds). Policy-Making in the European Union (5th Edition). New York: Oxford University Press

Rosamond, B. (2000). Theories of European Integration. Basingstoke; New York: Palgrave Macmillan.

Scharpf, F. (2003). Legitimate Diversity: The New Challenge of European Integration. In Scharpf, F. (Eds.), Community and Autonomy: Institutions, Policies and Legitimacy in Multilevel Europe (pp. 247 – 276). Frankfurt a. M.: Campus Verlag.

Scharpf, F. (2009). Legitimacy in the Multilevel European Polity. In Scharpf, F. (Eds.), Community and Autonomy: Institutions, Policies and Legitimacy in Multilevel Europe (pp. 247 – 276). Frankfurt a. M.: Campus Verlag.

Scharpf, F. (2009). The Double Asymmetry of European Integration – Or: Why the EU Cannot Be a Social Market Economy. In Scharpf, F. (Eds.), Community and Autonomy: Institutions, Policies and Legitimacy in Multilevel Europe (pp. 247 – 276). Frankfurt a. M.: Campus Verlag.

Seybert, H. & Lööf, A. (2010). Internet usage in 2010 – Households and Individuals. In: Eurostat (Eds.) Data in focus. 50/2010. Retrieved March 26, 2011, from: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF

Stone Sweet, A. & Sandholtz W. (1997). European Integration and Supranational Governance. *Journal of European Public Policy, 297 (4),* 299-300.

Reding, V. (2010). Privacy matters – Why the EU needs personal data protection rules. SPEECH/10/700. The European Data Protection and Privacy Conference, Brussels, 30 November 2010 Retrieved from: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700

Tömmel, I. (2008). Das politische System der EU. 3. Auflage. München: Oldenbourg. p

Young, A. (2010). The Single Market. In: Wallace, H,. Pollack, M. & Young, A. (Eds). Policy-Making in the European Union (6th Edition). New York: Oxford University Press

Windhoff-Héritier, A. (1987). Policy-Analyse. Eine Einführung. Frankfurt a.M.: Campus Verlag.