ONLINE PERSONAL DATA PROCESSING AND EU DATA PROTECTION REFORM

REPORT OF THE CEPS DIGITAL FORUM

APRIL 2013

RAPPORTEURS: **KRISTINA IRION**
Central European University

GIACOMO LUCHETTA
Centre for European Policy Studies

The CEPS Digital Forum is a multi-stakeholder platform aimed at raising the level of debate about policy challenges that follow from the European Commission's Digital Agenda for Europe. It brings together academics, telecommunications operators, broadcasters, equipment manufacturers, content providers, application producers, internet players, national regulators and European institutions to enable a constructive dialogue on how to achieve a successful transition to an information society for all stakeholders.

CENTRE FOR EUROPEAN POLICY STUDIES
BRUSSELS

This Final Report is the outcome of the CEPS Digital Forum on Online Data Processing and EU Data Reform. The Task Force met four times over a concentrated period from November 2012 to January 2013. Participants included senior executives from the business and industrial sector and other associations. Invited contributors from academia, the EU institutions, civil society, and businesses each presented on selected issues during one of the meetings of the Task Force.

The report is based on a synthesis of the presentations and discussions at the meetings and on the rapporteurs' own research and analysis. It reflects the topics and direction of the discussion among participants and contributors, but does not represent any common position agreed by all participants of the Task Force, nor does it necessarily represent the views of their institutions. A list of participants appears in Annex I.

This Final Report benefited greatly from the contributions of invited guests and speakers. Their involvement was limited to the topic of their expertise in one of the meetings. This report does not represent the positions of contributors or the views of their institutions. All contributors are listed in Annex II.

The report was drafted by Kristina Irion, Assistant Professor at the Department of Public Policy and Research Director at the Center for Media and Communications Studies (CMCS) at Central European University in Budapest, Hungary and Giacomo Luchetta, Researcher at the Centre for European Policy Studies, Brussels.

ISBN 978-94-6138-302-0

Centre for European Policy Studies
Place du Congrès 1, B-1000 Brussels
Tel: (32.2) 229.39.11 Fax: (32.2) 219.41.51
E-mail: info@ceps.eu
Website: http://www.ceps.eu

Table of Contents

Executive Summary and Policy Recommendations

Public policy governing data protection has followed an interesting trajectory in recent years, launched from being a niche regulatory subject into a mainstream concern for policy-makers, individuals and businesses. The emergence of an information-rich economy for which personal data are an important input explains the salience of data protection policy. Many commentators define digital confidence and trust as a key enabler of this information-rich economy. EU data protection regulation has a role to play in the enhancement of that confidence and trust.

The first-generation data protection rules of 1995 are struggling to keep pace with market and technological developments, to gain acceptance, and ultimately to deliver against its objectives. Yet, reform of this area is one of the most ambitious legislative objectives that EU policy-makers are presently grappling with. As a policy issue, data protection tends to polarise opinion, for obvious reasons. EU policy-makers find themselves having to strike a balance between the various interests at stake: How to observe European fundamental rights without offsetting the demands of an information-rich economy and all that has to offer consumers, businesses and the society at large?

Issuing policy recommendations at the same time as the second-generation EU data protection legislation is in progress runs the risk of being judged against the politics of the moment. The scope of these recommendations is more ambitious than merely informing this ongoing legislative process, however. Against the background of online personal data processing, the following policy recommendations address short- and mid-term policy goals and advocate a meta-governance approach to privacy and data protection.

Policy recommendations

Data protection in the EU translates the protection of fundamental rights into *sui generis* rules. As currently proposed, the general data protection Regulation **applies horizontally** for most public and private processing of personal data.[1]

1. In scope, the new regulation is **technologically neutral**; however, the **regulatory division of labour** with national legislation pursuant to the e-privacy Directive and potentially other legislation needs to be further clarified. Some participants of the CEPS Digital Forum stressed that the relationship between the general regulation and the e-privacy Directive should be addressed during the ongoing legislative process.
2. From the vantage point of online personal data processing, fragmentation persists along the lines of the e-privacy Directive. **EU data protection rules** that apply to all information society and value-added services online should be consolidated and thereby **unified** within the regulation.

[1] With the exception of the parallel initiative for a Directive on the protection of individuals with regard to the processing of personal data for police and judicial cooperation in criminal matters and in addition to certain sector-specific data protection legislation.

3. Strengthening the tenets of risk-based regulation, information assurance and management, as well as consumer protection **within** data protection is a plausible strategy in response to the privacy and data protection challenges of the digital environment.
4. The regulation should be further consolidated with the aim to **obtain a single and clear policy**. The draft legislation should be **edited**, using plain language, and **reducing implicit concepts** which really matter, e.g. transfer of personal data to third parties.

In addition, any future regulation should strive to achieve the following concrete and short-term policy aims:

1. Resolve the **legal treatment of online identifiers** so that it remains internally consistent with other provisions.
2. Ensure consistency in the event that definitions of controllers and processors are adjusted so as to retain **responsibility for the means of data processing**. Introduce a rule whereby **consumers cannot be the controller of their personal information** that resides on third party equipment under a non-negotiable agreement with the service provider.
3. Strengthen individuals' consent as the linchpin for quasi-market mechanisms in personal data transactions with a clear **separation principle** that prevents the bundling of online services with individuals' consent to unrelated additional personal data processing.
4. Clarify the concept of **'legitimate interest'** as a legitimate basis for the processing of personal data as well as **defined boundaries** in order to offer legal certainty to controllers and individuals alike.
5. In exercising the new 'right to be forgotten' **controllers should not be left in charge to balance conflicting fundamental rights**, i.e. the right to privacy vs. the right to freedom of expression, without further guidance.
6. Clarify the **scope of the new 'right to data portability'** and, where it is not otherwise legally permitted, require **profiling to be a distinct purpose** to which the data subject has to consent.
7. **Enable technologically mediated compliance**, e.g. complying with documentation duties at the level of IT systems and management through automated IT compliance systems – in other words, the automated means of expressing consent and managing permission.
8. Consistently **strengthen positive regulatory incentives** with the Regulation, using as leverage points:
    a. Processing of personal data where and insofar as this is necessary for the performance of a contract to which the data subject is party, which should ideally incur only the **minimum of administrative burdens**;
    b. **Privileging** the use of **data protection-compliant technologies** by controllers and recognising off-the-shelf compliance for those parts of data processing equipment and software that are sold or licensed to controllers;

   c. Enabling **EU-wide compliance schemes**, in particular for SMEs, (perhaps with variations per industry or sector) and granting legal certainty as well as clarifying the role of codes of conduct in complying with data protection regulation.

9. Fully implement the **one-stop-shop premise** without undermining the mutual assistance and joint operations of national Data Protection Authorities (DPAs). The **consistency mechanism needs more consolidation** so as not to exceed its capacity or inflate the decision-making back-end.

10. Strengthen the capacity for **reflexive governance** at the level of national DPAs and the European Data Protection Board, e.g. defining enforcement priorities.

11. Regarding sanctions, enable DPAs to take into account **commitments by controllers** when imposing a fine. If SMEs are exempted from certain data protection requirements, in lieu of or complementary to a fine, reinstating the requirements to designate a Data Protection Officer (DPO) and documentation duties is a **tactical remedy**.

12. As a transparency measure, require member states to draw up a **public repository of legal data processing obligations** to which the controller is subject.

Medium-term policy recommendations aimed at strengthening data protection as a field of public policy are addressed to the EU and the member states:

1. **Fostering a culture of privacy and data protection** should be firmly embedded in a **meta-governance approach** where member states and the EU co-operate at all levels and ensure the optimal attainment of both objectives through a variety of measures.

   a. In consultation with member states, the EU should adopt a **comprehensive strategy** that addresses all participants in the public and the private sector according to their respective roles and responsibilities.

   b. Data protection legislation is bound to become the centre-piece of EU policy, but its values should be reinforced at various levels and via other measures comprising **public and private policies, technology and cultural measures**.

   c. **Cultural impulses are indispensible** to promote the values of privacy and data protection in the EU and beyond. Measures have to equally target data subjects, controllers, processors and professional groups and should, wherever possible, be integrated with other policy fields at EU and member state level.

   d. In the area of fundamental rights EU and member state bodies should adhere to **principles of procedural legitimacy**, notably participation and transparency, and promote these principles vis-à-vis other stakeholders.

   e. The EU and member states should continue to collect and showcase best practices in the public and private sector in an effort to exchange information and promote the uptake of innovative privacy and data protection solutions.

2. Measures to protect privacy and data protection must be scalable to retain their effectiveness in the information-rich economy.

   a. **Standardisation** and **Privacy-Enhancing Technologies (PETs) in middleware** should become more central in the regulatory strategy, without mandating specific technologies, however.

b. **EU-wide certification** and **compliance schemes** that grant legal certainty need to be prioritised.

c. Policies should recognise the role of **PETs for empowering individuals directly** and promote them.

As privacy and data protection challenges evolve, EU and national governments should regularly review data protection policy implementation, continue to produce evidence and assess the need for (de)regulation where appropriate.

Introduction

Public policy governing data protection has followed a very interesting trajectory in recent years, from being a niche regulatory subject to a mainstream concern for policy-makers, individuals and businesses. The salience of data protection policy can be linked to the emergence of a data-rich economy for which personal data act as an important input resource. Various accounts enthusiastically emphasise the economic growth and innovation potential associated with the use of personal data (BCG, 2012; WEF, 2011 and 2012). They underscore that public policy is an important vehicle to ensure the free circulation of personal data across organisations and frontiers.

The European Union guarantees the fundamental rights to privacy and data protection. In order to give effect to both these fundamental rights, data protection legislation regulates what is legitimate processing of personal data and confers rights to individuals. The EU approach consists of horizontal and comprehensive regulation, which tempers some expectations of rendering personal data a commercial asset class without constraints imposed on its use. At the same time, this regulation struggles to keep pace with market and technological developments, to gain acceptance and ultimately to deliver against its objectives.

The opportunity to influence public policy during the legislative process of the EU data protection reform has allowed for much controversy and politicised debate, which has assumed a global dimension in the online environment. Policy-makers have to balance the opposing interests of companies and business on the one hand and of individuals on the other. Both sides, however, are bound by the elusive notion of trust which, although not a data protection concept itself, is understood to be a key enabler of the new information-rich economy. Data protection policy can help to engender trust and confidence because it defines a framework of rights and responsibilities when using personal information.

This report was produced by the Task Force on Online Personal Data Processing in the Context of the EU Data Protection Reform, an activity of the Digital Forum within the Centre for European Policy Studies (CEPS).[2] The purpose of the Task Force is to develop a dialogue among stakeholders, EU institutions, consumer and user representatives, internet advocacy groups and academics. This activity tackles fundamental questions underlying the present dilemma between policy objectives, compliance strategies and global trends in online personal data processing. Between November 2012 and January 2013 the Task Force held four meetings devoted to the following topics:

1. The economics of privacy and the information economy
2. Compliance, risks and management
3. Old paradigms and new approaches to data protection regulation
4. (R)evolution: The EU data protection reform

[2] It builds on CEPS' expertise in the area of privacy; see inter alia Centre for European Policy Studies et al. (2011).

This report is the outcome of the Task Force and is based on a synthesis of the presentations and discussions at the meetings and the rapporteurs' own research and analysis.

The scope of the Task Force, and hence of this report, is limited to online personal data processing in the private sector. The basis of this report is the EU approach to privacy and data protection, i.e. the fundamental rights approach, and is conscious that corresponding general regulation applies horizontally across public and private sectors. The report aims to assess compliance with data protection rules, particularly in the online environment, against the touchstone of effective regulation and public policy. As an outcome of the Task Force, the report aims at analysing underlying concepts and general principles, thereby deriving policy conclusions to make the EU data protection policy more fit for purpose and today's online technological context. Please note that the outcome constructively engages with the EU data protection framework, but it does not deliver a textual analysis of the EU data protection reform proposal.

This report is structured as follows: section 1 describes the emerging information economy with a view to the role of online personal data processing. Section 2 briefly introduces the fundamental rights to privacy and data protection and the corresponding EU regulatory framework. Section 3 identifies relevant yardsticks against which it assesses data protection regulation, and introduces economic research that would explain some of the contemporary challenges to preserving privacy and data protection online. The next section discusses old paradigms and new approaches to data protection, unpacking regulatory key concepts and unresolved issues for compliance. From a public policy vantage point, section 6 reviews proposals about how to modernise data protection radically or within the existing system. The last section turns to the EU data protection reform proposal followed by conclusions and policy recommendations.

1. The emerging information economy and online data processing

On a global scale and fuelled by an unprecedented 'data boom', economic activities are increasingly information-driven. The Boston Consulting Group estimated that the volume of global data transactions increases annually by 45%, which implies that the data volume doubles every one and a half years.[3] The same study projects that the EU stands to gain €1 trillion annually by 2020, or 8% of EU GDP, stemming from the information-driven economy (BCG, 2012, p.3). The study suggests that two-thirds of this benefit would accrue to consumers and one-third to public and private organisations. Forecasts about long-term efficiency gains and their distribution can be optimistic, yet the principle shift towards value creation that involves some form of information processing is sizeable.

Against this backdrop, policy-makers and pundits proclaim the arrival of the information-rich economy (Acquisti, 2010a; Nissenbaum, 2011; Gervais, 2012). Personal data, likely to be the most important input, emerge as a new commercial asset class that is referred to as the "new oil" of the information-rich economy (ENISA, 2011b, pp. 26ff; WEF, 2011 and 2012). According to Acquisti (2010a, p. 8),

> We live in a consumer data-driven and consumer data-focused commercial revolution in which individuals are at the same time consumers and producers of a most valuable asset: their personal information.

Personal data, however, are not like any raw material that can be gained and exploited, but they relate to individuals and are a protected subject matter under the fundamental rights to privacy and data protection in the EU. This can create tensions between the market's demands for personal data on the one hand and public policy and the rights of individuals on the other.

The law of feasibility

Technical and economic constraints on the processing of personal data have almost disappeared (Brown, 2011):

- Qualitative and quantitative leaps: what can be collected, analysed, searched, stored, retrieved, connected in a computerised online environment is radically different from the pre-ICT era (Kang, 1998; Lessig, 2006);
- Costs of online data processing have plummeted: the price per unit of performance of processing power, sensors, bandwidth, and storage elements has gone down steeply (Brown, 2011) and will continue to do so (Yoo, 2011);

Today's socio-technological environment fosters the generation of more and more data, both personal and non-personal:

[3] Social network services and the "Internet of Things" are two key drivers of the data expansion (BCG, 2012, p. 10).

- Always-on and ubiquitous internet and connected (mobile) devices that are often personalised as well as the increasing interlinking of online and offline through geo-location technology and localised services
- Web 2.0 and the production and sharing of user-generated content, either publically or semi-publically
- The internet of things and services that connects devices, sensors and applications produces a constant stream of information (RAND, 2008, p. 17).
- Cloud computing, i.e. access to remote computing resources on demand and the corresponding developments in cloud services.

There are several ways in which online companies, in particular, derive economic value from personal information (Acquisti, 2010a; Brown, 2010; ENISA, 2011, pp. 26ff; Goldfard & Tucker, 2011; WEF, 2012; BCG, 2012):

1. Generating efficiencies in the allocation and/or production process
2. Creating new forms of interactions, personalised services and other value propositions
3. Targeting advertising or geo-localised services to help match supply and demand, thereby lowering advertising expenditure and/or increasing advertising effectiveness
4. Trading and sharing personal data with third parties and across networks, thereby merging disparate data sets together
5. Generating new insights about individuals through profiling and from exploiting advanced predictive analytics to large data sets (so-called "big data")

Private-sector participants and contributors to this Task Force formed a representative sample of companies engaged in the listed commercial activities.

The emerging online personal data ecosystem is complex and highly interconnected with large intermediaries at its centre, which essentially aggregate, process and distribute information, including personal information (see Appendix 1 in WEF, 2012, p. 32). Online business models vary and are constantly refined but they essentially generate revenues via fees charged to users, or advertisements or any combination thereof. A wide range of online services thrive from online and/or targeted advertising which may involve some degree of monetising users' personal information.[4] Some Task Force contributors observed that many online services are not fully transparent about their data handling practices or can only be accessed on a 'take-it-or-leave-it' basis where consumers have to agree to extensive data processing operations by the website in exchange for a service.

[4] Online advertising techniques and practices vary widely also in as much they rely on personal data processing.

Two developments that are likely to emerge hand in hand can stifle the transition to and growth of the information economy, as discussed below:

On the one hand, both online and offline companies, which accumulated large data sets over time, are now very keen to exploit 'their' commercial asset. The attitude to claim a sort of ownership and control over corporate data, including the personal data of customers and other individuals, may not fully correspond with the roles, rights and responsibilities under the legal framework in the EU (ENISA, 2011b, pp. 26ff; WEF, 2012, p. 5). However, with commercial expectations running high – one Task Force contributor compared the phenomenon to the gold rush – data protection regulation and fair information practices are easily perceived as an obstacle.

On the other hand, consumers and users frequently lack assurance about the use of their personal information. Worries about privacy can negatively impact e-commerce and online services (Eurostat, 2009; for US see Pew, 2012). A vast majority of users are concerned by how their data are used (70% according to Eurobarometer, European Commission, 2011; 88% according to BCG, 2012, p.12). At the same time, awareness of data processing activities fluctuates; depending on the industry concerned, between 30% and 50%. These results are fairly in line with the 2011 Eurobarometer, where it is stated that about 75-80% of respondents do not feel in control of the data they disclose online, and that the level of trust in internet companies is very low, at 22% (European Commission, 2011). Nevertheless, individuals are not generally inhibited from sharing personal data in a trusted relationship (Nissenbaum, 2010, p.2). In online transactions this can be achieved by demonstrating transparency and responsibility in addition to deploying state-of-the-art data management techniques, all of which offer the potential of becoming a key market differentiator.

The combined effect highlights the urgent need to consider public policy to fix the problem, with the aim of infusing the trust that is so central to the information economy. The EU is working to revamp its data protection rules of 1995 to set new rules that can deliver data protection, legal certainty and, ultimately, trust with the wider ambition to enhance the EU's competitiveness and spur innovation and competition in privacy-savvy product and services (European Commission, 2012a; 2012b, Annex 10). Finding the right balance when protecting personal data through regulation will be crucial. Failure to establish a trusted flow of personal data under a firm but flexible regulatory framework could result in forfeiture of up to €440 billion of gains (BCG, 2012, p.111).

Moreover, data protection creates significant compliance costs, which almost all participants in the Task Force representing larger online companies underlined. According to the European Commission's impact assessment, the present EU framework for data protection imposes on European companies a total of €5.3 billion of administrative burdens.[5] Another

[5] The impact assessment entails only a partial cost-benefit analysis; therefore the overall burden is likely to be even higher. For example, costs related to obtaining consent from users seem to have escaped quantification. See Etro (2013).

source reports that very large companies (with more than 1,000 employees) spend up to €2.5 million per year in privacy compliance costs (Ponemon Institute, 2011). Overcoming the fragmentation of data protection regulation within the EU alone promises to cut an estimated €1.6 billion from the €5.3 billion administrative burden for companies doing business in Europe (European Commission, 2012b, Annex 9).

Last but not least, the EU is also spearheading the protection of personal data worldwide and, especially in a globe-spanning medium such as the internet, the EU approach is criticised for being overly ambitious. Considerations about the EU's global competitiveness are necessary, but positions tend to reflect different philosophies on the virtues of data protection. One end of the spectrum would argue for strong data protection in the EU that could infuse confidence in EU businesses, also from outside the region. At the other end of the spectrum, it is argued that data protection should not obstruct online businesses but rather provide for the global flow of personal data (WEF, 2012, p. 29). These positions are not mutually exclusive, but where the regulatory pin is placed depends in part on a contemporary interpretation of fundamental rights, which is also partly a political decision.

2. EU data protection rights and regulation

2.1 Fundamental rights to privacy and data protection

This report necessarily begins by invoking the fundamental rights that underpin the approach to privacy and data protection in the European Union, because this ultimately impacts the regulatory level. Relevant sources that serve to protect the rights to privacy and data protection are the national constitutional heritage of EU countries, EU primary law and international human rights law.

2.1.1 EU member states

The right to privacy is recognised in most constitutions of EU member states, and where this is not explicitly the case (e.g. in Germany, France and Sweden), its substance is derived from other constitutional guarantees, such as the right to human dignity but also liberty. Although the wording and the construction vary from country to country, the right to privacy – explicitly or implicitly – forms part of the common constitutional heritage of all EU member states (Koops et al., 2007, p.152).

With a few exceptions (e.g. the Netherlands and Sweden), the right to data protection is commonly not recognised in EU member states' constitutions. Nonetheless, the right to data protection can be derived from the national constitutional heritage of most EU countries as an extension of the right to privacy (FRA, 2010, p.14; Koops et al., 2007, p.153).

2.1.2 EU primary law

The Charter of Fundamental Rights (CFR) of the European Union of 2000 provides in its Art. 7 for the right to respect for private and family life.

Art. 7 of the Charter of Fundamental Rights of the European Union

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

With the enactment of the Charter of Fundamental Rights of the EU in 2000, the right to data protection is now listed as a self-standing fundamental right (Art. 8) after the right to privacy in the catalogue of freedoms of the individual. Art. 6(1) of the Treaty on European Union (TEU) incorporates the Charter into EU primary law, and the European Court of Justice of the EU now refers to data protection as a fundamental right (CJEU, *Promusicae*, 2008).

Art. 8 of the Charter of Fundamental Rights of the European Union

Protection of personal data

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

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Interestingly, Art. 8(2) CFR elevates a fair number of core data protection concepts into the EU fundamental rights *acquis* (Centre for European Policy Studies et al., 2011, p. 20). It carries some of the regulatory substance that circumscribes requirements for lawful data processing (e.g. fairness, purpose specification, consent, etc.), as well as certain rights for the individuals concerned and independent supervision of "these rules". Art. 8(2) CFR provides that any processing of personal data must be legitimate on the basis of either the concerned individual's consent or law. Hence, the new right to data protection also protects *against* the processing of personal data where there is no legitimate basis.

The CJEU also maintains that the right to data protection is not absolute, "but must be considered in relation to its function in society" (CJEU, *Volker und Markus Schecke and Eifert,* 2010). Whenever the processing of personal data has its legitimate basis in a law, Art. 52(1) CFR must be complied with. It provides that, subject to the principle of proportionality, limitations to the exercise of this right may be made only if they are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others (Art. 52(1) CFR).

Moreover, EU primary law holds a second reference to the right to the protection of personal data in Art. 16(1) of the Treaty on the Functioning of the European Union (TFEU). Another novelty is Art. 16(2) TFEU, which equips the EU with the distinct competence to adopt data protection regulation, including "the rules relating to the free movement of such data".

2.1.3 International human rights law

From the body of international human rights law, only the European Convention on Human Rights (ECHR) is revisited because it reinforces the trend to regulated data protection.[6]All EU member states are signatories of the ECHR and the EU is committed to accede to it (Art. 6(2) TEU). Art. 8(1) ECHR provides for the right to respect for private and family life, among others. In order to be justified, any interference with this right by a public authority must be in

[6] For an overview, see Bygrave (2008).

accordance with the law and necessary in a democratic society in pursuit of one of the interests enumerated in Art. 8(2) ECHR.

In the jurisprudence of the European Court of Human Rights (ECtHR), Art. 8 ECHR entails a positive obligation of the signatory states to introduce measures that would give effect to the right for respect of private life, including in the private sphere (ECtHR, *X and Y v Netherlands*, judgement of 26 March 1985, para. 23). Moreover, the Court has interpreted Art. 8 ECHR as encompassing data protection rules from the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[7] Convention 108 introduced a system of data protection regulation that is systematically similar to the EU regulatory framework on data protection.

It is important to note that, outside Europe, constitutional traditions and international human rights law recognise the right to privacy, but in their respective contexts cannot be interpreted to require a comprehensive data protection approach. Nonetheless, third countries maintain and continue to adopt data protection laws (see Rule & Greenleaf, 2010; Koops et al., 2007).

2.1.4 The constitutionalisation of the right to data protection

With the advent of automated and computerised data processing, the right to privacy now rests to a considerable extent on effective data protection. The right to the protection of personal data has evolved from a regulatory strategy to guarantee privacy to a modern fundamental right in the EU. This constitutionalisation has certainly entrenched the right to the protection of personal data further. Purtova (2012, p. 223) thus rightly observes that "it is no longer possible to avoid human rights issues when discussing data protection matters".

After the Lisbon treaties, EU primary law now furnishes two legal bases for the new right to data protection (Art. 6(1) TEU in connection with Art. 8 ECFR and Art. 16(1) TFEU) as well as a new EU competence to legislate this area (Art. 16(2) TFEU). Like the right to privacy, the right to data protection can be subject to restrictions as long as the restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard important general interest objectives. Moreover, the rights to privacy and personal data protection need to be reconciled with other fundamental rights, such as the right to freedom of expression, by balancing competing rights against each other (FRA, 2012).

The following section introduces the EU regulatory framework on personal data protection, portions of which actually pre-date the Charter's right and largely inspired it.[8]

[7] Court of Europe, European Treaty Series, No. 108, commonly referred to as Convention 108.

[8] See e.g. the explanations relating to Art. 8 CFR.

2.2 EU framework on personal data protection

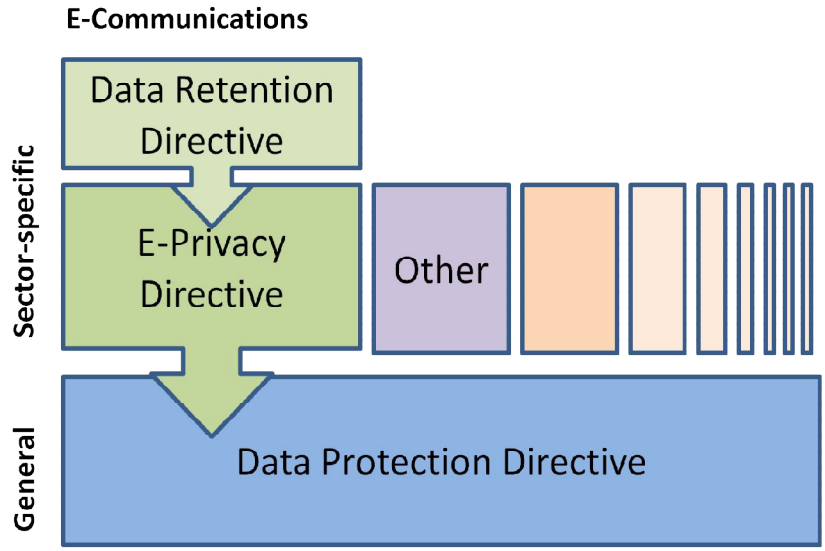
The EU regulatory framework on data protection comprises several instruments that address different EU policy domains. However, for this report, which is concerned with online personal data processing in the private sector, the focus is on legislation that aims at establishing an internal market, that is, legislation falling within the former first (or Community) pillar. Privacy and data-protection policies in the EU's Area of Freedom, Security and Justice (AFSJ) fall outside the scope of this report.[9]

It is important to note that the first edition of an EU data protection framework under the former first pillar did not emerge from the void. The 1995 Directive builds conceptually on two international standard-setting instruments: the non-binding 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data from 1981. Both instruments endorse a set of principles intended to narrow the scope of legitimate personal data processing and to introduce procedural legitimacy and accountability.

The core instrument is Directive 95/46/EC 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 (hereinafter, the data protection Directive). Other sector-specific harmonisation directives complement the general data protection Directive. In the context of this report, the most significant is Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications (hereinafter, the e-privacy Directive). Finally, there is a plethora of legislation at both the EU and the member state level that mandates data processing for public and private organisations. Within the EU data protection framework, such legislation provides a legitimate basis if it meets constitutional requirements.

[9] See the study for the European Parliament on "Towards a New EU Legal Framework for Data Protection and Privacy. Challenges, Principles and the Role of the European Parliament" carried out by the Centre for European Policy Studies, Centre d'Etudes sur les Conflicts, Vrij Universiteit Brussel (2011).

Figure 1. EU data protection framework pertaining to online data processing



Source: Authors' own elaboration.

The following carries a highly condensed summary of the main data protection instruments in the EU that govern online personal data processing activities in the private sector.

2.2.1 The data protection Directive

The data protection Directive harmonises member states' national laws (to a certain extent) with the dual aim to:

1. protect the fundamental right to privacy with respect to the processing of personal data, and
2. provide for the free flow of personal data between EU member states (Art. 1).

This dual ambition exposes the regulation to a fair amount of internal tension whenever personal data protection and personal data flows cannot be achieved simultaneously.

The Directive applies horizontally across public and private sectors' automated or systematised personal data processing activities. The regulatory approach is in compliance with *a priori* and comprehensive regulation. 'Personal data' and the 'data subject's consent' are key definitions of the Directive (Art. 2), which are decisive for its application. The Directive operates with different roles, i.e. the data subject, the controller, the processor and the recipient, to which different rights and responsibilities are attached. Conceptually, the data protection Directive endorses five principles (Art. 6, see box below) and six alternative legal grounds that render data processing legitimate (Art. 7), out of which the data subject's unambiguous consent to the data processing is just one possibility.

Art. 6 of the data protection Directive

1. Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. […];
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; […];
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. […].
2. It shall be for the controller to ensure that paragraph 1 is complied with.

The processing of special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life is prohibited (Art. 6(1)) unless derogations apply (Art. 6(2)).

Aside from the ability to legitimise most data processing with an unambiguous consent, data subjects have several rights in relation to their data, such as the rather comprehensive rights of access (Art. 12) concerning all matters of personal data processing and which can further extend to demand rectification, erasure or blocking of personal data; or the right to object (Art. 14), which can pre-empt certain legitimate bases for data processing and the use of personal data in direct marketing.

Controllers are responsible for adhering to the data protection principles (Arts 6(2)) and rules, including certain information duties (Arts 10 and 11), being responsive to data subjects' rights, and ensuring the security of the processing (Art. 17), as well as being liable for any damages and supervised by the competent data protection authorities (DPAs). Processors are auxiliaries under the authority of the controller which receive instructions on the data processing (Art. 17(3)).

Transfer of personal data from the EU to a third country is only permissible if an adequate level of personal data protection is ensured in that third country. Finally, the Directive mandates that member states entrust independent authorities with the monitoring and enforcement of the data protection regulation (Art. 28(1)).

As secondary EU legislation, the Directive is addressed to the member states and does not produce direct effects for individuals and companies. Every member state transposed the data protection Directive into national law and this framework has been operating for almost 15 years now. However, national variations in terms of implementation, interpretation and enforcement prevail.

With the aim to modernise data protection in the EU, a draft proposal for a new general data protection Regulation is currently going through the legislative process (European Commission, 2012a). If passed it would replace the current data protection Directive with the new Regulation, the hallmarks of which are discussed in section 6 below.

2.2.2 The e-privacy Directive

The 2002 e-privacy Directive, as amended by Directive 2009/136/EC, forms part of the regulatory framework for electronic communications. The Directive spells out the rights of users and subscribers, including legal persons, of electronic communications services and protects the confidentiality of communications, while ensuring the free movement of personal data within the EU. The e-privacy Directive makes reference to central notions of the data protection Directive, for example the definition of consent.

The economic significance of the e-privacy Directive is mounting steadily due the shift towards digital services. This effect can be best observed in three areas:

- The processing of traffic and location data,
- Unsolicited commercial electronic communications and
- The storing of information and access to information already stored in the terminal equipment of a subscriber or user (the so-called 'cookie rule').

The three examples of the regulatory effect of the e-privacy Directive are explained below.

The e-privacy Directive governs traffic data and location data (Arts 6 and 9), which are increasingly in demand and processed by electronic communications providers and third parties. As an illustration, mobile apps frequently involve location data when offering geo-localised services, such as maps and local information. Under the scope of the Directive, the provision of value-added services requires the processing of additional traffic data or location data (Art. 2(g)), which is legitimate when the concerned user or subscriber has given his or her consent.

Art. 13 of the e-privacy Directive imposes limitations on unsolicited commercial electronic communications, namely direct marketing via automatic calling systems, fax and email. Here an exception that produces an effect beyond the sector-specific scope of the Directive allows the use of email for direct marketing in the context of an existing customer relationship. However, in order to benefit from this exception, the customer's email address must have been obtained in accordance with the general data protection Directive.

The introduction of the so-called 'cookie rule' in 2009 (Art. 5(3)) is an attempt to come to terms with the increasing practice to store or access already stored information on the user's or subscriber's communications device for a variety of purposes. These are often called 'HTTP cookies', but the new rule is technologically neutral. This practice is "only allowed on

condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing." (Art. 5(3)) As an exemption from this rule, cookies are permissible if they are technically required in the process of electronic communications or in order to carry out an information society service explicitly requested by the subscriber or user (WP29, 2012, p.2).

All three examples described above have in common that they concern most online transactions and offerings of content and services, for free or against remuneration, to the effect that the e-privacy Directive develops into a mainstream data protection instrument.

The e-privacy Directive is not concerned by the ongoing data protection reform. As it stands, only technical adjustments are planned to take into account the transformation of the data protection Directive into a regulation and to clarify the relationship between the two instruments (see the Draft for a general data protection Regulation, Recital (135)).

2.2.3 Other legal obligation that mandates the processing of personal data from the controller

Apart from the positive regulation of data protection, an ever-increasing body of legislation at both the EU and the member state levels authorises, requires or obliges the processing and storage of personal data. Examples are record-keeping obligations, such as those contained in national tax and social security laws. Under the EU regulatory framework for data protection, these laws actually provide a legitimate basis for data processing (data protection Directive, Art. 7(c)). Because such statutory plug-ins to data protection interfere with the exercise of fundamental rights, the interference must be justifiable (Art. 8(2) ECHR and Art. 52(1) CFR). This link between specific laws and data protection regulation is not always well explored and, arguably, there may be legislation in the member states and the EU that does not meet the threshold for justification (ENISA, 2012b, p. 48).

An area that is experiencing a proliferation of new obligations is government access to private-sector data for the purpose of national security and law enforcement (Centre for European Policy Studies *et al.*, 2011 p. 15). Central to this report is Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (hereinafter, the data retention Directive). This Directive, which amends the e-privacy Directive, aims at harmonising member state provisions concerning the obligations of the aforementioned providers to retain certain data in order to ensure its availability for law enforcement purposes (Art. 1(1)).

The data retention Directive defines types of data to be retained between six months and up to two years, depending on the national transpositions in the member states. Data retention is concerned with defined sets of traffic and location data, but it should not interfere with the

actual content of electronic communication (Arts 1(2) and 5). This Directive leaves it actually to the member states to define a catalogue of serious crimes for the investigation, detection and prosecution of which the retained data can be accessed by the competent authorities (Art. 1(1)). Thus, the harmonisation stops short of the legal requirements under which the data can be accessed.

2.3 Supervisory authorities in the EU

Supervision and enforcement are key features in assessing the functioning of the EU data protection framework. While much attention is focused on the required independence of the competent supervisory authority (Art. 8(3) CFR; CJEU, *European Commission v. Germany*, 2010; and CJEU, *European Commission v. Republic of Austria*, 2012), this section explores the distribution of competences at national level and EU level.

2.3.1 National supervisory authorities

EU data protection regulation mandates supervision and enforcement by independent supervisory authorities, so-called national DPAs (data protection Directive, Art. 28(1)). Member states have to designate one or more public authorities to monitor the application of national legislation pursuant to the data protection Directive and the e-privacy Directive. Thus, local arrangements tend to reflect national administrative and governmental cultures as well as divisions of competences according to sectors.

In the majority of member states, the competencies for general data protection regulation and pursuant to the e-privacy Directive are divided between different authorities. On the one hand, there are one or more national DPAs (this may be in federal or regional-configured states, such as Germany and Spain, further distributed to regional and state DPAs) in charge of data protection in the private sector. On the other hand, sector-specific DPAs, such as the National Regulatory Authority (NRA) for the electronic communications sector, which are in charge of enforcing the e-privacy Directive (e.g. in Germany and the Netherlands) (FRA, 2010, p. 19). Often, data protection competence is embodied in a personalised authority such as a Commissioner for Data Protection (e.g. in Germany or in Hungary) or an Ombudsman (e.g. Finland) supported by staff.

2.3.2 Responsibilities for data protection at the EU level

For EU institutions, the European Data Protection Supervisor (EDPS) is an independent supervisory authority charged with supervising the EU institutions' and bodies' adherence to their own set of data protection rules, i.e. Regulation (EC) 45/2001. EDPS is not involved in enforcing generally applicable data protection regulation but has an important advisory role on EU policies and legislation that affect privacy. In this capacity, the EDPS also participates in EU-wide and international regulatory networks on data protection.

The so-called Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data (hereafter WP29) is an EU-wide advisory body that is composed of a representative of each member state's DPA(s), the EDPS, and the European Commission (data protection Directive, Art. 29(1) and (2)). Its main tasks are to contribute to the uniform application of national measures by:

- examining the national application of legislation pursuant to EU data protection regulation,
- issuing opinions and recommendations on the interpretation of core notions in data protection regulation and
- enhancing cooperation between national DPAs in the interest of joint procedures and enforcement actions (data protection Directive, Art. 30; e-privacy Directive, Art. 15).

Although WP29 has stepped up its activities, which aim to streamline the application of the national laws pursuant to EU directives, the results of its endeavours are not deemed sufficient to effectively deal with intra-European data transfers. Furthermore, the Kantor study criticises legal fragmentation and the fact that WP29 consistency mechanisms cannot be authoritatively imposed at the domestic level (Kantor Ltd., 2010, para. 92).

Additionally, two specialised EU agencies should be mentioned that have non-operational competencies in relation to data protection: first, the Fundamental Rights Agency (FRA) provides EU institutions and bodies, as well as EU member states when implementing European law, with assistance and expertise relating to fundamental rights.[10] Second, the European Network and Information Security Agency (ENISA) is a centre of expertise which studies the intersection of privacy and data protection with information technology and security as well as economics.[11]

[10] See, for example, the studies "Data Protection in the European Union: The Role of National Data Protection Authorities" (FRA, 2010) and "Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package" (FRA, 2012).

[11] A list of ENISA publications in the area of identity and trust can be found on its website http://www.enisa.europa.eu/activities/identity-and-trust/library. The most important contributions include the studies on Privacy, Accountability and Trust – Challenges and Opportunities (ENISA, 2011a), Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments (ENISA, 2011b), data breach notifications (2011), on the use of cryptographic techniques 2011), on monetising privacy (ENISA, 2012a), on data collection and storage (ENISA, 2012b), on the right to be forgotten (2012) and on online tracking and profiling (2012).

3. An assessment of EU data protection policy

This report aims to assess EU policy and regulation of online personal data protection and thus needs to adopt an analytical angle against which the existing concepts and the reform proposals can be probed. Despite a significant body of research pointing to the numerous shortcomings of today's regulation and practice, this section first clarifies what are the right yardsticks for assessing the EU data protection framework (Baldwin et al., 2012, p.25) and subsequently reviews arguments on what makes good regulation.

3.1 What are the right benchmarks for assessing EU data protection regulation?

Given numerous, but rather confusing, accounts of what data protection is and is expected to deliver, understanding the purpose and motivation of its regulation becomes an important intermediary step. The following paragraphs provide arguments that exclude data protection from these regulatory regimes and adopt a fundamental rights approach.

Data protection is ***not:***
- economic regulation,
- consumer protection regulation,
- immaterial property rights,
- risk-based regulation,
- information assurance or management or
- risk-based regulation.

- **Not economic regulation**

Despite a recent trend to analyse the economics of privacy and data protection (see section 3.3 below), data protection regulation is not economic regulation (Acquisti, 2010a, p.3; ENISA, 2012a, p.1). Economic regulation is characterised by a direct intervention in market decisions, such as pricing, competition, market entry or exit, and this is mostly justified by the aim to correct market failure (Veljanovki, 2010, p.20). In contrast, the data protection Directive takes a horizontal approach and addresses equally data processing activities in both the public and private sectors, as well as market and non-market activities. Although there are a few propositions that explain market failure in the context of privacy and data protection, the expressive ambit of EU data protection regulation is the protection of the fundamental rights to privacy and data protection. Hence, as a regulatory sphere, data protection does not have to satisfy allocative efficiency in the strict economic sense. However, it should not overlook the economic implications that enhance the effectiveness of the regulation (see section 3.3.5 below).

- **Not consumer protection**

Data protection is also not consumer protection, which refers to a cross-cutting EU policy field that aims at enhancing the positions of consumers and end-users of products and services (Art. 169 TFEU). Insofar as consumer protection regulation modifies contract law to the benefit of the consumer (e.g. regarding unfair terms and practices), it departs from the 'party autonomy' principle. Conversely, data protection regulation strongly emphasises the control and autonomy of the individual when it allows his or her consent to legitimise the processing of personal data (WP29, 2011, p. 8). The notion that the interest of data subjects deserves special protection can nevertheless be found in a number of provisions in the data protection Directive (Art. 7(d) and (f)) – a trend that is likely to be reinforced with the data protection reform (European Commission, 2012a; RAND, 2009, p.30).

- **Not property rights**

As such, personal data does not confer any property right that would then protect the subject matter vis-à-vis other parties (the so-called *erga omnes* effect) (Lynskey, 2013; Purtova, 2012, p. 80 and p. 250). Public and private stakeholders continue to invoke 'information 'ownership' which may wrongly imply some generic proprietary right (Reed, 2010; WEF, 2011). Property rights subsist in chattels on which data may be recorded (e.g. sheets of paper, disks, pen drives, etc.) but not in the information itself. Admittedly, information can sometimes be subject to intellectual property protection, such as copyright, but this does not subsume personal data in general. Data protection is *sui generis* regulation that does not replicate concepts of property protection. Using 'propertisation' as a strategy to introduce a market mechanism for personal data is discussed in more detail in section 5.1 below.

- **Not information assurance or management**

The protection of personal data cannot be fully explained in terms of information assurance or management, which is a practice of managing ICT-related risks in order to ensure confidentiality, integrity and availability. First and foremost, EU data protection regulation establishes that personal data must be processed fairly and lawfully and compatibly with specified, explicit and legitimate purposes (data protection Directive, Art. 6(1)(a) and (b)).Only insofar as the data processing is already legitimate does the data controller have to ensure the accuracy, confidentiality and security (data protection Directive, Arts 6(1)(d), 16 and 17(1)). Thus, information assurance and management duties arise under data protection regulation as an obligation placed on the data controller, e.g. the state-of-the-art principle according to which data controllers shall "ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected" (Art. 17(1) of the data protection Directive).

- **Not risk-based regulation**

In general risk-based regulation seeks "to control relevant risks, not to secure compliance with sets of rules" (Baldwin et al., 2012, p. 281). However, a purely risk-based approach would not suffice to protect the right to privacy and data protection because it would presuppose the legality of data processing activities regardless of individuals' fundamental rights to privacy and data protection. Data protection regulation already borrows from risk-based regulation, e.g. special categories of personal data receive a higher level of protection because of the 'riskiness' of processing sensitive information (Art. 8 of the data protection Directive).

Risk-based regulation entered the discussion surrounding the legislative process of the draft general data protection Directive. Accordingly, more emphasis should be given to a gradual regulatory approach under which controllers' obligations would step up relative to the riskiness of the processing operation in question. This solution has the charm that with the increasing sophistication of the processing of personal data, controllers can also be expected to take more advanced steps to ensure compliance with data protection regulation. How to create meaningful thresholds for risk-based regulation in this area could be more controversial because many of the regulatory requirements are interdependent (e.g. the controller has interrelated responsibilities of notification, documentation and accountability).

- **But fundamental rights approach**

Data protection in the EU translates the protection of fundamental rights into *sui generis* rules (Kantor, 2010, para. 26; RAND, 2009, p.27) while invoking supporting elements from other regulatory regimes. The regulatory literature acknowledges a rights-based and public interest rationale for regulation (Baldwin et al., 2012, p.22; Feintuck, 2010).Consequently, this Task Force took a fundamental rights-based approach when appraising data protection regulation's functioning and impact (CEPS Digital Forum, 2012) but against this backdrop considers supporting measures, such as a meta-governance approach to privacy and data protection.

As is the case with most *sui generis* regimes, however, little specific guidance can be deduced from regulatory experiences elsewhere. However, when assessing the performance of EU data protection regulation, wrong assessment benchmarks should be refused. In other words, data protection regulation does not need to perform solely against efficiency criteria that guide economic regulation or measures that are commensurate with the risk, as in risk-based regulation.

3.2 Is data protection meeting good regulation standards?

Nonetheless, universal standards on what makes good regulation "have general currency" to also assess data protection regulation and performance (Baldwin et al., 2012, p. 26) and are explored below. This section amalgamates literature on regulatory governance and the EU smart regulation strategy when drawing up a framework against which it assesses the

performance of EU data protection regulation. As an EU act, data protection is now expected to internalise the hallmarks of smart regulation.

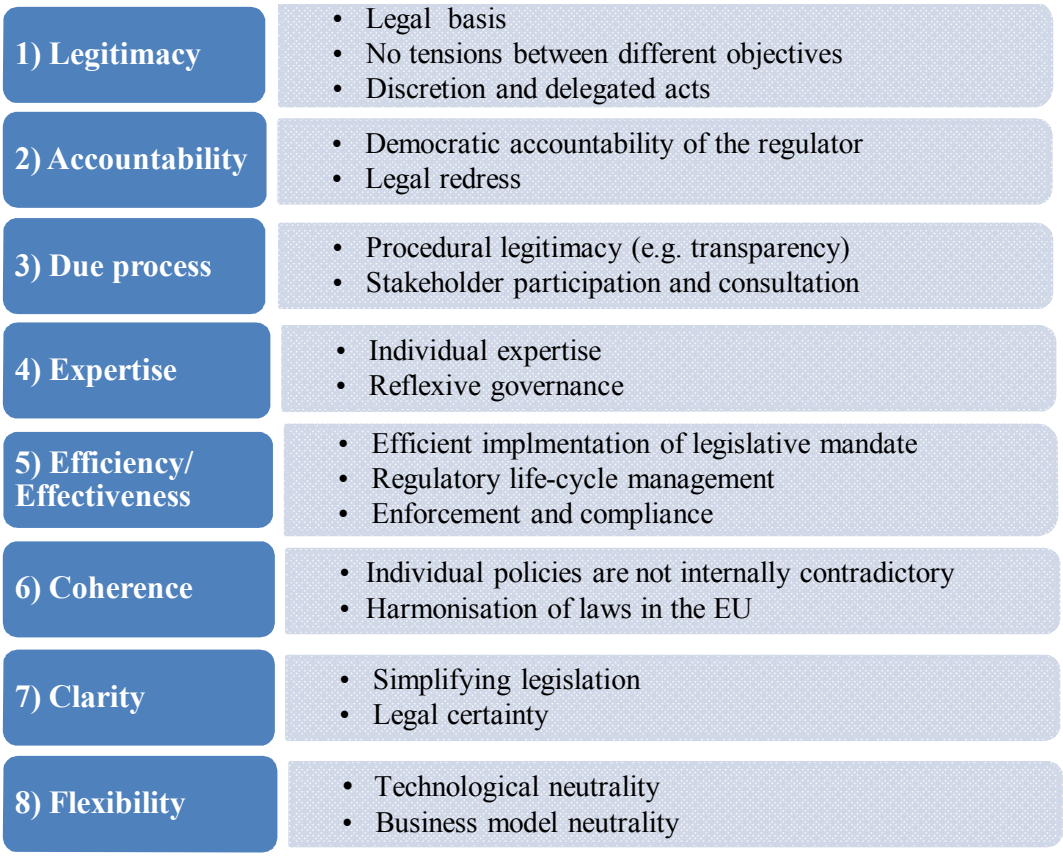
3.2.1 What good regulation has to achieve

In the theory of regulation, "what constitutes 'good regulation' is difficult to establish and is a matter that is inevitably subject to contention" (Baldwin et al., 2012, p. 37). As a bottom-line, Baldwin et al. (2012, p. 26) propose five criteria to identify good regulation: 1) legitimacy, 2) accountability, 3) due process, 4) expertise and 5) efficiency as well as effectiveness. This last criterion means efficiency in pursuit of the regulation's objectives and its effectiveness. In addition the OECD (2005) advances a sixth criterion, policy coherence, which incidentally encourages harmonisation legislation in the EU aimed at the establishment and functioning of the internal market (Art. 114 TFEU).

Beginning with the better regulation agenda, the 2010 EU smart regulation strategy of the European Commission stepped up its commitment to manage the quality of regulation throughout the lifecycle (European Commission, 2010a).The strategy aims on the one hand at making regulation more efficient through an increasing reliance on *ex ante* impact assessment and *ex post* evaluation, which are evidence-based (linking it to criteria (5) above). On the other, it aims at reducing administrative burdens, simplifying legislation and making legislation clearer and more accessible. The latter aim adds a seventh criterion to the catalogue, namely clarity.

An eighth and final dynamic criterion (flexibility) helpfully expands this catalogue that is keeping pace with the economic and technological state-of-the-art (Black et al., 2005; OECD, 2005). The resulting catalogue of eight criteria that characterise good regulation is summarised in Figure 1 below.

Figure 2. Catalogue of criteria for good regulation



Source: Authors' own elaboration.

3.2.2 Assessing EU data protection regulation

This section analyses the EU framework on data protection as it pertains to online personal data processing against the catalogue of criteria for good regulation. In retrospect it considers experiences with the EU regulatory framework on data protection and introduces a forward-looking prognosis regarding the reform proposals.

1) Legitimacy

In light of EU primary law and the new EU competence in Art. 16 TFEU, the legal basis and mandate for EU data protection legislation are not causes for concern. Instead, and as a recurrent feature of EU harmonisation legislation, the concerns centre on the dual aim of EU directives on data protection (see section 2.2.1). As one participant of the Task Force argued, the combined objective to ensure the protection of personal data and the free flow of personal data between member states creates tensions because of apparently clashing philosophies.

However, the data protection Directive itself offers an interpretation that would reconcile the different ends. According to the Directive, member states should not restrict or prohibit in their national data protection laws the free flow of personal data within the EU (Art. 1(2)).

Thus, in the internal market, cross-border processing of personal data should be enabled as long as personal data are lawfully obtained and processed in compliance with the data protection Directive. What hinders EU-wide data protection appears to be more an issue of the inconsistency of national legal frameworks and their efficient implementation than tensions between the objectives of data protection and the internal market.

2) Accountability

At the EU level, it can be observed that Art. 28(5) of the data protection Directive makes it obligatory for national DPAs to publish a report on their activities at regular intervals. A critique, which is already embedded in the EU regulatory framework and therefore extends to the national level, is that DPAs may have too many different functions. A national DPA is expected to supervise, enforce, guide, advise, approve and advocate and, depending on the particular role assumed, the authority is required to constantly change perspectives. This requirement may undermine the impartiality and arms-length relationship of the institution (Kantor, 2010, para. 106; RAND, 2009, p. 36).

The data protection Directive requires both administrative and judicial remedies for any breach of an individual's rights under national data protection laws (Arts 22 and 28(4)). Commonly, the parallelism of regulatory supervision and judicial redress is considered to be a strong accountability mechanism. Ultimately, national courts oversee the decisions of national DPAs, and individuals have the additional possibility to call on national courts for decentralised enforcement of the data protection Regulation. Insofar as democratic accountability of national DPAs and the right to appeal against their decisions are concerned, this has to be taken into account when assessing national data protection regimes.

The accountability of data controllers and processors, however, is a question of regulatory effectiveness, as discussed below.

3) Due process

A regulation adheres to due process requirements if regulatory procedures are sufficiently transparent (e.g. work programme, draft and final decisions are published) and participatory (consultations, right to be heard). The split between EU legislation and member states' transposition means that local governmental and administrative culture will influence due process in the implementation of the law. Nonetheless, there are issues of due process that can be traced back to the provisions of the EU data protection Directive. On a positive note, this Directive recognises the need for transparency in that it requires DPAs to maintain a public register of processing operations that have been notified to them (Art. 21(2)).

Participation, however, is less pronounced under the present framework, which may for example hamper due process when drawing up private codes of conduct at national and EU level (Art. 27). Also, WP29 does not allow for participation of civil society and business

representatives irrespective of the consideration that DPAs are supposed to make up for power imbalances (Poullet & Guttwirth, 2008, p. 27; RAND, 2009). Attention to the fair representation of the interests of data subjects vis-à-vis data controllers is becoming paramount the more the information-rich economy progresses and the role of private policies increases (e.g. codes of conducts but also standards-setting).

In the preparation of and during the legislative process of the data protection reform, the European Commission launched two public consultations and held targeted consultations with private sector organisations, NGOs and member states. It also convened public events and fora to discuss contemporary challenges to data protection, to introduce and stimulate reform proposals and to gather stakeholders' feedback. Task Force members participated in these events and CEPS contributed by organising a public panel on data protection reform, adding to the host of events surrounding the international 2013 data protection day, celebrated on January 28th every year.[12]

4) Expertise

In some regulatory regimes, there is pressure to delegate expertise to specialised agencies (Majone, 2005, p. 135; Gilardi, 2005, p. 102), while in data protection, DPAs were set up as guardians and to institutionalise data protection (FRA, 2010, p. 10). Bundling expertise obviously matters, but requiring too much of it would actually be counterproductive to promote good practices in data protection (see clarity criteria below). However, online personal data-processing practices and analytics advance rapidly and require specific expertise that cuts across statistics, computer and system engineering and IT management. National DPAs have often been criticised for their lack of technical and IT forensic expertise, which greatly inhibits their ability to monitor compliance and enforce data protection regulation in the context of online data-processing activities (Kantor, 2010, para. 105).

Reflexive governance connotes a learning process that can complement the governance of data protection in the EU, which is arguably a moving target that requires a constant adjustment of regulatory focus. The expertise needed in the context of reflexive governance requires the definition of policy priorities, exercising discretion and anticipating problems, compromise and consensus-seeking that goes beyond the exercise of top-down authority (Poullet & Guttwirth, 2008, p. 27). WP29 exemplifies some aspects of reflexive governance already when setting priorities in the work programme and selecting problematic issues in the protection of personal data that are followed through (e.g. Google's new privacy policy).

The capacity for reflexive governance of DPAs at the national level varies, with some being less able to effectively set and follow through own priorities and enforcement strategies (European Commission, 2003, pp. 12ff; FRA, 2010, p. 42). Given the ubiquity of data

[12] An initiative of the Council of Europe (see http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day_en.asp).

processing activities, reflexive governance needs to be strengthened and effected at all levels (Poullet & Guttwirth, 2008, p. 27).

5) Efficiency and effectiveness

This criterion tackles whether the legislative mandate has been implemented efficiently in the member states and whether data protection regulation is effective in practice.[13] It does not address the costs of compliance, which are taken up below (see section 3.3.5).

- *Efficient implementation of the legislative mandate*

The implementation of the data protection Directive was reviewed in 2003 and 2007 (European Commission, 2003 and 2007). Both reviews acknowledged progress made with respect to the internal market for personal data, but noted the differences between member states on how the Directive was transposed, applied and enforced. The European Commission could be "more robust in taking action against member states that manifestly do not properly apply the provisions of the directive" (Kantor, 2010, para. 91).

In 2007, the European Commission was satisfied that the Directive ensured a high level of data protection (European Commission, 2007a, p. 9), notwithstanding that most evidence pointed towards deficiencies with compliance and enforcement (see below). Eventually, in 2010 the European Commission concluded that the EU needed a more comprehensive and coherent policy on the fundamental right to personal data protection (European Commission, 2010c), which led to the proposal for a general data protection Regulation in 2012 (European Commission, 2012a).

- *Effectiveness in terms of enforcement and compliance*

A lack of credible and effective enforcement is one of the weaknesses of the data protection Directive. For example, research that used the number of notifications (pursuant to Art. 18 of the Directive) as indicators for assessing the effectiveness of the Directive regularly concluded that data controllers often do not notify DPAs about automated data processing operations (FRA, 2010, p. 29; European Commission, 2012b, p. 133). This criticism is mainly addressed to national DPAs, which do not adequately monitor and enforce data protection compliance (FRA, 2010, p. 29; Kantor, 2010, para. 104; see also European Parliament, 2011, paras 28 and 44). In addition to the shortcomings identified in relation to expertise and accountability, DPAs' watchdog function is particularly obstructed because:

- DPAs are under-resourced, both in terms of staff and financial means (FRA, 2010, p. 8; European Parliament, 2011, para. 28; Rand, 2009, p. 35);

[13] Implementation consists of the practical steps taken by national authorities to give effect to, here, the EU regulatory framework on data protection; compliance consists of the actions undertaken by public and private parties to abide by an EU act; and finally enforcement is the process of ensuring compliance, through monitoring and prosecuting (Nicolaides, 1999, p. 5).

- Member states emphasise 'soft' methods to promote compliance with data protection legislation over 'hard' instruments that would enforce and sanction non-compliance more rigorously (FRA, 2010, p. 8);
- Sanctions are 'mosquito bites' – to quote one of the contributors to the Task Force; in particular the maximum amount of pecuniary fines is insignificant compared to the revenues of large data controllers (FRA, 2010, p. 6); and
- Cross-border cooperation and enforcement action among DPAs is lacking or insufficient (European Commission, 2012b, Annex 10).

Individual legal remedies before courts, albeit in place in all member states, are rarely resorted to (Korff, 2010, p. 98). Possible explanations of this lack of private enforcement action may be:

- Damages to the individual may not occur immediately after the violation of privacy obligations;
- Damages may be difficult to quantify; or
- Individual damages are too small to compensate for the cost of legal action (Rand, 2009, p. 35).

Effective enforcement is even more under strain in the context of online data processing because:

- Probation of violations and damages is more difficult;
- The cross-border extent of data practices is the rule rather than the exception; and
- Cross-border enforcement of legal rights before the court is more cumbersome and costly (European Parliament, 2011, para. 5; Rand, 2009, p. 41).

Consequently, the European Commission's proposal for a general data protection Regulation clarifies enforcement mechanisms, introduces higher sanctions and new consistency mechanisms as well as other means of compliance, such as the appointment of Data Protection Officers (DPOs) by controllers (European Commission, 2012a).

6) Coherence

Since the EU data protection framework pertaining to online personal data processing is a combination of different instruments (i.e. data protection Directive, e-privacy Directive as amended by the data retention Directive) as transposed into 27 member states national laws, overall consistency is known to be a major challenge. EU policy-makers, practitioners and pundits agree that the level of harmonisation achieved in data protection is not sufficient, and that national variations in terms of implementation, interpretation and enforcement considerably hamper the internal market for legitimate personal data processing (see in

particular European Commission, 2012b, p. 11; TrapleKonarskiPodrecki and Partners and European Legal Studies Institute, 2012 p. 42; Kantor, 2010, paras. 45ff.).

One of the central motivations for the EU data protection reform is to establish a uniform general data protection Regulation (European Commission, 2012a and b). The European Parliament (2011) in its resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union agrees that full harmonisation is the way forward while maintaining the level of data protection that the EU data protection Directive of 1995 already provides.

7) Clarity

A regulation which applies horizontally for all types of automated or systematic processing of personal data in the public and the private sector should gear for legal certainty[14] and clarity. By way of analogy, Task Force participants invoked public traffic rules, which would fail its primary objective to organise public traffic and protect all participants in it if the system of rules is too complex. Likewise, data protection regulation is bound to pervade all aspects of public and private organisations' activities vis-à-vis individuals whose personal data are protected subject matter. For its own sake, data protection should embrace simplicity because it is a driver of compliance.

The envisaged Regulation that would bring about one single set of data protection rules in Europe is an important step in the right direction because it consolidates 27 member states' jurisdictions. However, because the new Regulation would be directly effective, the legal document has to engender policy acceptance directly flowing from its text. Conversely, most Task Force participants would concur that the reform proposal is astonishingly complex and, aside from any substantial critique, is capable of being implemented by larger organisations, but may fail to gain recognition by small to medium-sized enterprises (SMEs) and individual data processors. This claim for simplification is not about deregulation: one can have very simple yet strict rules.[15]

8) Flexibility

Ultimately, in order to keep pace with technical and economic developments, EU data protection regulation should maintain the principles of technological and business-model neutrality (Traple Konarski Podrecki and European Legal Studies Institute, 2012; RAND, 2009, p. 24). Although neutrality is a guiding principle of the 1995 Directive, dramatic changes in data processing practices in scale, scope and magnitude rendered modernisation

[14] In the EU judicial system, legal certainty is based on the concept of legal predictability.

[15] Reducing legal complexity would sometimes require a decision whether a rule should be stricter or more relaxed and whether and how to introduce derogations. What matters most is to take the perspective of those who will be applying the regulation in question.

necessary. The Regulation must be capable of internalising pending technological paradigm shifts, such as cloud computing, and be sufficiently flexible to apply to new data-driven business models, e.g. big data.

To sum up the assessment, EU data protection regulation is performing reasonably well against criterion #1 (legitimacy). There is scope for improvement regarding #2 (accountability) with respect to the omnibus role of DPAs, #3 (due process) with respect to participatory processes and #4 (expertise) with respect to DPAs' capacity for reflexive governance, while #6 (coherence) is being taken up in the data protection reform. Major deficiencies show in two criteria, i.e. #5 (efficiency of the regulation) in terms of compliance and enforcement and #7 (clarity), in terms of the normative framework. The regulation appears to internalise criterion #8 (flexibility), but practical applications are lacking, which could be a topic for an EU research and innovation priority.

3.3 Economic analysis of data protection

This section uses the economic analysis of regulation to advance the understanding why data protection as a regulatory regime struggles to deliver.

More specifically, this section offers a *positive* economic analysis of data protection to answer three questions:

- How can personal information be framed in economic terms?
- Why is market behaviour irrational and do consumers value privacy and data protection?
- What are the costs and benefits of data protection regulation?

For reasons set out earlier, this report does not provide a normative economic analysis.

There are a number of caveats: first, most economic research in this area tends to focus on static equilibriums and single transactions, and this may not be conducive to providing a full picture of iterative online data-processing processes (Acquisti, 2010a, p. 5). In other words, economic analysis is much more informed by short-term rather than long-term efficiency. Secondly, it is difficult to properly account for fundamental rights even in a positive economic approach. Moreover, economics can hardly capture second-order effects, such as the right to privacy being an enabler for other democratic institutions and rights.

3.3.1 Economics of information

Some features of personal information that are amplified in online data processing would challenge any regulatory scheme.

Information is often equated with a 'public good', that is, a good that is characterised by two concepts: non-excludability and non-rivalry (Cohen, 2000; Heverly, 2003). The former

concept implies that it is not feasible, for technical or economic reasons, to restrict individuals from consumption. Once information is divulged, the cost to replicate information is negligible, thereby creating a situation close to non-excludability. Non-rivalry implies that an additional consumer does not reduce the utility for the existing consumers. Indeed, information seems, at first sight, also non-rival: if information is shared, the originator is not deprived of that same information. This can generate a market failure, however, contrary to the classic public good dilemma that leads to undersupply: information markets are believed to diminish societal welfare by the excessive creation, disclosure and trade of personal information.

The public good nature of information is not uncontested; the reading of non-rivalry could be more nuanced, in particular.[16]Although information can be shared without the originator being depleted, the value of information, i.e. the utility that an individual can extract from it, can create rivalry. The value of knowing certain classes of information may be affected, positively or negatively, by the number of individuals sharing that knowledge (Renda, 2008). For example, the value of knowing that a specific consumer intends to buy a coffee machine is rivalrous, as its exclusive knowledge confers an advantage to the advertiser or dealer aware of this intention. Information may be subject to the 'tragedy of the commons', that is, to over-consumption (Hardin, 1968).

Either way, information goods are prone to over-consumption, including 'personal information', which is the protected subject matter in data protection regulation. Regulatory intervention can set rules that would govern the collection and use of personal data in an attempt to maximise societal welfare. The underlying problem, however, persists because in the information-rich economy data-processing processes are ubiquitous and rule enforcement is a continuous challenge, as is underlined by the EU experience with data protection, and also with copyright enforcement with the latter being slightly more effective.

3.3.2 Economic theory of privacy

Early Chicago School theorists argued that any regulation that would restrict personal information disclosure creates economic inefficiencies (Stigler, 1980; Posner, 1981). This view is in line with the economic theory that asymmetric information causes market distortions. Until recently, it was argued that the unrestricted sharing of consumer information would increase social welfare (see summary in Acquisti, 2010a, p. 4). Later contributions take a more critical stance in arguing that individuals do benefit from sharing certain information, but full disclosure is not in their best interest (Varian, 1996).

Closer to today's reality of online information processing, widening the focus from a single transaction to the whole set of transactions with many counterparts leads to very different results. In a dynamic multi-transaction setting, consumers are exposed to future potential

[16] For a review of renowned economists on the opposite sides of the debate, see Bates (1988).

misuses of personal information, which may impose random costs (Acquisti, 2004, pp. 5ff). Disclosing personal data would be like signing a blank cheque: it may never come back to the consumer, or it may come back with an arbitrary low or high figure on it (Acquisti, 2010a, p.15).

Disclosing personal information in a certain transaction may result in costs for the data subject unrelated to that transaction. This means that the exchange of personal information is subject to a negative externality. More precisely, companies collecting personal data do not internalise future expected costs borne by individuals (Lessig, 2006, pp. 216ff.). This externality implies that, compared to the societal optimum, individuals may over-disclose information and companies may over-invest in collecting information. Such negative externality, being another source of market failure, may justify public intervention.

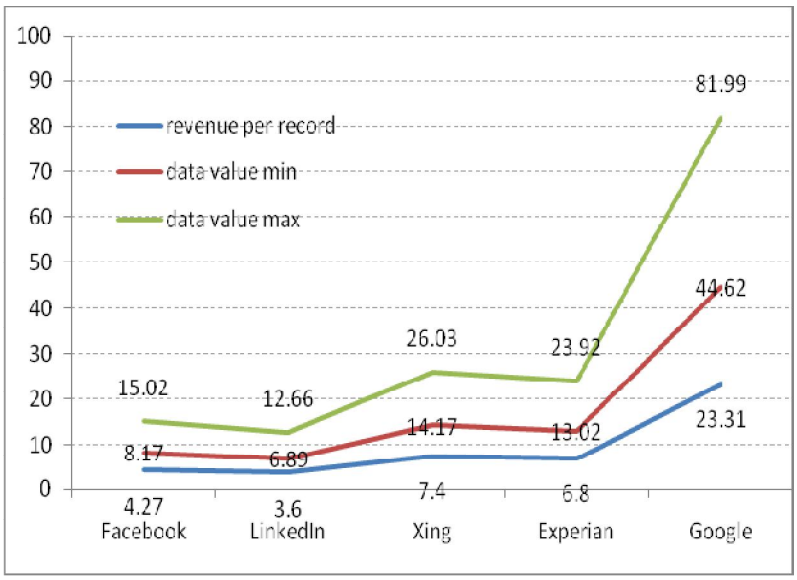
To conclude, economic theory is not monolithic when it comes to the economics of privacy and data protection.

> [D]epending on conditions and assumptions, the protection of personal privacy can increase aggregate welfare as much as the interruption of data flows can decrease it (Acquisti, 2010a, p.19).

3.3.3 The value of personal data

The economic value of personal information for data controllers is measurable, e.g. by looking at their advertising value and revenues. Figure 3 below shows estimated advertising value of personal information for several large internet platforms. Revenues per record vary from company to company, from €3.6 per year for a professional social network up to €23.3 per year for a large consumer-facing search engine and advertising network operator, such as Google. There is no data on what would be the effect if the collection and use of this personal data were more restricted.

Figure 3. Estimated annual advertising value of personal information (€/record)



Note: Y axis: €/year.

Source: Peter Voigt (2012).

Many online services' business models operate as multi-sided platforms, often in an extreme form in which the consumer-facing interface is completely subsidised with revenues from the business-facing interface. Consumers' personal data and attention are thus sought as input for the business model of online advertisers which are channelled through the platform (see Evans, 2013; Luchetta, 2013). The consumer-facing interface is free of charge to maximise participation.

Multi-sided markets

The concept of multi-sided markets or platforms, developed by Rochet & Tirole (2003), are characterised by three elements:

- Two or more groups of customers who are simultaneously served by the platform through distinct interfaces;
- The value that customers realise through their platform interface increases with the number of customers on another platform interface (so-called 'indirect externalities'); and
- The volume of transactions can be affected by charging more to customers at one interface and reducing the price paid by the customers at the other interface (a form of cross-subsidisation).

Consumer valuation of personal information is commonly measured according to people's willingness to pay for privacy or accept rewards in exchange for their data. Although there are

evidently markets for personal information, especially in the online economy, what can often be observed is that individuals apparently do not participate.[17] This is why research largely draws from economic experiments. Interpretations of research data about individuals' willingness to pay for privacy or accept rewards in exchange for their data draw a highly complex picture.

3.3.4 Behavioural economics and privacy

According to behavioural economics, when individuals are confronted with the challenges posed by disclosing and managing personal information, their choice is more often than not irrational. Research points to inconsistencies in individual decision-making:

- A vast majority of individuals are concerned about loss of control over personal information, but they would disclose personal information for very small, even nihil, rewards (see Berendt et al., 2005; Compañó & Lusoli, 2010; BCG, 2012, p.13).
- Privacy behaviour depends on the context and is easily influenced by framework conditions, the order in which choices are presented to the consumer and the default state (see Acquisti, 2004; Acquisti & Grossklags, 2004; Acquisti & Gross, 2006; Acquisti et al., 2009).
- "The 'price' people assign to protect a piece of information is very different from the price they assign to sell the same piece of information." (Acquisti et al., 2009, p. 31). According to this 'endowment effect' in personal information selling, personal data are valued higher than buying privacy protection (Acquisti et al., 2009, p.31).
- Where consumers are given more control, they tend to volunteer more, even sensitive personal information and allow more uses and disclosure (Brandimarte et al., 2010, pp. 3ff; BCG, 2012, p. 15).
- Often individuals do not differentiate between privacy and the value of personal information, but if made aware they value their personal information more (Spiekermann et al., 2012).

Social networks are a very good experimental test bed to study privacy decision-making (see box below).

[17] There are many different reasons, but it seems that individuals are sometimes not aware of data processing activities (BCG, 2012, p. 12), or ignorant about privacy policies and unlikely future risks, or their personal information is tied to another transaction or 'pays' for a gratuitous online service they desire ('Take-it-or-leave-it').

Research on social network sites and privacy

- While privacy attitudes matter in the decision whether to join Facebook or not (but only for the age cohorts and social groups for which Facebook is not a 'must-have' platform), the amount of information actually disclosed by Facebook users does not correlate with their privacy preferences (Acquisti & Gross, 2006).
- Social networks' different privacy policies make hardly any difference in terms of user behaviours (Bonneau & Preisbuch, 2010).
- Independent from their degree of privacy concern, users are willing to pay to prevent deletion or sale of personal information included in Facebook profiles (Spiekermann et al., 2012).

Where consumers are given the choice, both surveys and experiments confirm that a fair share of consumers value privacy and control:

- A significant share of individuals is willing to pay a small premium for more privacy controls in online services if choice is part of the transaction (Krasnova et al., 2009).
- Without price competition, the majority of consumers select a privacy-friendly offer; with price competition, a non-negligible proportion is still willing to pay a small mark-up for privacy (Beresford et al., 2012; ENISA, 2012a, p. 1).

However, both examples presuppose a highly transparent choice and a very reasonable privacy mark-up, in other words what would be a market for privacy.[18]

More recent research suggests that the economics of privacy and personal information may be distinct because the former is about the value of keeping information undisclosed, whereas the latter "relates to all information people share" (Spiekermann et al., 2012, p. 3). As stated initially, individuals are not generally inhibited from sharing personal data but want to be assured that it flows appropriately (Nissenbaum, 2010, p. 2; BCG, 2012, p. 42). There are indisputable benefits for individuals from online data-processing activities, such as personalised services and relevant advertising, but such benefits are context-sensitive too.

There are a number of reasons why these behavioural biases are large and relevant for data protection policies:

- Privacy policies (or fair information practices) are important transparency mechanisms, but are not likely to be decisive in determining user behaviour. Simplification and

[18] When juxtaposing the value some consumers attach to privacy (ENISA, 2012, p. 36) with the average advertising revenues per record (Figure 3), companies could differentiate their services and charge a small monthly for the private version of their online services.

standardisation of privacy terms are to be welcomed, but biases do not depend on limited information.

- In online transactions, product or service attributes are salient to consumers, but privacy attributes are not.[19] This means that frequently consumers will not weigh up the costs of data disclosure and will not select a privacy-savvy offer in a competitive market (except under experimental condition with perfect information).
- Consumers' disclosure and privacy behaviour concerning their personal information is 'malleable', which can be easily exploited to obtain more personal information and generate consent to its processing.
- Only if privacy choices are embedded in a given transaction and effectuated by rules and orders surrounding the sign-up are consumers likely to align with their privacy preferences. Hence, opt-in and opt-out rules as well as default settings have strong impacts on the level of data disclosure.

Acquisti (2010a, p. 6) concludes that "the market equilibrium will tend *not* to afford privacy protection to individuals". This can be a ground for regulatory intervention aiming for privacy. Strategies discussed in the literature are reversing dynamics in online transactions (through a combination of managing the default-setting, consent as opt-in and separation principle) and introducing markets for privacy (OECD, 2011, p.28).

- **Role of defaults**

Defaults that favour privacy or not, and would hence require an overriding action by users, make a difference; a point raised by many Task Force contributors. The significance of defaults can be witnessed in the discussions over the ongoing data protection reform and other significant developments, such as the 'Do-Not-Track' (DNT) browser settings (see box in section 4.2.3). Policy-makers should be vigilant about explicit or implicit defaults in standardisation, regulation and private policies.

- **Consent and the opt-in/ opt-out debate**

In a similar fashion, the consent of individuals is often the prerequisite for the legitimate processing of personal information. In online transactions, obtaining data subjects' consent is sensitive to how it is declared: as an opt-in where an active action is required or as an opt-out where the given consent is a default and the user would need to change it. Already under the present EU data protection Directive, simple inaction is deemed insufficient to constitute valid consent (Kosta, 2013; WP29, 2011, p. 12).

[19] A product attribute is salient when it is relevant to a consumer's choice (see Korobkin, 2003). In each transaction, only a few attributes are 'processed' by the consumer. Firms can therefore explore non-salient attributes in their favour. For example, it is claimed that legal warranties are not salient, and therefore firms will always draft warranties in their favour. In a nutshell, there is no competition on non-salient attributes. See also ENISA, 2012.

- **Separation principle**

The separation principle, as it is known, would unbundle an online service from secondary data processing (such as marketing unrelated to the customer relationship, profiling or the transfer of personal data to third parties) and ultimately reinforces how 'free' the consent is (no 'take-it-or-leave-it' transactions; see BCG, 2012, p. 111). A strict separation principle would mandate the provider to offer two transactions on separate terms (ENISA, 2012, p. 3; Novotny & Spiekermann, 2012, p.5).[20] As a follow-up problem, the question will arise how to determine a fair premium for more privacy vis-à-vis the provider, which may ultimately call for regulatory intervention.

- **Markets for privacy**

Promoting markets for privacy could be a promising strategy to help privacy attributes to become more salient in competition. If trust was truly to become a key market differentiator, as Task Force participants proposed, then companies' reputation and privacy-savvy offers should face competition. There are a few additional measures that help improve privacy to become a more salient attribute for competition. First, certification and public trust marks or seals can signal adherence to high privacy standards. Second, in some markets, such as social networks, data portability may significantly lower switching costs for users (Costa & Poullet, 2012, p. 257; European Commission, 2010c, pp. 7ff).[21]

3.3.5 Costs and benefits of data protection law

Understanding the costs and benefits of data protection regulation can inform public policy and help better calibrate regulation. The data available are still very fragmented and far from complete, but allow a glimpse into the problem.

Quantifying the costs and benefits of data protection regulation for individuals and data controllers has not yet been accomplished. From the perspective of data controllers, certain costs of data protection measures are known, but aggregate costs are still unspecified (European Commission, 2012b, Annex 10; Ponemon Institute, 2011). Moreover, determining which costs can be attributed to regulation and which costs a company would bear out of other considerations (such as brand reputation) is difficult to establish. Where they occur and are made public, privacy breaches can have a significant impact on public trust in the company concerned, which can affect other profit-generating operations.

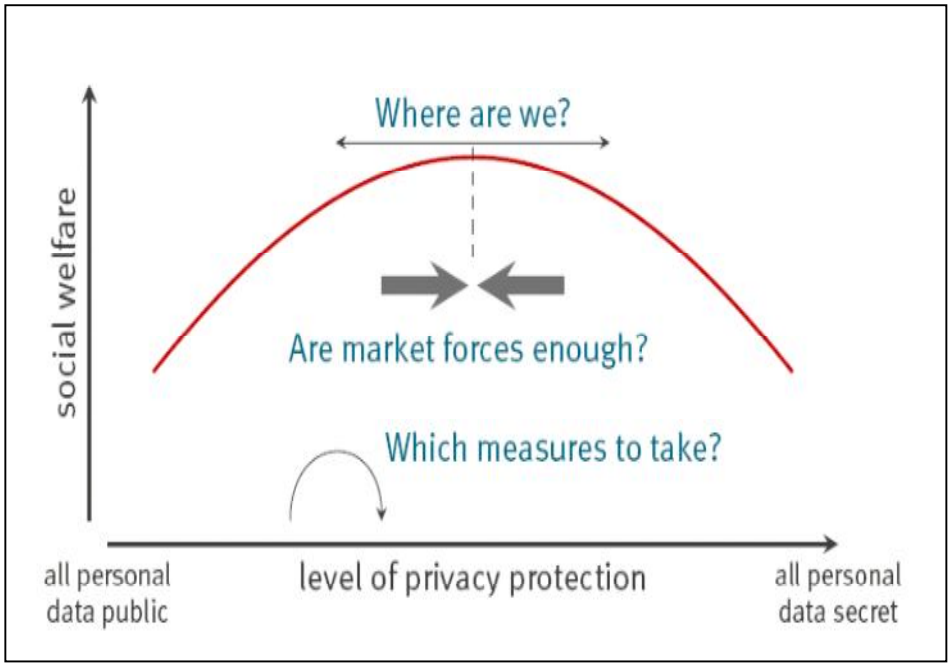
[20] It should be noted that for a number of online services that are offered for business and retail customers this type of versioning is already practised, e.g. Google apps for business. For various reasons, e.g. confidentiality and legal obligations, business customers tend not to tolerate the processing of (personal) data for secondary purposes.

[21] NB: the similarity to number portability in electronic communications in Art. 30 of the universal service Directive (Directive 2002/22/EC).

The costs and benefits of data protection regulation for consumers receive little attention, also because normative arguments are commonly resorted to. Possible costs for consumers are often framed as identify theft and related abuse of personal data, but also foregone opportunities and monetary disadvantages should be taken into account, above all ethical implications. According to a US example, opportunity costs of reading online privacy policies would amount, in the US alone, to $781 billion per year (McDonald & Cranor, 2008, p. 561). Hence, consumers are also burdened and regulation can alleviate their need to micro-manage privacy preferences.

To sum up, state-of-the-art cost-benefit analysis only confirms that making all data public is welfare-diminishing, and so is full privacy. From an economic point of view, data protection regulation has to reconcile the protection and the flow of personal information. In principle, there is an optimal level of data protection regulation, but, given the state of the art, it is not possible to locate it with any degree of precision. There is no indication whatsoever if the existing legal framework is on the right or the left of the optimum, that is, whether more or less privacy would be beneficial.

Figure 4. The optimal amount of privacy regulation



Source: Boehme (2012).

Future research should be directed at understanding whether the benefits of data protection regulation are truly translating in practice. According to cost-benefit analysis, benefits are maximised when the difference between societal benefits and the cost of privacy precautions is the largest. If enforcement is lower than optimal (up to the case of no enforcement), a rational actor will choose a lower level of privacy, where the difference between the

controller's *private* benefits and the costs of precaution are maximised. At the same time, societal welfare would not be maximised if it is not clear how to meet regulatory requirements. Depending on the perceived risk of sanctions, a company may either play it safe, therefore taking more precautions than optimal from a welfare economic point of view, or play it boldly, also creating a welfare loss due to lower privacy benefits.

4. Old paradigms and new approaches to data protection regulation

This section deconstructs the conceptual approach behind EU data protection regulation in order to identify systematic shortcomings before discussing possible avenues for modernisation from different angles.

4.1 Deconstructing the conceptual approach behind EU data protection regulation

The EU data protection framework rests on a so-called *a priori* and horizontal regulatory approach. *A priori* regulation means that prior formalities must be complied with in order for data processing activities to be lawful (see RAND, 2009, p. 20). As a horizontal instrument, data protection Regulation applies across all sectors' automated or otherwise systematic data-processing activities (see European Commission, 2012b, p. 148). It appears that the new fundamental right to data protection in the CFR endorses this approach (see also section 2.1.2).

In this section, the discussion takes up a number of core data protection concepts and contemporary challenges they are facing. In the discussion about the reform proposals these core concepts have turned out to be highly politicised, despite the fact that they are already part of the EU data protection *acquis*. Therefore the following discussion about the conceptual approach behind EU data protection regulation is timely.

4.1.1 Personal data and special categories of personal data

'Personal data' is an important concept because it essentially determines the subject-matter scope of data protection regulation, therefore triggering the application of the obligations incumbent upon data controllers and processors (European Commission, 2010c, p. 8; RAND, 2009, p. 26). According to the definition in the data protection Directive, personal data consist of "any information relating to an identified or identifiable person" (Art. 2(a)). It is interpreted to comprise all direct and indirect ways to single out an individual (European Commission, 2012c, p. 8; WP29, 2007; 2013, p. 1).

Because of their sensitive nature, special categories of personal data receive a higher level of protection. The data protection Directive defines as special categories data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and health or sex life (Art. 8(1)). The rationale for the special protection is the associated higher risks in processing such information, which is relatively uncontested.

Any data that do not relate to an individual or, although constituting personal data, has been "rendered anonymous in such a way that the data subject is no longer identifiable" (data protection Directive, Rec. 26) are not considered personal data.

Criticism focuses on several points:

- The concept of personal data does not differentiate between different categories corresponding to different sensitivities or risks ('one-size-fits-all') (BCG, 2012, p. 14; RAND, 2009, p. 26).
- The higher protection for special categories of personal data is arbitrary in that it does not include other, possibly equally sensitive categories.
- There are differences of opinion about whether online identifiers are or should be considered personal data (pro: WP29, 2007, p. 14; 2013, p. 1; cautious: RAND, 2009, p. 27) and
- Concerning the retracting boundaries of the anonymity frontier, there are questions whether data protection *s*hould subsist up to defined levels of relative anonymity (BCG, 2012, p. 36; Ohm, 2010).

Each point of contention is considered below in more detail.

- Personal data as a one-size-fits-all concept

The advantage of a one-size-fits-all approach to personal data is that it is flexible to apply in different situations and circumstances, underpinning the horizontal approach of the regulation. The criticism favours a more granular understanding of personal data categories according to associated sensitivities or risks (BCG, 2012, p. 14; RAND, 2009, p. 26). The critique does not stick because a differentiated treatment does not allow for the exclusion of any personal data under the subject-matter scope of application of the regulation.

- Special categories of personal data are arbitrary

The existing catalogue of specially-protected categories of personal data is rarely contested for its content, but rather for its arbitrariness, for example:

- Individuals in most European countries tend to consider financial information as highly sensitive (see BCG, 2012, p. 43; RAND, 2009, p. 26), but under data protection Regulation it is not.
- The e-privacy Directive introduces special protection for traffic and location data that exceeds that provided by the data protection Directive for non-sensitive personal data (even if they are not considered a special category of personal data).
- Processing biometric information may involve similar risks as the processing of genetic data, but the proposal for a new general data protection Regulation integrates only the latter in the catalogue of special categories of personal data (European Commission, 2012a, Art. 9(1)).
- Also, a comprehensive digital identity (see box below) is not especially protected, although longitudinal and combined data sets can be very revealing about individual circumstances.

Digital identity

"A digital identity is the sum of all digitally available data about an individual" (BCG, 2012, p. 35).

Inherent characteristics. Where does an individual come from and who is she or he? Date of birth, gender and nationality are examples of this type of information.

Acquired characteristics. What is an individual's story? His/her history? Here, information such as address, medical record, social capital (*added by the authors*) and purchases history are relevant.

Individual preferences. What does an individual like? Data types here would include interests, hobbies and favourite music (a*mended by the authors*).

Source: BCG (2012, p. 36), with some amendments.

- Personal data and online identifiers

Whether online identifiers are considered as personal data has far-reaching implications for the scope of data protection Regulation. The increasing reliance on online identifiers, especially on the internet (such as IP addresses, cookies, location data, and browser fingerprinting) would trigger the application of data protection Regulation. The WP29 underlines that for identifiability it suffices if an individual can be singled out (WP29, 2007, p. 14; 2013, p. 1). This interpretation is contested, however, not the least by online companies.

The proposal for a general data protection Regulation lists online identifiers expressly in the definition of data subjects but also maintains that not all online identifiers need "necessarily be considered as personal data in all circumstances" (Recital 24). These contradictory references to online identifiers, which the reform proposal sets out to improve, must be resolved (Traple Konarski Podrecki and Partners and European Legal Studies Institute, 2012, p. 25).

When taking this decision, it is important to bear in mind the close relationship between online identifiers and 'pseudonymisation', as well as the regulatory objective to harness the use of privacy-enhancing technologies (hereinafter, PETs, see section 5.2.2). Because online identifiers could also be perceived as "retraceably pseudonymised data" (WP29, 2007, p.18), any solution has to be internally consistent. Besides, the use of PETs would hardly be encouraged if online identifiers did not fall under the scope of data protection regulation.[22]

[22] See section 6.3.3 concerning the lack of positive regulatory incentives.

Today's data protection Directive (Recital 26) and the reform proposals aim to decide on the legal nature of an online identifier by taking into account "all the means likely reasonably to be used either by the controller or by any other person to identify the said person". Identification thus does not require the person to be named or correlated to an official identifier, such as ID numbers, addresses, etc. Second best to the WP29's interpretation of 'singling out' is the proposal to take the intention of the controller and processor into account (in quoting the UK ICO 2012[23] and also Traple Konarski Podrecki and Partners and European Legal Studies Institute, 2012, p. 48). In both cases, processing information in connection with online identifiers is going to be regarded as personal data – a regulatory decision that is appropriate in most situations.

- The anonymity frontier

Neither anonymous nor anonymised data fall under the scope of data protection regulation because anonymous data does not relate to an individual; while anonymised data becomes anonymous because the individual is no longer identifiable (WP29, 2007, p. 21; 2012, p. 1). The challenge is establishing if digital data are (still) anonymous because technical and methodological advancements continue to push back the anonymity frontier (see, generally, Ohm, 2010). Anonymity is an important concept because it is one of the best (technical) strategies to privacy and data protection.

In principle, many purposes for which data processing is deployed can be achieved by using anonymous data, e.g. audience measuring tools could rely on collecting aggregate data of page views[24] (WP29, 2012, p.10). This should create a strong incentive to use anonymised data whenever possible, but controllers can face a trade-off between privacy and utility (BCG, 2012, p.16). Although techniques that are more efficient in this trade-off, i.e. sacrifice less utility for more privacy, have been developed, anonymisation necessarily implies a loss of information. Research disagrees on the utility of anonymised datasets (sufficient according to: Aggarwal & Yu, 2008, p. 25; Novotny & Spiekermann, 2012, p. 11; insufficient: Ohm, 2010, pp. 1753ff), but this can hardly be generalised as it depends on the context and purpose of the data processing in question.

With the concept of real anonymity becoming increasingly contested, EU data protection regulation already supports a relative notion according to which "account should be taken of all the means likely reasonably to be used to identify an individual" (data protection Directive, Recital 26). This would require a better definition of anonymous data[25] and

[23] As proposed by the UK ICO (2012, p. 5): "Where IP addresses or similar identifiers are processed with the intention of targeting particular content at an individual, or otherwise treating one person differently from another, then the identifier will be personal data and, as far as is possible, the rules of data protection will apply."

[24] After a cookie has been installed on the end-user terminal, for details see WP29, 2012, p.10).

[25] As foreseen in the draft report of the LIBE Committee, European Parliament, by Albrecht (2012): "This Regulation should not apply to anonymous data, meaning any data that cannot be related, directly or indirectly, alone or in combination with associated data, to a natural person or where establishing such a relation would require a disproportionate amount of time, expense, and effort, taking into account the state of the art in

possibly a technical implementation guidance clarifying a threshold, in terms of statistical probability of re-identification, under which a dataset can be considered sufficiently anonymous. This should be flanked with a prohibition to intentionally break the anonymity barrier, which would also trigger obligations incumbent on data controllers.

4.1.2 Principles relating to data quality

The data protection Directive formulates five broad principles relating to data quality (Art. 6(1); see box in section 2.2.1): In short, there are 1) fairness and lawfulness, 2) purpose specification, 3) collection limitation, 4) data quality and 5) use limitation.[26] Collection limitation and use limitation are also combined in the principle of data minimisation. The principles' combined purpose is to narrowly frame the processing of personal data. It is a perceived strength of the principles-based framework that it permits flexibility (RAND, 2009, p. 24) while at the same time operationalising at a high level the correct input of personal data in relation to a given processing activity (or purpose) and how data should be treated.

It would appear, however, that a few of these principles are increasingly contested by economic developments and social practices. Most obviously data minimisation seems at odds with an information-rich society (see e.g. Novotny & Spiekermann, 2012, p. 3). Under the current rules "[c]ollecting data because they might prove useful in the future would be in breach of both the purpose limitation principle and the data minimisation principle" (Van der Sloot & Borgesius, 2012, p. 92). However, this is exactly what many companies are doing and hoping to exploit in the near future (De Hert & Papakonstantinou, 2012, p.135). This perception was shared by many Task Force participants who call for more flexibility when it comes to potential uses of personal data held by these companies.

Conversely, it can be argued that:

> Data minimisation, i.e. processing and storing only those personal data that are necessary for a legitimate purpose, is becoming more and more important when technical limitations to storage, processing and transfer capacity are quickly disappearing, and when at the same time security risks and data breaches are becoming more prevalent (European Commission, 2012b, p. 96).

Data minimisation should remain a central descriptor of data quality, not least because it is backed by good practices from information assurance, management and security. Overall, one Task Force contributor maintains that the principles governing data quality have been very

technology at the time of the processing and the possibilities for development during the period for which the data will be processed."

[26] These principles build conceptually on two international standard-setting instruments: the non-binding 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Council of Europe's (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data from 1981.

successful as a defining concept for the protection of personal data because they are still the most intuitive element of this regulation.

4.1.3 Roles and responsibilities

Data protection regulation rests to a large extent on the definition of roles to which obligations and accountability are attached. Central roles are data controllers and data processors. The present data protection Directive defines, on the one hand, the controller as those persons or bodies, public or private, "which alone or jointly with others determine the purposes and means of the processing of personal data" (Art. 2(d)). The processor, on the other hand, is any other body "which processes personal data on behalf of the controller" (Art. 2(e)). Controllers must be accountable for complying with the regulation on personal data protection, whereas processors are not.

In light of distributed data processing practices and data-sharing arrangements, this conception meets with a number of challenges and criticisms:

- In the case of joint controllers, how to ensure a line of accountability that is adequate to the shared control over personal data?
- With respect to determining the means of processing, can the present delineation between controller and processor still be maintained given that processors are gaining increasing control over the means (RAND, 2009, p.36; Traple Konarski Podrecki and Partners and European Legal Studies Institute, 2012, p.9)?
- Do consumers and end-users become controllers in cloud computing?

- Joint controllers

The present data protection regulation acknowledges that joint control can exist in the definition of controllers, but it does not clarify how the arrangement may distribute responsibilities among them. As it stands, each of them carries full responsibility. In its draft for a general data protection Regulation the European Commission proposes a shared responsibility that, however, carries the risk of obscuring overall accountability (European Commission, 2012a, Art. 24). To ensure unified accountability over the process, it would be preferable to designate a lead controller according to the relative weight in determining the purpose, condition and means of data processing. The other controllers would remain responsible for compliance with regulatory obligations according to their particular contributions as assigned to them by the lead controller.

- Relationship between controllers and processors

Distributed personal data processing has also reshuffled the relationship between data controller and processor. The chains of delegation are getting longer with more sub-processors becoming involved, but processors are also increasingly independent in carrying

out the tasks assigned to them by the data controller. Under the present regulation, it is unclear to the participating stakeholders "when a processor becomes a controller or vice versa" (RAND, 2009, p.36).[27]

Cloud computing

Cloud computing is a major paradigm shift in networked computing. Digital data resides and computing is performed on powerful computing platforms ('the cloud'), which can be accessed remotely.[28]

Business customers of cloud services benefit from lower prices, minimal upfront IT investments and scalable as well as customisable services.[29] Consumers' end-user terminals are about to become 'thin clients' that rely on cloud services for access to software, computing and storage.

The relationship between a customer of cloud services, whether a business client or a consumer, and the provider can be difficult to fit into roles defined under data protection regulation, i.e. controller and processor (Hon et al., 2011, pp.11-22). Depending on the context, this relationship can be heavily intertwined and dynamic where data protection regulation presumes a controller's determination of the purposes, conditions and means of the processing of personal data.

Whenever the cloud service provider uses its clients' personal data for its own purposes, it would qualify as a controller fully liable to data protection compliance.

The solution of extending more leniency to processors in deciding about the means of data processing has been put forward (Traple Konarski Podrecki and Partners and European Legal Studies Institute, 2012, p.9) and is also supported by some Task Force participants. Although this solution may resolve some confusion about roles, it can create gaps in the process-oriented accountability. In fact, the means of data processing carries a stand-alone risk for the protection of personal data; important procedural aspects and decisions are deployed, such as algorithms. Regulation should therefore not be blind to the means even if this aspect of data processing is no longer under the exclusive control of the controller. Here, parallel to reducing

[27] In addressing the problem, the draft proposal for a general data protection Regulation provides: "If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing […]" (Art. 26(4)).

[28] According to the definition of the US National Institute for Standards and Technology, cloud computing is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (NIST, 2011).

[29] For a full taxonomy of cloud services, see NIST (2011).

the level of responsibility on the part of the controller, accountability on the part of the processor would need to be stepped up. Other regulatory strategies may also be affected when surgically removing the means of data processing from the responsibility of the controller. For example, privacy by design may fall between what the regulatory responsibilities of controllers and processors (Traple Konarski Podrecki and Partners and European Legal Studies Institute, 2012, p.32).

- Are consumers really controllers?

Another paradoxical result would be one in which consumers are legally the controllers of their personal data that reside in the cloud without the possibility to exercise control. As it is common in end-user markets, the underlying contractual relationship is based on a contract of adhesion that predefines the terms and conditions of service. In this case, the consumer as controller cannot impose much control on the processor, which somewhat contradicts the conceptual approach in data protection where the processor is an 'auxiliary' of the controller. There should be a rule under the scope of data protection regulation that prohibits individuals from acting as the controller of their own personal information if the information resides in third-party equipment.

4.1.4 Informed consent and control

Individuals' control exercised through consent is an important concept in the fundamental rights approach to data protection (WP29, 2011, p.8). Consent, as defined in the data protection Directive, is "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Art. 2(h)). At the time of collecting personal data, controllers have to provide a minimum set of information (Art. 10), which also allows the consent to be 'informed'. Out of six alternative legal grounds, the individual's consent has emerged as the most significant basis for legitimate personal data processing by far (Art. 7(a)). Task Force participants confirmed the prominent role of consent in facilitating personal data processing.

The regulation's ideal notion of consent does not always translate into practice and certain points of criticism are frequently raised:

- The link between the information about data processing and consent is weak (Acquisti, 2010b, p. 19; RAND, 2009, p.44).
- The capacity to consent does not often give effective control to users and individuals about the use of their personal data (Acquisti, 2010a; 2010b, p.19).
- A definition of consent should be more flexible to allow different types of consent that fit the context and type of data at issue (BCG, 2012, p. 15; WEF, 2012, p. 24).

Different stakeholders have different issues with the consent requirement, which explains certain tensions between calls to lower the threshold for obtaining valid consent and calls that

aim to strengthen individuals' consent. The reason why informed consent has not delivered (yet) can be explained in a number of ways, notably by economics (see section 3.3) and a tendency to generate consent instead of extending controls to users and individuals. Some Task Force participants believe that increasing the formal requirements for obtaining valid consent may result in a shift towards more subscription-based online services, and that larger online service providers are in a more advantageous position than smaller ones.

Despite these shortcomings, consent as a legal basis for data processing is necessary because it remains the best lynchpin for quasi-market mechanisms in personal data transactions. Consequently, the draft proposal for a general data protection Regulation ramps up the formal conditions for consent (Art. 7) and stresses the need for "a genuine and free choice" (Recital 32). The draft proposal carries an embryonic 'separation principle' (Recital 25), but a more straightforward rule should be included in the Regulation. The burden of proof showing that the data subject consented to the processing of their personal data would be unequivocally placed on the controllers (Art. 7(1)).

To conclude this section, with some fine-tuning the basic conceptual approach to data protection regulation is fit to carry the regulatory treatment of personal data processing into the future. The horizontal and technologically neutral approach needs to be preserved; data quality principles remain an essential conceptual framework; individuals' consent should be improved but caution may be needed when adjusting roles of controllers and processors. The regulatory approach very much underpins what a number of studies recommend as a thorough change of culture towards privacy as a virtue or a new paradigm for digital identity (BCG, 2012; WEF, 2012).

Towards a new paradigm for digital identity

"To unlock the full value, organisations need to make the benefits of digital identity applications very clear to consumers. […]

As we show in this report, three elements are essential to ensure a sustainable flow of data:

First, the benefit a consumer receives has to exceed the 'cost' of sharing the data.

Second, there needs to be transparency in how the data are used. While this might initially reduce sharing, it limits the risk of brand damage and helps to attract more informed customers.

Third, privacy controls should be available and easy to use. They will significantly increase data-sharing by individuals, likely offsetting any negative impact on sharing resulting from increased transparency."

Source: BCG (2012, p. 17).

4.2 Compliance, risks and management

Instead of changing the basic conceptual approach, modernising data protection should focus on enhancing compliance, balancing risks and improving the management of data protection. A necessary ingredient is more legal clarity, because data-protection regulation is often implicit when it should be direct.

4.2.1 Tensions between regulation and compliance

In order for regulation to achieve its objective, addressees must be motivated to comply and that compliance must not 'outsmart' the regulation. Presently, there is a paradoxical situation: practitioners, policy-makers and pundits concur that compliance is rather low and many controllers ignore data-protection regulation in part or entirely (see, for example, the SME survey, European Commission, 2012b, Annex 8; Kuner, 2012b). Conversely, there are very responsible companies that invest in compliance management relating to data-protection regulation that should make a difference to the privacy and data protection of individuals and users. But this too is not always a certain outcome.

Complex and composite online transactions that involve a good or service and personal information as *by-product* prevail (ENISA, 2012a, p. 9). Consumer-facing businesses collect personal data in the course of a legitimate transaction, i.e. the primary purpose being the performance of a contract (data protection Directive, Art. 7 (b)). In order to facilitate the data processing for additional purposes, the original transaction has to help generate individuals' consent (data protection Directive, Art. 7 (a)). This is when the objective to generate valid consents may take priority for many businesses over offering their customers true choice concerning the processing of their personal data for other, unrelated purposes (see Laudon, 1996, p.99).

Task Force participants were concerned about their ability to obtain consent, and stressed the economic repercussions that would occur if data protection regulation were to firmly require opt-in and introduce a separation principle, as explained in section 3.3.5. However, it should not be forgotten that the present regulatory regime eases the processing of personal data in preparing or carrying out a contract.

As it stands, data-protection regulation could be applied in such a way that systematically undermines its very aim, that is, to protect the fundamental right to privacy with respect to the processing of personal data (data protection Directive, Art. 1(1)). Flexibility is needed where it can aid innovation, business models but also users and consumers to manage their privacy preferences. However, it should not be possible to invoke flexibility against the spirit of the regulation.

4.2.2 Implicit regulation

Implicit regulation is an important issue in that it contributes to regulations not being sufficiently accessible to inexperienced practitioners. Even though the regulation is internally consistent, some major applications are not directly addressed. The following examples, which illustrate the problem, are discussed below.

- The purpose for which personal data are processed
- 'Legitimate interest' of the data controller
- Data transfers to third parties

- The purpose for which personal data are processed

The purpose for which data are processed is a central notion in data-protection regulation, but it is not defined.[30] The data controller determines the purpose alone or jointly with others (data protection Directive, Art. 2(d)), whereas the legitimate basis for personal data processing is defined in relation to each purpose. When the first-generation EU data protection framework was issued, automated data processing was characterised by filing systems and computer mainframes (RAND, 2009, p.7). Contemporary data processing is more integrated, interconnected and diffuse, thereby challenging any understanding along discrete lines of processing operations.

In terms of general administrative burden, it matters if purpose is defined more inclusively. It is to be welcomed that, according to the draft proposal for a general data protection Regulation, consent "should cover all processing activities carried out for the same purpose." (European Commission, 2012a, Recital 25) For example, the purpose of marketing is very broad, which potentially covers all types of marketing, such as direct marketing and targeted advertisements. Because online behavioural advertising relies on tracking individuals' preference online as a self-standing input, the entire practice cannot be generally subsumed under the purpose of marketing, which is commercial communication (see box).

[30] The data protection Directive uses the notion in two different connotations: firstly in a more general sense to describe sectoral data processing activities such as "purposes of journalism or for purposes of literary of artistic expression", and, second, in a more granular fashion for each discrete line of processing operation.

Online behavioural advertisement

Online behavioural advertising is a combination of online tracking and targeted advertisement.[31]

Internet users' browsing history and other preferences are tracked to create preference-based profiles, and correspondingly targeted advertising is displayed to users.

On the one hand, as a particular practice online behavioural advertisement can help making advertising more relevant for users, and as a marketing technique it is deemed more efficient compared to other advertising methods online (e.g. Beales, 2010).

One the other hand, the 2011 Eurobarometer survey showed that four out of ten Europeans are concerned about their online behaviour being recorded and in just below half of the EU member states the majority of users surveyed are concerned about profiling on the internet (European Commission, 2011, p. 67).

Where online behavioural advertising is facilitated by installing a tracking cookie, prior informed consent of the individual user is required under the e-privacy Directive (Art. 5(c)) (WP29, 2010a).

In Europe, industry associations[32] adopted best practice recommendations on behavioural advertising and set up a website for users to opt-out.[33] Nonetheless, this best practice recommendation was not approved by the responsible EU body because it does "not result in compliance with the current e-privacy Directive" (WP29, 2011, p.12).

When discussing personal data processing it is useful to distinguish between *primary* and *secondary* purposes.[34] Pronouncing the difference between *primary* and *secondary* purposes can greatly enhance the clarity of the regulatory logic. On the one hand, the *primary* purpose often concerns a processing necessary for the performance of a contract. The *secondary* purpose, on the other hand, connotes the use of personal information for a different and unrelated purpose that would need a separate legal ground for legitimate data processing (data protection Directive, Art. 7).

[31] As a 2012 ENISA study puts it: "Much of the debate today focuses on [online behavioural advertising] instead of tracking. […] Tracking is the problem – not behavioural advertising" (ENISA, 2012c, p. 20).

[32] i.e., the European Advertising Standard Alliance and the Internet Advertising Bureau Europe.

[33] See (www.youronlinechoices.eu).

[34] This separation is implicit in data protection regulation (Korff, 2010, FN 114) when it provides that personal data must be "collected for specified, explicit and legitimate purposes (i.e. *primary purpose*, authors' addition) and not further processed (for *secondary purposes*, authors' addition) in a way incompatible with those purposes" (data protection Directive, Art. 6(1)(b).

- 'Legitimate interest' of the data controller

The 'legitimate interest' of the data controller can render the processing of personal data legitimate if certain conditions are met (data protection Directive, Art. 7 (f)). The 'legitimate interest' test involves a balancing exercise between the legitimate interest of the data controller and the interests for fundamental rights and freedoms of the data subject. Although inherently flexible, this legal ground is very vague and "thus the one perhaps most in need of clarification as to how it can and should be applied in specific contexts" (Kantor, 2010, p.32; see also Traple Konarski Podrecki and Partners and European Legal Studies Institute, 2012, p.10).

Task Force participants, for example, prefer not to rely on 'legitimate interest' for data processing as it is today, but see a lot of potential if the new General Data Protection Regulation would better operationalise the 'legitimate interest' test. Clear boundaries would be helpful to delineate what data processing purposes can be performed under this flexible clause.

- Data transfers to third parties

In data protection regulation, which also aims at establishing an internal market for personal data, the disclosure, sharing and transfer of personal data is generally acknowledged. Strictly speaking, when the *first* controller discloses personal data to one or several third parties, this constitutes a distinct processing purpose.[35] The recipient who (is not an auxiliary processor) but intends to process personal data for own and unrelated purposes becomes the *second* controller and would need legitimate grounds. The regulatory requirements for lawful data processing become very difficult to adhere to for any further instances of disclosure to third parties.

The above is to illustrate that certain practical questions are not addressed in the legal framework as they should be. Data transfers to third parties are increasingly inherent in online personal data processing and the law has to afford clarity about what practices are in compliance with data protection regulation.

4.2.3 Timing and scalability

This final point highlights the importance of timing and scalability of regulatory intervention in order for data protection to keep pace with technological and economic developments. Timing matters because, after its collection, the lifecycle of personal data is no longer linear, but multiplies. Measures to protect privacy and data protection must be scalable in order to have some effect in ubiquitous data processing. Both time and scalability underpin the principle of data minimisation (ENISA, 2012b, p.4).

[35] The *first* controller is required to inform the data subject about the recipients of the data (data protection Directive, Arts 10(c) and 11(c)).

The EU regulatory framework presupposes individuals' control at the stage of the collection of personal data and with regards to specific purposes. One significant implication of today's online data processing practices is that it is no longer feasible or even adequate to expect control to be exercised on a per unit basis and vis-à-vis each controller. Instead, data protection regulation must rely on a summary or proxy approach, i.e. wholesale means of expressing privacy preferences and complying with data protection regulation. One example, if realised, would be the Do Not Track (DNT) browser settings (box below).

The Do Not Track (DNT) browser settings

DNT would allow internet users to express their choice of online tracking vis-à-vis other websites through their browser settings.[36]

To have recipients accept and conform to DNT, the World Wide Web Consortium (W3C) is drawing up a recommended standard, expected to be finalised in 2014.[37]

Top EU policy-makers welcome these efforts: "the DNT standard must be rich and meaningful enough to make a difference, when it comes to protecting people's privacy. It should build on the principle of informed consent, giving people control over their information. And, indeed, it must be designed to let people choose to not be tracked." (Kroes, 2012)

In the online environment, interoperability is an architectural principle running through the IT stack and interfaces bridges between different technology layers. Such interfaces, i.e. middleware and application programming interfaces,cannot only facilitate the exchange of information but could also leverage data protection more effectively. Online, various platforms (e.g. operating systems, in cloud computing platforms as a service and app stores) are competing, yet within their respective developers' environment they cater for the possibility to exchange data, including the personal data of users. These are the bottlenecks where PETs should be deployed and users should be able to exercise centralised control over personal data exchanged.[38]

[36] It is implemented as a HTTP header added by the browser to the IP packet through which it requests content from a website. If the header has value 0, the user is expressing consent to tracking; if the header has value 1, the user is negating consent to tracking. If the user does not set the value, the header has value *null* and does not prevent tracking.

[37] See W3C Working Group of Tracking Protection at http://www.w3.org/2011/tracking-protection (accessed on 20 March 2013).

[38] Zittrain (2008) in his seminal book explained that the architecture of online platforms takes the shape of an hourglass, the waist-line is the platform to which, on the one side other services and applications connect, and on the other side devices, and ultimately users.

To conclude this section, the key concepts in data protection discussed above are not as affected by dramatic technological developments as is sometimes claimed. The regulation is flexible and can be applied in different situations and circumstances, underpinning the horizontal approach of the regulation. The basic concept still provides a consistent framework that allocates roles, responsibilities and rights – with only a few adjustments necessary, for example reorganising roles such as data controllers and processors in accordance with today's needs.

Regulation has an important role to play in underpinning the impending shift of culture and to deliver against the objective of data protection, but may require removing known disincentives for compliance. Aside, regulatees' ability to situate themselves in what is required under data protection may be sacrificed in the regulatory maze. Legal clarity is compromised because too many concepts are implicit. The early timing and scalability of any measures that aim at enhancing privacy and data protection is increasingly important for the regulation to make an impact.

5. Modernising data protection regulation

This section first takes a step back when looking at proposals for how to fundamentally rethink data protection (i.e. 'out of the box' modernisation) before turning to modernisation that builds on the existing *acquis* (i.e. 'inside the box' modernisation).

5.1 Reconceptualising data protection

The idea to reconceptualise data protection is mainly motivated by "the economic reality of information richness on one side and increasingly voluminous data protection legislation on the other" which are arguably drifting apart (Novotny & Spiekermann, 2012, p.2; also Laudon, 1996, p.92). As an attempt to embrace radically different conceptions that would more adequately protect personal data, three influential concepts are discussed: propertisation, contextual integrity, and an abuse centred approach to regulation, which are briefly explained below.

5.1.1 Propertisation

First, proponents of the property approach suggest conferring property rights to personal information (Laudon, 1996; Purtova, 2012; Schwartz, 2000; *inter alia* Novotny & Spiekermann, 2012). A property right lends itself as a reference framework because – contrary to data protection in its present form – it is more recognised in the public mind. Property rights possess three key attributes: they are exercisable *erga omnes*,[39] alienable, and divisible (Lyndskey, 2013).

[39] *Erga omnes* (Latin: "toward all") signifies obligations that apply universally.

As an advantage, a property regime allocates unambiguous rights and responsibilities, thereby fostering personal information markets. It would overcome the dilemma with present data protection regulation in which roles are defined, such as data controllers, to which a set of obligations are attached. Instead, the protection vested in personal data becomes more fluid because the obligation applies to all subjects (i.e. *erga omnes*). A number of ambiguities with existing roles could thus be avoided (see, for example, the difficult question in cloud computing of who the data controller and who the processor is). Beyond this small accomplishment, data protection regulation already permits transactions involving personal information, insofar as individuals can consent to the processing of their personal data. Alienability is probably at odds with the fundamental rights to privacy and data protection, under which personal data belongs to the data subject even where it is legitimately processed.

Moreover, whether property rights in personal information would tangibly protect personal information better is disputable. In economics, property rights are a means of reducing scarcity (which was induced by non-excludability) by promoting incentives in their acquisition, creation and improvement. In digital information the nature of the problem is inversed in that there is an overconsumption (see section 3.3). Introducing property rights to force scarcity rather than to reduce it is unlikely to produce the desired outcome.[40] Finally, responsibilities would be fully transferred to data subjects. In light of the economic peculiarities of personal data and insights from behavioural economics, this may still require regulatory intervention. At the same time, propertisation of personal data does not follow the legal traditions of many national property right systems and will be accordingly met with political and legal resistance.

5.1.2 Respect for context

Contextual integrity is an influential concept originating from Nissenbaum (2010). In its original connotation, for personal data processing to be permissible, consistency with the underlying consumer relationship and the context of the data disclosure is required. Contextual integrity is now taken up as one of seven principles in the US proposal Privacy Bill of Rights (The Whitehouse, 2012) which does not have legal force (see box below). The concept's salience stems from its relative flexibility, which resonates very well with stakeholders, including the Task Force participants. It is also diffused in the discussions surrounding the EU data protection reform.

Respect for Context Principle

"Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data. Companies should limit their use and disclosure of personal data to

[40] In the digital age, experience with intellectual property rights, such as copyrights, made it clear that *de iure* excludability doe not easily translate into *de facto* excludability (Samuelson, 2000).

those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. If companies will use or disclose personal data for other purposes, they should provide heightened Transparency and Individual Choice by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. If, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice. Finally, the age and familiarity with technology of consumers who engage with a company are important elements of context. Companies should fulfil the obligations under this principle in ways that are appropriate for the age and sophistication of consumers. In particular, the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults."

Source: US Privacy Bill of Rights proposal (The Whitehouse, 2012).

Whether this principle would ameliorate the EU regulatory framework on personal data protection is doubtful (as advocated by Alvaro 2012, p. 12). Both tiers that would define the consistency of personal data usage with the underlying context are already firmly embedded in the present regulatory framework. The data protection Directive holds that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes" (Art. 6(1)(b)). Hereinafter, the data processing is legitimate if it is necessary for the performance of a contract to which the data subject is party (data protection Directive, Art. 7(b)).[41] The contract is a context that would combine a number of purposes for which personal data is processed (e.g. communication with the customer, facilitating payment, personalising the service, entry into customer database etc.). No consent is required in addition to this. Contextual integrity would implicitly feature in determining whether the data controller could invoke his/her legitimate interest (data protection Directive, Art. 7(f)), and could also define the limits for invoking legitimate interest.[42]

[41] In addition, under the e-privacy Directive 2002/58/EC as amended by Directive 2009/136/EC, with regards to storing information or to gain access to information stored in the terminal equipment of a subscriber or user (e.g. cookies) as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user (Art. 5(3)); with regards to email marketing in a customer relationship as long as customers can opt-out (Art. 13 (2)). Only the processing of location data and traffic data is to be based on the consent of the users or subscribers even if they are processed in the context of a value added service (Arts 6(3) and 9(1)).

[42] See also the proposal for a General Data Protection Regulation, Recital 40: "The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, […]".

5.1.3 Abuse-centred approach

A third and highly controversial idea considers an abuse-centred approach, thereby shifting from *a priori* protection to *a posteriori* regulation of data abuse.

> [I]t can be questioned whether the European data-protection system, with its focus on *a priori* regulation of data collection and processing, can be upheld much longer in a world where data processing occurs in so many ways, to such an extent, and for so many purposes as it does today. Shifting the focus of legal protection to *a posteriori* regulation of data abuse might turn out to be a better strategy to protect individuals in the long run (Koops et al., 2007, p. 154).

The abuse-centred regulatory approach has operated since 2007 as an exemption to unstructured processing in Sweden (Magnusson Sjöberg, 2007, p.111).[43] In principle, it allows data processing unless processing constitutes a misuse of the privacy of an individual. Legal changes are considered to be a reaction to the CJEU seminal judgement in *Lindquist* (CJEU, judgement of 6 November 2003, Case C-101/01).[44] It is important to note that Swedish data protection regulation is reactive only in unstructured processing activities, i.e. the facilitation of everyday processing of personal data in electronic communications and ordinary composing of text (Kosta, 2013). In cases of structured processing activities, that would concern most online data processing activities by companies, this rule could therefore not be invoked.

A general overhaul of online consumer data protection in the EU in favour of *a posteriori* regulation of data abuse may not be adequate in light of the fundamental right to data protection in Art. 8 of the CFR. An abuse-centred approach to data protection could further be contested under the jurisdiction of the ECtHR, which ruled that Art. 8 ECHR entails a positive obligation to introduce measures that would give effect to the right for respect of private life including in the private sphere (ECtHR, *X and Y v Netherlands*, judgement of 26 March 1985, para. 23).

To conclude this section, all proposals for reconceptualising data protection struggle with the issue of delivering a real benefit for the protection of personal data. Market- and property-based approaches to data protection, especially, have little impact on the current debate. Data protection regulation in Europe is more likely to evolve in a path-dependent way, and modernisation is more likely to bring about piecemeal changes to the existing conception of data protection regulation. Some ideas would ramp up consumer protection style or/ and risk-based regulation (Kantor, 2010, para. 57; RAND, 2009, p.26 and p.30).

---

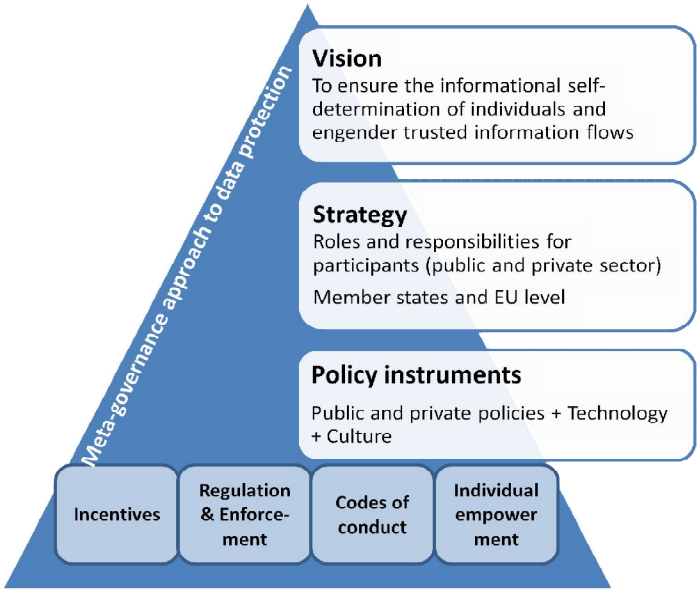
[43] It remains open whether the CJEU would uphold this interpretation as complaint with the data protection Directive.

[44] The *Lindquist* case concerned the publication of personal data on an internet website. The CJEU clarified that on the internet personal data are made public and accessible for an unlimited number of people, and therefore the processing cannot be considered a purely private matter and falls within the application of the general data protection Directive (CJEU, judgement of 6 November 2003, Case C-101/01).

5.2 Meta-governance approach to data protection

What is more promising to revive the virtues of privacy and data protection is a meta-governance approach to this policy issue, where regulation is but one of several pillars supporting the overall policy. Such a meta-governance approach combines policy consistency and joined-up governance over a series of public and private measures that share the same vision. For the EU this approach would have the advantage that privacy and data protection becomes more firmly embedded in public and private sector activities and related values are reinforced at various levels.[45]

Figure 5. Meta-governance approach to data protection



Source: Own representation based on Carblanc (2010).

Member states and the EU would need to co-operate at all levels and ensure the optimal attainment of data protection through a variety of measures. Once adopted, the proposed general data protection Regulation would become the centre-piece of this strategy but there is an important role for private policies. However, this normative basis needs to be accompanied by other measures that tackle technological and cultural aspects of privacy and data protection, in particular.

[45] There are some areas where the EU already harnesses meta-governance, e.g. the European Commission's Safer Internet Programme, which is mainly about children's internet use, see (http://ec.europa.eu/information_society/activities/sip/index_en.htm).

5.2.1 Private policies

In the context of online data processing, resorting to the knowledge and expertise of private organisations can strongly enhance the effectiveness of the whole data protection framework.

EU data protection regulation is already seeking to encourage codes of conduct as a contribution to the proper implementation of the rules while taking account of the specific features of the various sectors (data protection Directive, Art. 27(1)). Codes of conduct are neither self-regulatory nor co-regulatory, because national DPAs or, in the case of EU-wide codes, the WP29 can ascertain whether the proposed code is in accordance with the law. There has been criticism that this approach has not been very successful given the low number of codes adopted in line with this procedure (European Commission, 2003, p.26; RAND, 2008, p.37; see also box on Online behavioural targeting in section 4.2.2).[46]

The draft proposal for a general data protection Regulation by and large continues this practice, but foresees (for now) a role for the European Commission to grant general validity to codes of conduct within the EU (European Commission, 2012a, Art. 38). It is important to clarify how codes of conduct in the area of data protection fit into the wider framework for private policy-making with the participation of EU bodies. The 2003 inter-institutional agreement on better law-making prohibits the use of self- and co-regulation where "fundamental rights are at stake" (European Parliament et al., 2003). Finally, provided this obstacle can be overcome, there should be a clear reference to good practices in self- and co-regulation, such as transparency, representativeness of stakeholders, accountability and enforceability, among others.[47] Moreover, once a code of conduct has been approved by the competent public body at national or EU level, would compliance with the code be deemed as being compliant with data protection legislation? (Kuner, 2012a, p.16)

Outside of Binding Corporate Rules, private policies are often somewhat narrowly equated with collective codes of conduct. Currently there are a number of single firms in the online environment whose policies and terms of use can influence the conditions for privacy and data protection for a large share of individuals and users. Here, an individual company's example can signpost good practices for a whole industry and, vice versa, reflexive governance can monitor large data controllers' practices.[48]

---

[46] So far only one, i.e. European code of conduct of FEDMA for the use of personal data in direct marketing and the online marketing Annex as ascertained by opinion 4/2010 of the WP29 (2010b) but "the implementation of Directive 2002/58/EC, as amended by Directive 2009/136/EC, into Member States' legislation may require the amendment of the Annex, particularly as far as cookies and spyware are concerned to be in line with the new provisions." Another request from IATA did receive a positive comment from WP29 in 2001.

[47] Also in the light of the forthcoming "Code for Effective Open Voluntarism: Good design principles for self- and co-regulation and other multi-stakeholder actions" promoted by the European Commission, DG CONNECT.

[48] E.g. DNT controversy over Microsoft's early move, see *The New York Times* "Do Not Track? Advertisers Say 'Don't Tread on Us'", published 13 October 2012, (http://www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html).

5.2.2 Technology

Among policy-makers, harnessing technology for privacy and data protection online is possibly the most promising avenue aside of regulation. Three intervention points and practices are presently considered: 1) standardisation and 2) PETs and privacy by design, both of which are backed-up by 3) independent audits and/or certification of compliance with EU data protection regulation.

- Technical standardisation processes

In its impact assessment, the European Commission already takes up the possible role of technical standardisation processes (European Commission, 2012b, pp. 47, 63, 87, 92; see 2007b, p.7). The internet largely builds on open technical standards, which are devised by international, often private, standardisation bodies.[49] These standards define crucial building blocks, such as protocols and interfaces (APIs), in the internet's IT stack. Some of the most significant developments for effective privacy controls are expected from accepted outcomes of standardisation, such as the DNT browser settings (see box in Section 4.2.3).[50] Privacy and data protection are certainly not absent from standardisation processes today, but would certainly benefit from a sustained representation in standardisation bodies with a view on creating compatible solutions to the EU data protection regulation.

- Privacy enhancing technologies and privacy by design

Technology can be both privacy invasive and privacy enhancing, and to a large extent it depends on the patrons' decision about how to reconcile a given functionality with data protection requirements. Privacy by design is a particular approach to privacy-enhancing technologies (PETs) "where privacy considerations are integrated from the start with the business model as well the systems and processes of the organisation" (London Economics, 2010, p. 31). Because privacy is difficult to retro-fix in information systems without incurring other significant trade-offs, it is important to address implications of data protection and privacy before they are commissioned (Kantor, 2010, para. 131). The proposal for a general data protection Regulation carries as new principles privacy by design and by default (Art. 23). The European Commission and member states can promote research and development of PETs by making it one of the priorities in their respective research and innovation programmes, such as EU's Horizon 2020 research and innovation framework.

EU funded PET research

[49] Most significant are the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF), among many others not mentioned here, but also the International Standards Organisation (ISO) and increasingly the International Telecommunications Union's (ITU) Standardisation Bureau.

[50] However, privacy standards are not always adopted in the market, e.g. the Platform for Privacy Preferences Project (P3P) was developed and recommended by the World Wide Web Consortium (W3C) in 2002, but it never really had any impact.

Sixth Research Framework Programme (FP6, 2002-2006), ICT for Trust and Security:

- PRIMELIFE: bringing Sustainable Privacy and Identity Management to Future Networks and Services.
- PICOS: Privacy and Identity Management for Community Services.

Seventh Framework Programme (FP7, 2007-2013), Secure, dependable and trusted Infrastructures:

- PRIME: developing solutions for solutions on privacy-enhancing identity management. PRIME received the 2008 HP-IAPP Award in the category 'Privacy Innovation Technology'.
- FIDIS: developing new ways of dealing with identities, including so-called user-controlled virtual identities, embodying concepts such as pseudonymity, anonymity and strong identification, as required by circumstances.

Source: European Commission at http://cordis.europa.eu/fp7/ict.

- Data protection audits and certification schemes

Certification schemes (or privacy seals) can be a way to recognise and showcase compliance with EU data protection rules, which may become especially relevant in online personal data processing (European Commission, 2012b, p.47 and p.112). Certification is consequently encouraged under the draft proposal for a general data protection Regulation that would take into account "the specific features of the various sectors and different processing operations" (Art. 39). With a view to the costs of certification this measure would not be mandatory for controllers (European Commission, 2012b, p.112). It is important that certification ties in with technical standardisation, however, where appropriate, including with regards to PETs. Experience gained in other sectors should guide the implementation of certification schemes, e.g. the forthcoming JRC study on privacy seals and trustmarks (Tirtea, 2013).

5.2.3 Cultural

Finally, cultural impulses are indispensible to promote privacy and data protection in the EU and beyond. Measures have to target data subjects, controllers, processors and professional groups equally and should, wherever possible, be integrated with other policy fields at EU and member state level.

The role of education and awareness raising is largely recognised among EU policy-makers (European Commission, 2010c, p. 8; European Parliament, 2011, paras 16 and 18), e.g. the

Fundamental Rights and Citizenship programme of the European Commission DG Justice.[51], Measures need to be more systematic and sustainable, however, as well as adequately resourced.

In addition to transparency and awareness, individual empowerment needs better tools and tactics for data subjects to recognise and control the collection and use of their personal data. PETs can be deployed at both ends, by controllers and data subjects. There are many useful applications for consumers and users that could be presented, explained and made available on a user-friendly online portal.

Capacity-building concerns the need to support the training of EU data protection professionals and sensitising relevant professionals to the fundamentals rights dimension and regulatory implications. In light of impending requirements for data controllers to appoint data protection officers (hereafter DPOs), this needs to be matched with publically accredited training programmes and online resources to develop these new capacities. Privacy by design requires patrons to subscribe, but also software developers and IT processionals to be attuned to his aim.

The EU and member states should leverage privacy and data protection best practices as a horizontal issue through public procurement and other publically funded programmes, e.g. the existing incorporation of ethics in EU research and innovation policy.[52]

All in all, the new Regulation should be firmly embedded in an overall strategy that combines various approaches that would jointly contribute to privacy and data protection and integrate this concern widely in other public policies and programmes.

6. (R)evolution? The reform of EU data protection

There is broad consent that the first-generation EU data protection framework is in need of reform in order to 1) better reflect significant advancements in information technology and systems; 2) formulate responses to the ubiquity of personal data processing; and 3) overcome fragmentation in the internal market. The 2010 Digital Agenda for Europe proposed a review of the EU data protection rules as one of the key actions (European Commission, 2010b, p.13). On 25 January 2012 the Commission published a draft for a Regulation with the aim of modernising the legal framework and enhancing the trust and confidence of European consumers (European Commission, 2012a).

Against this backdrop, the draft proposal for a general data protection Regulation pursues two general objectives: 1) to enhance the internal market dimension of data protection and 2) to increase the effectiveness of the fundamental right to data protection (European Commission

[51] See (http://ec.europa.eu/justice/grants/programmes/fundamental-citizenship/index_en.htm).

[52] See e.g. Ethics in ICT research at (http://cordis.europa.eu/fp7/ethics-ict_en.html).

2010c, p. 5; 2012a; European Parliament 2011). The proposal is based on the premise that the existing data protection level is to be maintained.

Contributors to the Task Force emphasised the fact that the reform is an evolution in that it modernises existing rules and not a revolution in the sense that it would overhaul the data protection *acquis*. Task Force participants generally welcomed the proposal to introduce a single set of rules for the EU and a number of proposed measures that benefit data controllers, e.g. removing the notification requirement and the vision of a 'one-stop-shop' according to which one DPA in the EU is responsible for a controller. Reflecting the division of interests among stakeholders, other aspects of the reform proposal were the subject of more fervent debate, in particular key concepts, the definition of which influences the scope of application.

This section does not offer a detailed discussion of the draft Regulation but necessarily focuses on three issues: overcoming fragmentation, regulatory innovation, and major critical issues that remain unresolved.

6.1 Overcoming fragmentation

Once adopted, the Regulation would overcome the present fragmentation of data protection rules, because its provisions would be binding and directly applicable in the member states (TFEU, Art. 288). Indisputably, the Regulation would unleash much potential for making business throughout the EU (digital) single market, since the processing of personal data is today almost commonplace in every company, e.g. employees' data processing and among groups of companies. Unifying rules also implies that differences are levelled out even where national or local good practices have successfully taken hold (see, for example data protection officers in Germany described in Kuner 2012a).

Online personal data processing – the subject of this Task Force – is bound to thrive on fully harmonised rules. Task Force participants and contributors discussed two issues in which fragmentation is likely to persist: 1) regulatory competences and 2) the regulatory division of labour between general and sectoral data protection rules, including legislation mandating data processing operations from private parties.

6.1.1 Regulatory competences

The one-stop-shop premise may not be fully accomplished. The draft proposal for a general data protection Regulation links supervisory competences to the main establishment of the data controller or processor (Art. 51(2)). The notion of main establishment is defined, but the definition presupposes a centralised decision-making structure in relation to decision-making about data processing (Art. 4(13)). Task Force participants argue that decisions about data processing are made in a more decentralised fashion, according to the distributed work-share within the group or corporation. If, however, the place of the central administration in the EU triggers the supervisory competence of the national DPA (see Recital 27), then the definition

of main establishment in relation to decision-making about data processing becomes superfluous (see also Falque-Pierrotin, 2012, p.5).

Participants in the Task Force expressed concern that the extensive consistency mechanism that any other DPA, the new European Data Protection Board, and the European Commission can request may significantly inflate the back-end of the one-stop-shop premise (Arts 57 and 58; see Traple Konarski Podrecki and Partners and European Legal Studies Institute, 2012, p.45). Nevertheless, a consistency mechanism is deemed necessary in order to build the mutual trust in shared regulatory supervision in the first place. What could be contested is the overall capacity of the consistency mechanism to comply with potentially several hundreds of notifications about draft measures and requests at the same time.[53] How to reconcile the consistency mechanism with the independence of DPAs is another open question (Kuner, 2012a, p.20).

Finally, the Regulation's intention to introduce a regulatory one-stop-shop in the EU could be problematic in member states with more than one public authority in charge of data protection supervision (see section 2.3.1). A federal system would also designate one responsible authority; however, sectoral divisions of competences may add up, especially in countries in which supervision for general data protection and in electronic communications (pursuant to the e-privacy Directive) is distinct. The draft proposal for a general data protection Regulation prescribes designating a "single contact point"; a pragmatic solution that was piloted under the services Directive (Directive 2006/123/EC of 12 December 2006 on services in the internal market).

6.1.2 Regulatory division of labour

The residual division of labour between general data protection legislation and national laws pursuant to the e-privacy Directive will continue to exist once a new general data protection Regulation enters into force (see section 2.2). In the present EU regulatory framework sectoral data protection rules are *lex specialis* with respect to the data protection Directive, which means that specialised rules take precedence over general ones. The ensuing regulatory division of labour is not trivial because an EU regulation is directly effective and supersedes member states' laws. The relationship between sectoral norms and the new regulation needs clarification, which the draft proposal for a general data protection Regulation does not fully achieve (Art. 89).

Due to the shift towards digital services, the economic significance of the e-privacy Directive is mounting steadily, with the effect that it develops into a mainstream data protection instrument (see section 2.2.2). Online personal data processing tends to be covered by both,

[53] When juxtaposing the proposals with the consistency mechanism under the regulatory framework for electronic communications, which already incurs a heavy workload, the number of cases is largely pre-determined by the number of recommended relevant markets multiplied by the number of member states (so-called Arts 7 and 7a procedures, see (https://ec.europa.eu/digital-agenda/en/consultation-procedures).

general and sectoral instruments.[54] Task Force participants realise that fragmentation will persist in many important details covered by national laws pursuant to the e-privacy Directive. Task Force contributors, including from the European Commission DG CONNECT, are well aware of the two tracks, which can be explained against the background of competencies and reform agendas opening different windows of opportunity to introduce new data protection rules. Prospectively, data protection rules that apply across the information society and value added services, which involve the processing of personal data emanating from electronic communication services, should be transferred and thereby unified within the Regulation.

Significant fragmentation will also occur with regards to legislation at EU and especially member state level mandating data processing operations to the controller for general interest purposes, e.g. national transpositions of the data retention Directive (see section 2.2.3). In addition to this, each member state maintains countless national laws that data controllers may need to be aware of if their operations fall within the jurisdictions of different member states. In most instances, this is not a question of harmonisation, but of transparency. Member states should be encouraged to draw up a public repository of rules that mandate the collection, conservation or retention, and disclosure of personal data from private parties, which are controllers. This is critical because businesses may find it difficult to navigate the national systems of data protection and other opposite obligations. It can also help policy-makers to shift perspective from a single measure to a systematic view on data processing.

Another area that should be observed is general competition law, even though it protects undistorted competition, not privacy and data protection as such. Personal data assets will be scrutinised under EU and member states' competition law and merger control sooner or later, the more they become an integral part of companies' business models (Almunia, 2012).

6.2 Modernisation

The scale and magnitude of online personal data processing is widely perceived as a disruptive challenge that would require an evolution in the tactics and means of data protection regulation. Modernisation can take two directions: 1) on the one hand, measures that aim at strengthening individuals' rights; 2) on the other hand, reinforcing requirements placed on data controllers and processors while removing excessive administrative burdens.

6.2.1 Strengthening individuals' data protection rights

Much of the proposed modernisation addresses individual rights in the digital environment (European Commission, 2010c, p. 5; 2012, Recital 5). Not all proposals add up to regulatory innovation that could offer new responses to a technical paradigm shift.[55]

[54] Online behavioural advertising, for example, where each component - online tracking, behavioural profiling and targeted advertising – would be covered by both instruments simultaneously.

[55] Provisions relating to children have not been covered by the Task Force.

- Clarification

In parts, the legislative proposal clarifies and removes certain ambiguities:

- In the definition of consent, a statement or affirmative action is a prerequisite (European Commission, 2012a, Art. 4(8));
- The nascent separation principle also clarifies that consent is not "freely" given where the data subject has no choice not to consent (European Commission, 2012a, Recitals 32, 33).

Neither proposal reforms the law, but may out-law practices that relied on interpretations according to which the consent mutates to a right to object (Kosta, 2013). While Task Force participants stress the need for flexibility and shared responsibilities, as well as the benefits of free online content for consumers, pervasive commercial practices essentially place the opportunity costs of managing privacy on individuals.

Germany, and possibly the new EU framework, foresees a lighter form of the separation principle, which requires that the request for consent for additional data processing must be prominently separated. The economic evidence would also support measures that reverse dynamics in online transactions to the benefit of users and consumers (see section 3.3.4). Some Task Force participants cautioned that, as a result, a "privacy divide" can emerge where those who can afford privacy enjoy it. However, it also emerged that businesses are specifically interested in this segment of the population that is happy to pay a premium for privacy. What other consequences of a separation principle would be, beyond the possible need to determine what is a fair premium for privacy (which may require regulatory intervention), cannot be predicted.

The regulatory treatment of consent in a situation of significant imbalance between the data subject and the controller is still very much in flux. Originally inferred as a safeguard in employment relationships, this provisions now oscillates between dominant firms in a consumer relationship and other situations that are critical for free decision-making, e.g. individual insurances. Participants of the Task Force were particularly sensitive to expand the provision to dominant firms *per se*. Perhaps a clear separation principle under fair conditions would suffice to address the concern regarding online service, be they free or for remuneration.

- Extensions of existing rights

Certain rights of the data subject in the draft proposal for a general data protection Regulation could be better perceived as extensions of existing rights:

- The right to be forgotten as an extension to the right of erasure (Art. 17) (Kuner, 2012a, p. 11);

- The right to data portability as a modern means to access one's own personal data, but with the new edge to transfer it between providers (Art. 18).

The right to be forgotten appears to be most controversial where the controller has made the personal data public, not the least because of the right to freedom of expression. Leaving the arguably legalistic exercise of balancing conflicting fundamental rights to the controller may potentially result "in a chilling effect on use of the Internet" (Kuner, 2012a, p. 11; see also FRA, 2012, p. 15f.).[56] Beyond clashing fundamental rights, the right to be forgotten and erasure is designed as a best effort approach and requires the controller to inform third parties that are processing the personal data about the data subject's request "to erase any links to, or copy or replication of that personal data" (Art. 17(2).

- Regulatory innovation

The rules on data portability and profiling are new to the fabric of personal data protection and can therefore be considered regulatory innovation (European Commission, 2012a, Arts 18, 20).

The right to data portability is a highly controversial issue, largely because it is not clear from the legislative proposal whether this is a '*lex* social network' (European Commission, 2010c, pp. 7ff; see also De Hert & Papakonstantinou, 2012, p.138) or would concern every other context, such as electricity providers and banks. The feasibility of implementing the portability of personal data and the extent to which this implies mandating electronic data exchange formats are also contested points (Art. 18(3)). The principle of portability is, however, capable of significantly strengthening individuals' rights where personal information is compiled over time and could be transferred to a different provider (Costa & Poullet, 2012, p. 527; De Hert & Papakonstantinou, 2012, p.138).

The concern about profiling, which is now within the reach of nearly every controller of systematic personal data collections, is difficult to pin down. While the draft proposal for a general data protection Regulation appears to settle for regulating measures based on profiling, a few Task Force contributors expressed caution about the very process of creating personal profiles (Leenes, 2013) and possibly discrimination and indirect processing of sensitive data in algorithms (De Hert & Papakonstantinou, 2012, p. 138; Korff, 2012).[57] Several legitimate bases for profiling would be offered. However, the threshold for measures legitimately based on profiling is comparatively low and the interests of the data subject *not*

[56] See also the provisions on the processing of personal data for journalistic purposes or artistic or literary expression and freedom of expression in the draft proposal for a General Data Protection Regulation (Art. 80).

[57] See also the definition used by the Council of Europe (2010, at 1(e)) regarding profiling: "an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".

to be subject to profiling in a commercial context, except where explicitly consented to, would not be specifically protected.[58]

6.2.2 Updated requirements placed on data controllers

The reform proposal for a general data protection Regulation envisages removing some administrative burdens, but simultaneously introduces a range of new obligations that aim to enhance systematic compliance with data protection rules. Because abolishing the dysfunctional notification requirement is well received by all stakeholders, new technical and organisational measures for controllers are reviewed below.

- Data protection by design and by default

The principles of data protection by design and by default have been fashioned for some time as a promising remedy for automated processing of personal data (see section 5.2.2; European Commission, 2012a, Art. 23(1) and (2)).

Data protection by design is an umbrella for all kinds of technical and organisational measures that the controller could adopt in order to ensure data protection rights of individuals and compliance with relevant data protection legislation. It is a general principle that is sensitive to the state of the art and the cost of implementation of any such measures. It is flexible because it does not hold much prescriptive substance apart from requiring that privacy by design should be taken account of both at the time of the determination of the means for processing and at the time of the processing itself. The risk for this principle may consist in the lack of any benchmarks against which good or bad practices are assessed. Indeed, the lack of a clear benchmark may prevent this principle from living up to its aim, beyond only requiring more documentation for controllers regarding their efforts to comply.

Data protection by default seeks to harness technical means to give effect to important principles of data quality, i.e. purpose specification, collection limitation, and use limitation (see section 4.1.2; European Commission, 2012a, Art. 23(2)). "In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals" (Art. 23(2)). As a technical design principle adherence to this requirement could be relatively easy to verify.

There is a good chance that the demand for technological solutions that deliver data protection by design and default could jumpstart a market for producers of devices and software. EU data protection regulation should be clear that controllers comply with data protection by design and default if they use assured products and services of third parties, e.g. where they are certified under a data protection certification scheme.

[58] As it stands, certain types of commercial communication could legitimately involve profiling since it "could be construed as an invitation to accept a contract" (Winton & Cohen, 2012, p. 98).

There is an emerging view that from a societal and ethical point of view other central actors should also bear some responsibility for data protection, e.g. those who design technical specifications and those who actually build or implement applications or operating systems (European Commission 2007b, p. 2f.). PETs will only be truly beneficial if they are effectively incorporated into and used by technical equipment and software tools that carry out processing of personal data (European Commission 2007b, p. 6).

> When looking at the implementation of privacy by design and by default as shown by the Proposal, it can be questioned whether it is sufficient to only address controllers and processors, since there is a great relevance of these regulations for advisers, developers and producers of hardware and software as well. They should particularly be subject to the concept of privacy of design. It might be more efficient to attach this concept right at the source. (Traple Konarski Podrecki and Partners and European Legal Studies Institute, 2012, p.51)

Judged from the present draft, EU data protection regulation fails to acknowledge that individuals would also be empowered by PETs. Individuals should be free to install PETs on their personal devices.

- Data protection impact assessment

"Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope, and their purposes" the controller (or the processor on the controller's behalf) has to carry out a data protection impact assessment" (European Commission, 2012a, Art. 33). A catalogue designates processing operations that would trigger this obligation, i.e. a) automated measures based on profiling that produce a significant legal effect for individuals, b) measures and decisions regarding individuals based on the processing of special categories of personal data relating to sex life, health, race and ethnic origin in health care and medical research, c) large-scale video surveillance in publicly accessible areas, d) personal data in large-scale filing systems on children, genetic data or biometric data, and e) processing operations for which prior consultations of DPAs is required.

The processing operations listed raise high the bar for impact assessment; some would say too high to buttress privacy by design and by default. The impact assessment does not decide on the legitimacy of the purpose of the intended processing operation in relation to the fundamental rights and freedoms of the data subjects. Rather, it is a systematic exercise to describe the processing operations, identify corresponding risks and measures that would address these risks. Although representatives of data subjects should be involved, there is no transparency requirement concerning the impact assessment ("without prejudice to the protection of commercial or public interests or the security of the processing operations"). A lack of transparency may actually hamper the accountability on which the data protection framework rests.

- Data protection officers

An important organisational measure is to require controllers and processors to designate a data protection officer (hereafter, DPO) if they are crossing a certain threshold (European Commission, 2012a, Art. 35). The concept of DPOs originates in Germany as an early substitute of the notification requirement, and has taken root in many organisations elsewhere to ensure compliance with building expertise in-house or externally. As one Task Force contributor observed, for larger companies DPOs have really evolved from assuming a clerical to a strategic function (Kuner, 2012b).

DPOs must possess the necessary professional requirements.[59] Controllers and processors have to ensure that the DPO is involved in any decision concerning personal data; to guarantee his/her independence; and to provide the resources for his/her activities. DPOs have an advisory role and are involved in monitoring internal policies in relation to the protection of personal data (and namely the principles of data protection by design, default, data security, handling of data subjects' request, DPIA), have to maintain records and to fulfil notification and communication duties *vis-à-vis* the DPA.

There appears to be no agreement on what is a meaningful threshold to determine which controllers have to designate a DPO: number of employees, number of personal data processed per year, or if an organisation's core activity that concerns the systematic and large-scale processing of personal data should be decisive. It is reasonable to rely on a composite threshold, because large organisations can be expected to invest in data protection expertise, while other, even significantly, smaller organisations, when they specialise in processing and transfer of personal data, should be required to designate a DPO. One additional exemption should be considered when and insofar as personal data processing is necessary for the performance of a contract to which the data subject is party (see section 6.3.3.)

If well attuned, DPOs can indeed be a meaningful way to infuse data protection expertise in organisations that are significant controllers and processors of personal data. However, according to the impact assessment, DPOs are the single most burdensome addition to the privacy legal framework, creating administrative costs for €320 million if rolled out across Europe (European Commission, 2012b, p.69). As a way to better balance this burden, private organisations can rely on external DPOs that devote a fraction of their time, or designate an internal employee to take on this role together with other responsibilities.

6.2.3 Accountability and administrative burden to demonstrate compliance

Accountability, which is not a new concept in data protection (WP29, 2010c) is going to become the central bedrock of personal data protection regulation. The notion of accountability or responsibility is not defined as it perhaps should be, e.g. as "a permanent

[59] EU institutions and member states also have a role in supporting this emerging profession by building the capacity of DPOs-to-be (see section 5.2.3).

and dynamic compliance process" of a controller that would align internal processes and policies with data protection requirements (Falque-Pierrotin, 2012, p.7). A Task Force contributor pointed out that accountability would be best served by relating closely to established corporate governance mechanisms, such as mandatory annual corporate filings and (voluntary) corporate social responsibilities (Kuner, 2012a, p. 12; 2012b; see also WEF, 2012, p. 21).

Under the draft proposal for a general data protection Regulation it is the responsibility of the controller to ensure adherence to data protection Regulation and to demonstrate this compliance on request (Arts 5(f) and 22). It therefore links to a number of specific responsibilities, of which the documentation requirement has caused most controversy as creating additional administrative burdens for businesses (Art. 28). Thus, "[t]he commendable reduction of bureaucracy in some areas is at least partially offset by the introduction of other procedural requirements (Kuner, 2012a, p. 26).

There is, however, little alternative to internal documentation if a controller wants to be informed and up-to-date about processing operations under its control, not least with a view to ensuring compliance. It is important to recognise that documentation duties are inherently commensurate with the intensity of processing operations. They can be fairly simple for those private organisations whose main operations are not concerned with data processing operations. Prospectively, a large share of the required documentation of data processing operations could be automatised, e.g. logging data categories, rules, and routines.[60] The new Regulation should be specific about the possibility to comply with documentation duties at the level of IT systems and management.

It seems that the documentation duties would become subject to some threshold likely to converge with the DPO requirement. It is a difficult trade-off to reduce administrative burden for SMEs and nonetheless instil in them accountability for data protection. It may be better not to exempt SMEs wholesale from documentation duties but instead to privilege personal data processing when and insofar as is necessary for the performance of a contract to which the data subject is party (see section 6.3.3.). However, there should be schemes in particular for SMEs (perhaps with variations per industry or sector) that would enable EU-wide compliance and grant legal certainty (see also Kuner, 2012b).

6.2.4 Negative regulatory incentives

Negative regulatory incentives are very common in a command-and-control type of regulation where they are used as a deterrent against defection from the law (Baldwin et al., 2012, p.249). EU data protection regulation does already hold the possibility to impose

[60] Automated compliance tracking systems have greatly advanced as a consequence of recent US sectoral laws that require companies to assert compliance that also covers IT systems and management, notably the Sarbanes-Oxley (SOX) Act; the Health Insurance Portability and Accountability Act (HIPAA) as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

administrative and criminal sanctions as well as civil law liabilities but member states often rely on soft enforcement (see section 3.2.2).

If adopted, the general data protection Regulation would introduce significant sanctions for violating privacy obligations that can reach 2% of company revenues (Art. 79); however, sanctions would need to be commensurate with the wrongdoing or misdemeanour at stake. Although the ceiling is five times lower than for violations of EU competition law, monetary sanctions "are for the first time in the history of data protection law, of such a magnitude that they will get attention from companies' CEOs and general counsel" (Kuner, 2012a, p.21). This would give more teeth to enforcement and potential deterrence.

As it stands, administrative sanctions are very much geared towards fines, however, DPAs should be able to take into account voluntary commitments by controllers when imposing a fine, e.g. submitting to an independent data protection audit. Other enforcement actions may be necessary to assist compliance and rectify non-compliance, e.g. reinstating the requirement to designate a DPO in the case of exempted organisations.

Another negative incentive is the data breach notification that made its trajectory from the e-privacy Directive into the draft proposal for a general data protection Regulation (Arts 31 and 32). In combination with corporate efforts to protect their brand's reputation the data breach notification could harness controllers' best practices to protect the security of personal data. There are many benefits associated with a personal data breach notification duty because it enhances transparency and actionability in such events of DPAs and individuals.

6.3 Unresolved critical issues

Aside from the detailed wording that is still being negotiated in the legislative process, what critical issues did the reform proposals for a general data protection Regulation not address? In short, the Regulation remains too complex, regulatory concepts lack scalability and positive regulatory incentives.

6.3.1 Complexity

If simplification and clarification were a declared aim of the data protection reform, the proposals do not attain it (European Commission, 2010b, p. 18; Parliament, 2011, para. 25). On the contrary, the law is becoming more and more complex (Kuner, 2012a, p.5 and p.26).[61] Data protection regulation will undermine its own *raison d'etre* if it is not conceived from the perspective of regulatees and their varying expertise. Arguably, other legislation is highly

[61] "The draft Regulation is admittedly a long (and ambitious) text" (De Hert & Papakonstantinou, 2012, p.132) and "is considered one of the most complex pieces of legislation ever proposed by the EU Commission" (Novotny & Spiekermann, 2012, p.3). It should also be noted that the legislative convention to provide interpretative aid in the recitals before the actual legislation can be confusing for non-legally trained professionals. Obviously, the European Commission can issue a communication that would explain the General Data Protection Regulation better.

specialised too but often it is not meant to be complied with by virtually every company and business that processes personal data.

What is needed is a decisive effort to draft a document that uses plain language and a more accessible structure (e.g. introducing different tiers of obligations relative to the intensity and sophistication of making use of personal information). The basic tiers of data protection regulation must be capable of being understood and complied with by individuals who are themselves data controllers/processors or work for one, regardless of an organisation's size (see section 6.3.3 on personal data processing in the context of the performance of a contract to which the data subject is party). Required expertise in compliance management can be scaled up whenever the processing of personal data intensifies and more risks for the data subjects are involved. This logic is already present in data protection Regulation but it does not come across easily from the text.

6.3.2 Scalability

The reform proposals have been criticised for applying linear data protection concepts to a world of ubiquitous and distributed personal data processing. In spite of many welcome updates and regulatory innovation in the detail, the reform proposal appears to be path-dependent to an extent that it favours disaggregated management of personal data protection on the part of the companies and individuals concerned. What is missing are new concepts that would scale protection adequately in the information-rich future (Traung, 2012, p.47).

There are a few ideas, such as encouraging the development of data protection certification mechanisms and of data protection seals and marks. However, in order to meet the scale and magnitude of online personal data processing regulatory intervention points should be selected that are scalable (see section 4.2.3). Standardisation and PETs in middleware should become more central to the regulatory strategy. Moreover, the draft Regulation's reading of PETs is almost exclusively geared to controllers and processors rather than empowering individuals and users.

6.3.3 Positive regulatory incentives

We should be concerned that the draft proposal for a general data protection Regulation has so little capacity to nudge desired behaviour via positive regulatory incentives. Task Force participants did not identify any direct positive incentives either, and now policy-makers are still searching. However, the search for positive incentives should not conclude with carving out segments from personal data protection altogether but regulatory incentives should reward compliance from within the systematic of data protection.

Conceptually, data protection offers a few leverage points that could or should be used to instigate data protection compliant strategies on behalf of businesses: 1) use of anonymisation techniques, 2) personal data processing in the context of the performance of a contract to

which the data subject is party, and 3) purposefully promoting the uptake of privacy by design and by default.

- Anonymisation techniques

Using data rendered anonymous in such a way that the data subject is no longer identifiable does not fall under the scope of application of the EU regulatory framework on data protection (see European Commission, 2012a, recital 23). What could be a powerful incentive to use anonymisation techniques (Kuner, 2012, p. 9) may not receive widespread commercial support in an environment in which personal data is widely considered a commercial asset. Considering that data processing can be a mix and match strategy, for some purposes personal data would be used while other purposes can be achieved with anonymised data, with the advantage that the latter case does not incur any administrative burden. A public knowledge base of common issues and descriptions of how they can be addressed by relying on anonymised data could help raise awareness and promote this strategy.

- E-commerce and the performance of a contract to which the data subject is party

Personal data processing in the context of the performance of a contract to which the data subject is party should be better framed as a baseline situation, which should ideally incur only the minimum of administrative burden. EU data protection regulation recognises processing of personal data where and insofar as this is necessary for the performance of a contract to which the data subject is party as a legitimate ground for data processing (data protection Directive, Art. 7(b)). MSMEs and larger enterprises would benefit within the scope of this legitimate basis for personal data processing and exemptions from legal obligations could be justified, e.g. no DPO would be required and there would be no further documentation duties.[62] Perhaps this baseline scenario should be updated to fit e-commerce and online service better, in particular clarifying that it would also comprise the personalisation of services. What could work as a positive regulatory incentive in the realm of data protection in e-commerce would incidentally also serve the EU flagship initiative 'A Digital Agenda for Europe' (European Commission, 2012b, p. 12) to build digital confidence.

- Promoting the uptake of privacy by design and default

Positive regulatory incentives to promote the uptake of privacy by design and default are still sought (Traple Konarski Podrecki and Partners and European Legal Studies Institute, 2012, p.28). It is important to bear in mind that pseudonymisation of personal data could be an important ingredient of privacy by design and default but it does not equal this approach, which would require additional technical and organisational measures. One possibility is to

[62] The following activities would not fall within the proposed exemption: i) tying the online transaction to the consent to use personal data for secondary purposes; ii) the collection of personal data that is not necessary for the performance of the contract; and iii) the transfer of personal data to third parties when this is not necessary for the performance of the contract.

privilege the use of data protection compliant technologies by controllers in a way that would stimulate the demand for such products. One possibility would be to recognise off-the-shelf compliance for those parts of data processing equipment and software that are independently audited or certified as privacy by design and default, and then sold or licensed to controllers.

Another known strategy is leveraging public procurement at EU and member state level to express preferences for data protection audited or certified products and PETs (see European Commission, 2007b, p.12).

By way of summarising this section, the draft proposal for a general data protection Regulation offers substantial advantages compared to the present situation. However, the regulatory 'one-stop-shop' is still in legal limbo and from the vantage point of online personal data processing fragmentation persists along the lines of the e-privacy Directive and diverse EU/national legislation that mandate processing operations. Any modernisation is rather in the detail and evolutionary but overall the proposal remains complex and lacks scalability and substantial positive regulatory incentives that would nudge desired behaviours from controllers and processors.

Conclusions with policy recommendations

There is a wide consensus that the first-generation data protection rules of 1995 are in need of an update. The ongoing legislative reform aims to fully harmonise and modernise EU data protection regulation on the basis of the existing data protection *acquis*. Many commentators define digital confidence and trust as a key enabler of the new information-rich economy. EU data protection regulation has a role to play in the enhancement of that confidence and trust.

It is one of the most ambitious legislative objectives to engage EU policy-makers currently. Various legal traditions and cultures meet in the EU and individual perceptions about privacy and data protection tend to vary among member states (European Commission, 2011). Nonetheless, both, privacy and data protection form part of the common constitutional heritage of EU member states.

As a policy issue data protection understandably tends to be quite polarised (RAND, 2011, p.46). EU policy-makers find themselves in the unenviable position of having to strike a balance between the different interests at stake to satisfy European fundamental rights, without off-setting what the emerging information-rich economy has to offer for consumers, businesses and society at large.

Issuing policy recommendations at a time when the second-generation EU data protection legislation is in progress in the EU legislative process runs the risk of being judged against the politics of the moment; its scope is more ambitious than informing this ongoing legislative process, however.

Against the background of online personal data processing, this report issues policy recommendations that would address short- and medium-term policy goals that advocate a meta-governance approach to privacy and data protection.

Policy recommendations

Data protection in the EU translates the protection of fundamental rights into *sui generis* rules. As it is proposed, the general data protection Regulation **applies horizontally** for most public and private processing of personal data.[63]

1. In scope, the new regulation is **technologically neutral**, however, the **regulatory division of labour** with national legislation pursuant to the e-privacy Directive and potentially other legislations needs to be further clarified (see section 6.1.2). Task Force participants stressed that the relation between the general regulation and the e-privacy Directive should be addressed during the ongoing legislative process.

[63] With the exception of the parallel initiative for a Directive on the protection of individuals with regard to the processing of personal data for police and judicial cooperation in criminal matters and in addition to certain sector-specific data protection legislation.

2. From the vantage point of online personal data processing, fragmentation persists along the lines of the e-privacy Directive. **EU data protection rules** that apply to all information society and value added services online should be consolidated and thereby **unified** within the regulation (see section 6.1.2).
3. Strengthening the tenets of risk-based regulation, information assurance and management, as well as consumer protection **within** data protection is a plausible strategy in response to the privacy and data protection challenges of the digital environment.
4. The regulation should be further consolidated with the aim to **obtain a single and clear policy**. The draft legislation should be **edited**, use plain language, and **reduce implicit concepts** which really matter, e.g. transfer of personal data to third parties (see sections 3.2.2, 4.2.2 and 6.3.1).

In addition, the regulation to come should pay attention to further concrete short-term policy recommendations:

1. Resolve The **legal treatment of online identifiers** so that it remains internally consistent with other provisions (see section 4.1).
2. Ensure consistency in the event that the definitions of controllers and processors are adjusted and retain a **responsibility for the means of data processing**. Introduce a rule that **consumers cannot be the controllers of their personal information** that reside in third party equipment under a non-negotiable agreement with the service provider (see section 4.1.3.).
3. Strengthen individuals' consent as the lynchpin for quasi market mechanisms in personal data transactions with a clear **separation principle** that prevents the bundling of online services with individuals' consent to unrelated additional personal data processing. (see sections 3.3.4, 4.1.4 and 4.2.1).
4. The **'legitimate interest'** as a legitimate basis for the processing of personal data needs further clarification and defined boundaries in order to offer legal certainty to controllers and individuals alike (see section 4.2.2).
5. In exercising the new 'right to be forgotten' **controllers should not be left in charge to balance conflicting fundamental rights**, i.e. the right to privacy with the right to freedom of expression, without further guidance (see section 6.2.1).
6. The **scope of the new right to data portability** should be clarified and, where it is not otherwise legally permitted, **profiling is a distinct purpose** to which the data subject has to consent to (see section 6.2.1).
7. Regulation should ***enable technologically mediated compliance***, e.g. complying with documentation duties through automated IT compliance systems; automated means of expressing consents and manage permissions (see sections 4.2.3 and 6.3.2).

8. **Positive regulatory incentives should be strengthened** to be consistent with the Regulation, using as leverage points:
   a. the processing of personal data where and insofar as this is necessary for the performance of a contract to which the data subject is party, which should ideally incur only the **minimum of administrative burden** (see section 6.3.3);
   b. **privilege** the use of **data protection compliant technologies** by controllers and recognise off-the-shelf compliance for those parts of data processing equipment and software, which are sold or licensed to controllers (see section 6.3.3);
   c. enable **EU-wide compliance schemes**, in particular for SMEs, (perhaps with variations per industry or sector) and grant legal certainty (see section 6.2.3) as well as clarify the role of codes of conduct in complying with data protection Regulation (see section 5.2.1).
9. The **one-stop-shop premise must be fully accomplished** without depriving mutual assistance and joint operations of national DPAs. The **consistency mechanism needs more consolidation** so as not to exceed its capacity or inflate the decision-making back-end (see section 6.1.1).
10. As a transparency measure member states shall be asked to draw up a **public repository of legal data processing obligations** to which the controller is subject (see section 6.1.2).
11. Regarding sanctions, DPAs should be able to take into account **commitments by controllers** when imposing a fine. If SMEs are exempted from certain data protection requirements, instead of or complimentary to a fine, reinstituting the requirements to designate a DPO and documentation duties is a **tactical remedy**.
12. As a transparency measure, member states shall be asked to draw up a ***public repository of legal data processing obligations*** to which the controller is subject.

Mid-term policy recommendations which aim to strengthen data protection as a field of public policy are addressed to the EU and the member states:

1. **Fostering a culture of privacy and data protection** should be firmly embedded in a **meta-governance approach** where member states and the EU co-operate at all levels and ensure through a variety of measures the optimal attainment of both objectives.
   a. In consultation with member states, the EU should adopt a **comprehensive strategy** that addresses all participants in the public and the private sector according to their respective roles and responsibilities.
   b. Data protection legislation is bound to become the centre-piece of the EU policy but its values should be reinforced at various levels and via other measures spanning **public and private policies, technology and cultural measures** (see section 5.2).

c. **Cultural impulses are indispensible** to promote the values of privacy and data protection in the EU and beyond. Measures have to target data subjects, controllers, processors and professional groups equally and should, wherever possible, be integrated with other policy fields at EU and member state level (see section 5.2.3).

2. Measures to protect privacy and data protection must be scalable in order to retain their effectiveness in the information-rich economy (see sections 4.2.3 and 6.3.2).

   a. **Standardisation** and **PETs in middleware** should become more central in the regulatory strategy (see section 5.2).

   b. **EU-wide certification** and **compliance schemes** that grant legal certainty need to be prioritized.

   c. Policy should recognise the role of **PETS for empowering individuals** and the ability to exercise control over personal data via connected consumer devices (see sections 4.2.3 and 5.2.2).

References

Acquisti, A. (2004), "Privacy and Security of Personal Information", in J. Camp and R. Lewis (eds), *The Economics of Information Security*, Dordrecht: Kluwer.

Acquisti, A. (2010a), "The Economics of Personal Data and the Economics of Privacy", Background Paper for OECD Joint WPISP-WPIE Roundtable, 1 December 2010, Paris (http://www.oecd.org/sti/ieconomy/46968784.pdf).

Acquisti, A. (2010b), "The Economics & Business of Privacy: Past, Present, and Future", presentation at Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, Paris, 1 December 2010(http://www.oecd.org/sti/ieconomy/46944680.pdf).

Acquisti, A. and R. Gross (2006), "Imagined Communities: Awareness, Information Sharing, and Privacy on Facebook", in G. Danezis and P. Golle (eds), *PET '06*, Heidelberg: Springer-Verlag Acquisti, A. and J. Grossklags (2004), "Privacy Attitudes and Privacy Behavior", in J. Camp and R. Lewis (eds), *The Economics of Information Security*, Dordrecht: Kluwer.

Acquisti, A., L. John and G. Loewenstein (2009), "What is privacy worth?", presentation at workshop on Information Systems Economics (WISE 2009), Phoenix, 14-15 December 2009.

Aggarwal, C. and P. Yu (2008), *Privacy-Preserving Data Mining*, Heidelberg: Springer.

Almunia, J. (2012), "Competition and personal data protection", speech delivered at Privacy Platform event: Competition and Privacy in Markets of Data, Brussels, 26 November (http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm).

Alvaro, Alexander (2012). Lifecycle Data Protection Management. A contribution on how to adjust European data protection to the needs of the 21st century, 28.09.2012, (http://www.alexander-alvaro.de/wp-content/uploads/2012/10/Alexander-Alvaro-LIFECYCLE-DATA-PROTECTION-MANAGEMENT.pdf).

Baldwin, R., M. Cave and M. Lodge (2012), *Understanding Regulation: Theory, Strategy and Practice* (2nd ed.), Oxford: Oxford University Press.

Bates, B.J. (1988), "Information as an Economic Good and Sources of Individual and Social Value", in V. Mosco and J. Wasko (eds), *The Political Economy of Information*, Madison, WI: University of Wisconsin Press.

Beales, H. (2010), "The Value of Behavioral Targeting", Network Advertising Initiative. (http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf)

Berendt, B., O. Günther and S. Spiekermann (2005), "Privacy in e-Commerce: Stated Preferences vs. Actual Behavior", *Communications of the ACM*, Vol. 48, No. 4, pp. 101-106.

Beresford, A.R., D. Kübler and S. Preibusch (2012), "Unwillingness to Pay for Privacy: A field experiment", *Economics Letters*, Vol. 117, No. 1, pp. 25-27.

BCG (Boston Consulting Group) (2012), "The Value of Our Digital Identity", Liberty Global Policy Series, November (http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf).

Black, J., M. Lodge and M. Thatcher (eds) (2005), *Regulatory Innovation: A Comparative Analysis*, Cheltenham: Edward Elgar.

Boehme, R. (2012), presentation at the Workshop on the Economic Value of Personal Information, Amsterdam Privacy Conference, Amsterdam, 10 October.

Bonneau, J. and S. Preisbuch (2010), "The Privacy Jungle: On the Market for Data Protection in Social Networks", in T. Moore, C. Ioannidis and D. Pym (eds), *Economics of Information Security and Privacy*, New York: Springer.

Brandimarte, L., A. Acquisti and G. Loewenstein (2012), "Misplaced Confidences: Privacy and the Control Paradox", *Social Psychological and Personality Science*, published online on 9 August.

Brown, I. (2010), "Data protection: the new technical and political environment", *Computers & Law*, Vol. 20, No. 6, University of Oxford Institute, (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1548357).

Bygrave, L.A. (2008), "International Agreements to Protect Personal Data", in J.B. Rule and G. Greenleaf (eds), *Global Privacy Protection: The First Generation*, Cheltenham: Edward Elgar.

Carblanc, A. (2010), presentation at OECD Conference on the Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines, Jerusalem, 25-26 October.

Centre for European Policy Studies, Centre d'Etudes sur les Conflits and Vrije Universiteit Brussels (2011), "Towards a New EU Legal Framework for Data Protection and Privacy. Challenges, Principles and the Role of the European Parliament", Study for the European Parliament (http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=54351).

CEPS Digital Forum (2012), "Prospects of the Task Force on Online Personal Data Processing in the Context of the EU Data Protection Reform" (http://www.ceps.eu/files/Prosp_DF_TFDataProcessing.pdf).

Cohen, J. (2000), "Copyright and the Perfect Curve", *Vanderbilt Law Review*, Vol. 53, No. 6, pp. 1799-1819.

Compañó, R. and W. Lusoli (2010), "The Policy Maker's Anguish: regulating personal data behaviour between paradoxes and dilemmas", in T. Moore, C Ioannidis and D. Pym (eds), *Economics of Information Security and Privacy*, New York: Springer.

Costa, L. and Y. Poullet (2012), "'Privacy and the regulation of 2012", *Computer Law & Security Review*, Vol. 28, No. 3, pp. 251-378.

De Hert, P. and V. Papakonstantinou (2012), "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security* Review, Vol. 28, pp. 138-142.

Etro, F. (2013), Contribution, Conference on Computers, Privacy and Data Protection, Brussels, 24 January.

Evans, D. (2013), "Attention Rivalry among Online Platforms and its Implications for Antitrust Analysis", *Journal of Competition Law and Economic* (forthcoming).

Falque-Pierrotin, I. (2012), "What kind of European Protection for Personal Data?", Foundation Robert Schuman Policy Paper No. 250, 3 September (http://www.robert-schuman.eu/doc/questions_europe/qe-250-en.pdf).

Feintuck, M. (2010), "Regulatory Rationales Beyond the Economic: In Search of the Public Interest", in R. Baldwin, M. Cave and M. Lodge (eds), *The Oxford Handbook of Regulation*, Oxford: Oxford University Press.

Gervais, D. (2012), "Copyright, culture and the Cloud", in S. Pager and A. Candeub (eds), *Transnational Culture in the Internet Age*, Cheltenham: Edward Elgar.

Gilardi, F. (2005), "Evaluating independent regulators", in OECD (eds), *Designing Independent and Accountable Regulatory Authorities for High Quality Regulation*, proceedings of an Expert Meeting in London, 10-11 January 2005, pp. 101-125.

Goldfarb, A. and C.E. Tucker (2011), "Privacy Regulation and Online Advertising", *Management Science*, Vol. 57, No. 1, pp. 57-71.

Hardin, G. (1968), "The Tragedy of the Commons", *Science*, Vol. 162, pp. 1243-1248.

Heverly, R.A. (2003), "The Information Semicommons", *Berkeley Technology Law Journal*, Vol. 18, No. 4, pp. 1126-1189.

Hon, K., C. Millard and I. Walden (2011), "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", Queen Mary University of London, School of Law Legal Studies Research Paper No. 77/2011.

Kantor (2010), "Comparative Study of the Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments", study commissioned by the European Commission, Directorate-General Justice, Freedom and Security, 20 January, Brussels.

Koops, B.-J., R. Leenes and P. de Hert (eds) (2007), "Constitutional Rights and New Technologies. A Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States", Report commissioned by the Dutch Ministry of the Interior and Kingdom Relations, February (http://akgul.bilkent.edu.tr/crant-report-2007def.pdf).

Korff, D. (2010), "Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments. Working Paper No. 2", in Kantor (2010), Comparative Study of the Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments, study commissioned by the European Commission, Directorate-General Justice, Freedom and Security, 20 January.

———— (2012), "New challenges to data protection resulting from new technologies", presentation delivered at the 2nd meeting of the CEPS TF on Online Personal Data Processing in the Context of the EU Data Protection Reform, Brussels, 11 December.

Korobkin, R. (2003), "Bounded Rationality, Standard Form Contracts, and Unconscionability", *The University of Chicago Law Review*, Vol. 70, No. 4, pp. 1203-1295.

Kosta, E. (2013), "Consent in data protection: Lessons from the past, lessons for the future", presentation delivered at the 3rd meeting of the CEPS TF on Online Personal Data Processing in the Context of the EU Data Protection Reform, Brussels, 9 January.

Kroes, N. (2012), "Online privacy and online business: An update on Do Not Track", SPEECH/12/716 delivered at the Centre for European Policy Studies (CEPS), Brussels, 11 October.

Kuner, Ch. (2012a), "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *Bloomberg BNA Privacy and Security Law Report*, Vol. 6, February, pp. 1-15 (http://ssrn.com/abstract=2162781).

Kuner, Ch. (2012b), "Compliance, Risks and Management", presentation delivered at the 2nd meeting of the CEPS TF on Online Personal Data Processing in the Context of the EU Data Protection Reform, Brussels, 11 December.

Laudon, K.C. (1996), "Markets and Privacy", *Communication ACM*, Vol. 39, No. 9, pp. 92-104.

Leenes, R. (2013), "Cookies, profiling and the right to be let alone: Addressing the elephant in the room instead of talking about it?", presentation delivered at the 4th meeting of the CEPS TF on Online Personal Data Processing in the Context of the EU Data Protection Reform, Brussels, 22 January.

Lessig, L. (2006), *Code v. 2.0*, New York: Basic Books.

London Economics (2010), "Study on the economic benefits of privacy-enhancing technologies (PETs)", Final Report to the European Commission, July (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf).

Luchetta, G. (2013), "Is the Google Platform a Two-Sided Market?", *Journal of Competition Law and Economics*, (forthcoming).

Lynskey, O. (2013), "Propertisation of personal data in the European Union context", presentation at the 3rd meeting of the CEPS TF on Online Personal Data Processing in the Context of the EU Data Protection Reform, Brussels, 9 January.

Magnusson Sjoberg, C. (2007), "Chapter 6. Constitutional Rights and New Technologies in Sweden", in B.-J. Koops, R. Leenes and P. de Hert (eds) (2007), *Constitutional Rights and New Technologies. A Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States*, Report commissioned by the Dutch Ministry of the Interior and Kingdom Relations, February (http://akgul.bilkent.edu.tr/crant-report-2007def.pdf).

Majone, G. (2005), "Strategy and structure: The political economy of agency independence and accountability", in OECD (eds), *Designing Independent and Accountable Regulatory Authorities for High Quality Regulation*, Proceedings of an Expert Meeting in London, 10-11 January, pp. 126-155.

McDonald A.M. and L.F. Cranor (2008), "The Cost of Reading Privacy Policies", *I/S: A Journal of Law and Policy for the Information Society*, Vol. 4, No. 3, pp. 540-565.

Nicolaides, P. (1999), "Enlargement of the EU and Effective Implementation of Community Rules: An Integration-Based Approach", Working Paper 99/W/04, European Institute of Public Administration, Maastricht.

Nissenbaum, H. (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Palo Alto, CA: Stanford University Press.

———— (2011), "A Contextual Approach to Privacy Online", *Dædalus, the Journal of the American Academy of Arts & Sciences,* Vol. 4, Fall, pp. 32-48.

NIST (National Institute of Standards and Technology) (2011), "The NIST Definition of Cloud Computing", P. Mell and T. Grance for the US Department of Commerce, Special Publication 800-145, Washington, D.C. (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf).

Novotny, A. and S. Spiekermann (2012), "Personal Information Markets AND Privacy: A New Model to Solve the Controversy", paper presented at the Technology Forum Alpbach (http://www.wu.ac.at/ec/wi2013_pdmarkets_v13.pdf).

OECD (Organisation for Economic Co-operation and Development) (1980), *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*, Paris: OECD Publishing.

———— (2005), *Guiding principles for regulatory policy and performance*, Paris: OECD Publishing.

———— (2011), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, Paris: OECD Publishing.

Ohm, P. (2010), "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review*, Vol. 57, pp. 1701-1777.

Pew (Pew Research Center) (2012), "Privacy and Data Management on Mobile Devices" (http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx).

Ponemon Institute (2011) "The True Cost of Compliance – A Benchmark Study of Multinational Organisations", Research Report (http://www.tripwire.com/ponemon-cost-ofcompliance/pressKit/True_Cost_of_Compliance_Report.pdf).

Posner R. (1981), "The Economics of Privacy", *American Economic Review*, Vol. 71, No. 2, pp. 405-409.

Poullet, Y. and S. Gutwirth (2008), "The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'?", in V.P. Asinari and P. Palazzi (eds), *Défis du droit à la protection de la vie privée – Challenges of privacy and data protection law*, Brussels: Bruylant, pp. 570-610.

Purtova, N. (2012), *Property Rights in Personal Data: A European Perspective*, Alphen a.d.R.: WoltersKluwer.

RAND (2009), "Review of the European Data Protection Directive", RAND Corporation Technical Report Series (http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf).

Reed, C. (2010), "Information 'Ownership' in the Cloud", Queen Mary School of Law Legal Studies Research Paper No. 45/2010 (http://ssrn.com/abstract=1562461)

Renda, A. (2008), "Analisi Economica del Diritto", *pro manuscriptu* (on file with the authors).

Rochet, J.-C. and J. Tirole (2003), "Platform Competition in Two-Sided Markets", *Journal of the European Economic Association,* Vol. 1, No. 4, pp. 990-1029.

Rockelmann, A., J. Budd and M. Vorisek (2011), "Data Breach Notifications in the EU", study for the European Network and Information Security Agency, 13 January.

Rule, J.B. and G. Greenleaf (eds) (2010), *Global Privacy Protection: The First Generation,* Cheltenham: Edward Elgar.

Samuelson, P. (2000), "Privacy As Intellectual Property?", *Stanford Law Review*, Vol. 52, No. 6, pp. 1125-1173.

Schwartz, P.M. (2000), "Beyond Lessig Code for Internet Privacy: Cyberspace Filters, Privacy-Control and Fair Information Practices", *Wisconsin Law Review*, pp. 743-788.

Spiekermann, S., J. Korunovska and C. Bauer (2012), "Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy", 33rd International Conference on Information System, Orlando, Fl., 16-19 December.

Stigler, G. (1980), "An introduction to privacy in economics and politics", *Journal of Legal Studies*, Vol. 9, No. 4, pp. 623-644.

Tirtea, R. (2013), "ENISA activities in the area of privacy and data protection", presentation delivered at the 3rd meeting of the CEPS TF on Online Personal Data Processing in the Context of the EU Data Protection Reform, Brussels, 9 January.

Traple Konarski Podrecki and Partners and European Legal Studies Institute (2012), "Reforming the Data Protection Package", Study for the European Parliament (http://www.europarl.europa.eu/document/activities/cont/201209/20120928ATT52488/20120928ATT52488EN.pdf).

UK ICO (2012), "Initial analysis of the European Commission's proposals for a revised data protection legislative framework", 27 February (http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Research_and_reports/ico_initial_analysis_of_revised_eu_dp_legislative_proposals.ashx).

Van der Sloot, B. and F.J. Zuiderveen Borgesius (2012), "Google and Personal Data Protection", in A. Lopez-Tarruella (ed.), *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, The Hague: T.M.C. Asher Press, pp. 75-111.

Varian, H. (1996), "Economic Aspect of Personal Privacy", in US Department of Commerce, *Privacy and Self-Regulation in the Information Age*, Washington, D.C.

Veljanovki, C. (2010), "Economic Approaches to Regulation", in R. Baldwin, M. Cave and M. Lodge (eds), *The Oxford Handbook of Regulation*, Oxford: Oxford University Press.

Voigt, P. (2010), presentation at the Workshop on the Economic Value of Personal Information, Amsterdam Privacy Conference, Amsterdam 10 October.

WEF (World Economic Forum) (2011), "Advancing Cloud Computing: What To Do Now? – Priorities for Industry and Governments" (http://www3.weforum.org/docs/WEF_IT_AdvancedCloudComputing_Report_2011.pdf).

———— (2012), "Rethinking Personal Data: Strengthening Trust" (http://www.weforum.org/reports/rethinking-personal-data-strengthening-trust).

Whitehouse, The (2012), "Consumer Data Privacy in a Networked World. A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", February, Washington, D.C.

Winton, A. and N. Cohen (2012), "Proposed EU framework – Online Advertising, E-Commerce and Social Media", *Computer and Telecommunications Law Review*, Vol. 18, No. 4, pp. 97-101.

Zittrain, Jonathan (2008), *The future of the Internet and How to Stop It*, New Haven, CT: Yale University Press.

Official Documents

Council of Europe (1981), "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.: 108)", adopted in Strasbourg, 28 January (http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm).

Council of Europe (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted on 23 November.

ENISA (European Network and Information Security Network) (2011a), "Privacy, Accountability and Trust – Challenges and Opportunities", 18 February (http://www.enisa.europa.eu/act/it/library/deliverables/pat-study).

———— (2011b), Survey of Accountability, Trust, Consent, Tracking, Security and Privacy Mechanisms in Online Environments, 31 January (http://www.enisa.europa.eu/act/it/library/deliverables/survey-pat).

———— (2012a), Study on Monetising Privacy: An Economic Model for Pricing Personal Information, 28 February (http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy/at_download/fullReport).

———— (2012b), Study on data collection and storage in the EU, 8 February (http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection/at_download/fullReport).

———— (2012c) "Privacy considerations of online behavioural tracking", Report, 19 October (http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking/at_download/fullReport).

European Commission (2003), First report on the implementation of the data protection Directive (95/46/EC), COM(2003)265, 15 May (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF).

———— (2007a), Communication 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, 7 March (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:EN:PDF).

———— (2007b), Communication to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007)228, 2 May (http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf).

———— (2010a), Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, "Smart Regulation in the European Union", COM(2010)543, 8 October.

———— (2010b), Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, "A digital agenda for Europe", COM(2010)245, 26 August (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF).

———— (2010c), Communication 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, 4 November (http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf).

———— (2011), Special Eurobarometer (EB) 359, "Attitudes on Data Protection and Electronic Identity in the European Union", June (http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf).

———— (2012a), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012)11, 25 January (http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf).

———— (2012b), Impact Assessment. Accompanying the Documents Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC(2012)72, 25 January (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012SC0072:EN:NOT).

European Parliament (2011), Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union, P7_TA(2011)0323, 2011/2025(INI) (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2011-0323+0+DOC+PDF+V0//EN).

Eurostat (2009), "Internet usage in 2009 - Households and Individuals", Data in Focus 46/2009 (http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-09-046/EN/KS-QA-09-046-EN.PDF).

FRA (EU Agency for Fundamental Rights) (2010), "Data Protection in the European Union: The role of National Data Protection Authorities" (http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf).

———— (2012), Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, 1 October (http://fra.europa.eu/sites/default/files/fra-opinion-data-protection-oct-2012.pdf).

LIBE (European Parliament Committee on Civil Liberties, Justice and Home Affairs) (2012), Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), Rapporteur: Jan Philipp Albrecht.

WP29 (Art. 29 Working Party) (2007), Opinion 04/2007 on the Concept of Personal Data, WP136 (01248/07/EN), 20 June.

———— (2011), Opinion 15/2011 on the definition of consent, WP187 (01197/11/EN), 13 July.

———— (2012), Opinion 04/2012 on Cookie Consent Exemption, WP196 (01037/12/EN), adopted on 7 June.

———— (2013), Statement of the Working Party on current discussions regarding the data protection reform package, 27 February (http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_reform_package_en.pdf).

Legislation

Charter of Fundamental Rights of the European Union, (2000/C 364/01), OJ C 326, 26.10.2012, pp. 391-407.

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, OJ L 281, 23.11.1995, pp. 31-50.

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 (Directive on privacy and electronic communications), OJ L 201, 31.07.2002 pp. 37-47.

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, OJ L 105, 13.04.2006 pp. 54-63.

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, OJ L 376, 27.12.2006, pp. 36-68.

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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, OJ L 8, 12/01/2001, pp. 1-22.

Case law

Court of Justice of the European Union, Judgment of 6 November 2003 in Case C-518/07, *Lindqivst* (ECR 2003, pp. I-12971).

Court of Justice of the European Union, Judgment of 29 January 2008 in Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU* (ECR 2008, pp. I-00271).

Court of Justice of the European Union, Judgment of 9 March 2010 in Case C-518/07, *European Commission v. Germany* (ECR 2010, pp. I-01885).

Court of Justice of the European Union, Judgment of 9 November 2010 in Joint Cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert v. Land Hessen* (ECR 2010, pp. I-11063).

Court of Justice of the European Union, Judgment of 16 October 2012 in Case C-614/10, *European Commission v. Republic of Austria* (not yet published).

ANNEX I

List of Task Force Participants (*to be completed*)

Afore Consulting

Edelman

Facebook

Fleishman Hilard

Intuit

Italian Privacy Institute

Microsoft

Orange

Samsung

TechFreedom

Telecom Italia

Telefonica

Ziggo

ANNEX II

Invited Guests & Speakers

Agnieszka Wodecka, DG Communications, Content and Technology, European Commission

Raffaella D'Alessandro, IBM Global Technology Services, Italy

Joe McNamee, Executive Director, European Digital Rights

Bertin Martens, Institute for Prospective Technological Studies, Joint Research Centre of the European Commission

Chris Sherwood, Director for Public Policy, Yahoo!

James Philip Gray, DG Communications, Content and Technology, European Commission

Machiel Bolhuis, Senior Regulatory and Public Affairs Officer, Ziggo

Prof. Douwe Korff, London Metropolitan University

Christopher Kuner, Senior of Counsel, Wilson Sonsini, and Cambridge University

Rodica Tirtea, European Network and Information Security Agency

René Lamsfuss, Vice President Market Governance & Data Strategy Europe, Nielsen

Luca Bolognini, President, Italian Institute for Privacy and ICT Legal Consulting law firm

Eleni Kosta, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University

Orla Lynskey, London School of Economics

Thomas Boué, Director, Government Affairs, EMEA, BSA | The Software Alliance

Prof. Ronald Leenes, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University

Jean Gonié, Director of Privacy, EMEA Policy, Microsoft

Paul Nemitz, Director, DG Justice, European Commission

Anna Fielder, Trustee and Company Secretary, Privacy International

Grégoire Polad, EU Spokesperson for the Association for Competitive Technology, SVP FTI Consulting

Annex III

Abbreviations

AFSJ	Area of Freedom, Security and Justice
API	Application Programming Interface
BCR	Binding Corporate Rule
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DNT	Do Not Track (Standard)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
ENISA	European Network and Information Security Agency
FRA	Fundamental Rights Agency
ICT	Information and Communication Technologies
IaaS	Infrastructure as a Service
MEP	Member of the European Parliament
MSME	Micro-,Small- and Medium-sized Enterprises
OBA	Online Behavioural Advertising
OTT	Over-The-Top (Players)
PaaS	Platform as a Service
PET	Privacy Enhancing Technologies
SaaS	Software as a Service
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

ABOUT CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today,
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process, and
- Provide a regular flow of authoritative publications offering policy analysis and recommendations,

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts,
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach,
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals.

Programme Structure

In-house Research Programmes

Economic and Social Welfare Policies
Financial Institutions and Markets
Energy and Climate Change
EU Foreign, Security and Neighbourhood Policy
Justice and Home Affairs
Politics and Institutions
Regulatory Affairs
Agricultural and Rural Policy

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)

Research Networks organised by CEPS

European Climate Platform (ECP)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)