EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Economic and Monetary Affairs

Employment and Social Affairs

Environment, Public Health and Food Safety

Industry, Research and Energy

Internal Market and Consumer Protection

# Reforming the Data Protection Package

STUDY

EN

2012

Reforming the Data Protection Package


DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY

# Reforming the Data Protection Package

## STUDY

**Abstract**

This study aims to provide background information and advice on priority measures and actions to be undertaken in the reform of the data protection package. The study is based upon four aspects: mapping new technologies and services; analysing the internal market dimension; strengthening the rights of the consumer; and international data transfers.

IP/A/IMCO/ST/2012-02
PE 492.431

September 2012
EN

This document was requested by the European Parliament's Committee on Internal Market and Consumer Protection.

## AUTHORS

Xawery Konarski (Advocate Partner, TrapleKonarskiPodrecki and Partners, Cracow)
Damian Karwala (Legal Advisor, TrapleKonarskiPodrecki and Partners, Cracow)
Prof. Dr. Hans Schulte-Nölke (European Legal Studies Institute, Osnabrück)
Shaun Charlton (European Legal Studies Institute, Osnabrück)

## RESPONSIBLE ADMINISTRATOR

Mariusz Maciejewski
Policy Department Economic and Scientific Policy
European Parliament
B-1047 Brussels
E-mail: mariusz.maciejewski@europarl.europa.eu

## LINGUISTIC VERSIONS

Original: EN

## ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
Poldep-Economy-Science@europarl.europa.eu

Manuscript completed in September 2012.


This document is available on the Internet at:
http://www.europarl.europa.eu/studies

## DISCLAIMER

# CONTENTS

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **The 1995 Directive** | 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 |
| **Art** | Article |
| **BSRs** | Binding Corporate Rules |
| **CCTV** | Closed circuit television |
| **DPA** | Data Protection Authority |
| **EU** | European Union |
| **ICO** | UK Data Protection Authority, the Information Commissioner's Office |
| **ID** | Identification |
| **IP addresses** | Internet Protocol addresses |
| **IT** | Information Technology |
| **PIPEDA** | Personal Information Protection and Electronic Documents Act |
| **The Proposal** | Proposal for a Regulation of the European Parliament of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data' COM(2012) 11 |
| **PSI Directive** | Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information |
| **RFID** | Radio-frequency identification |
| **SMEs** | Small and Medium Sized Businesses |
| **UK** | United Kingdom |
| **WiFi** | Wireless fidelity, a local area network that uses high frequency radio signals to transmit and receive data |

# TABLE OF DEFINITIONS

| | |
|---|---|
| **Data controller** | Natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data |
| **Data processor** | Natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller |
| **Data subject** | The natural person capable of being identified whose data is being held by another. |
| **Personal data profiling** | Means any information relating to an identifiable natural person. The process by which information collected about identifiable persons is analysed, often through the use of complicated algorithms, in order to discover patterns of behaviour and preferences |
| **Pseudonymisation** | The process of disguising identities on a temporary basis by using correspondence list for identities and pseudonyms for individuals |
| **Purpose limitation principle** | Data should only be processed for specfic, specified purposes |
| **Technological neutrality** | Technological neutrality means that legislation should define the objectives to be achieved, and should neither impose, nor discriminate in favour of, the use of a particular type of technology to achieve those objectives |

# EXECUTIVE SUMMARY

The reform of the data protection package[1] promises both to improve the internal market dimension and consumer protection. There are, however, many issues which need to be addressed. The following paragraphs contain key findings and priority recommendations. The conclusions and recommendations can be found in full at the end of each respective chapter.

## Mapping new technologies

The vastness of the available business models, new technologies and services – including those of great importance in the context of e-commerce and Internal Market –have resulted in a spectrum of data protection issues ranging from those which hardly touch upon data protection to others which could have potentially devastating consequences for the use of sensitive data. Presented examples of new technologies with specific relevance to data protection include the most important developments in the field, like e.g., geo-location services and the actions of a few of the biggest market leaders, such as Google, to collate and assimilate data from all of the various sources which have been previously mentioned. Some other developments include: smart metering, face recognition technologies, social networking services, online gaming, scanning electronic emails, or RFID technologies. Companies and governments are using these technologies often without the individuals being aware of the impact they may have.

The analysis of the Proposal, in the context of the regulatory responses to new technologies, while improving and streamlining some concepts (e.g., definition of "purely personal or household activities", or purpose limitation principle), has shown that there is still some work to be done in this context, including:

- The proposed definition of "personal data" requires refining and clarifying as follows:
    - its further streamlining (e.g., in order to properly use the phrase "means likely reasonably to be used");
    - preservation of the "relative approach", otherwise it could result in significant extension of the definition of "personal data", and thus expansion of the obligations of entities involved in the processing of different types of information;
    - explicit qualification of online identifiers, because in the context of modern technologies, in particular those which are Internet-related, it is of fundamental importance how a variety of online identifiers, such as IP addresses or cookies, will be qualified. The Proposal is currently far from providing a clear qualification in this regard.

[1] 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 final 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, COM(2012) 10 final, although this study is restricted to an analysis of the Regulation as explained below.

- The reformed Proposal should encourage entities processing personal data to anonymise personal information, which allows data to be processed without reference to information which could identify the data subject. Given the broad definition of "personal data", adopted in EU law and maintained by the Package, anonymisation allows for the implementation of numerous projects that involve personal information without adversely affecting the privacy of natural persons (e.g. in the context of marketing activities or making certain information available online). This, further legislative work should pay greater attention to the issues of anonymisation and pseudonymisation of data, in particular in terms of:
    - creating a system of incentives for initiation of those processes;
    - determining the conditions for effective anonymisation, including the requirement to obtain consent to anonymise data or requirements to secure the data;
    - clarifying the requirements for data pseudonymisation, in conjunction with the "benefits" that may be associated with that process (e.g., exemption from specific legal obligations or facilitation of certain elements related to such data, for example as regards measures based on profiling).

- Given the role that is played in the context of anonymisation and pseudonymisation by certain technological conditions, various soft-law instruments and initiatives may be of relevance here, including in particular codes of conduct, and should be taken into account when reforming the Package.
- In terms of defining the term "data controller", there are doubts about the added provision that data controllers also determine the "conditions" of data processing. It seems that the definition of "data controller" should be limited to determining the "purposes" of data processing. Such a solution seems to be less revolutionary, permitting the developments generated on the basis of the present definition to be taken into account, in particular those of the Article 29 Working Party.
- The Proposal should be refined as regards precise division and determination of the obligations and responsibilities of the data controller and data processor. Due to the fact that data processors generally perform only tasks assigned to them by the data controller, the question arises about the validity of the adoption of solutions according to which the data controller may expect the support of the processor in satisfying such obligations as the obligation to provide information, to conduct data protection impact assessment, etc.
- The so-called "household exception" should be limited to the condition of "exclusively personal or household activity". Any possible additional restrictions of the "household exception" should be adopted with regard to their impact on other values, in particular freedom of expression, which is especially important in the online community.
- Profiling operations ("measures based on profiling") are being dealt with rigorously in the proposed Regulation, with much wider scope of application and many restrictions. This important legal issues, highly "technology sensitive", and the underlying regulatory approach require fundamental rethinking, taking into account the broader context, the differences in "profiling" in the different sectors of the economy or legal relations, as well as taking into account the consequences of overly restrictive regulation in this area. Any decisions in this context – for the most part – are of political nature, but should be based on a much more thorough analysis than that presented by the Commission.

- Detailed analysis and decision (mostly political) is required as regards the issue of permissible further processing of data for purposes incompatible with the one for which the personal data have been collected, also on the legal basis of legitimate interest pursued by the controller. In this context, additional precision would also be required in the case of the notion of "compatible use".

Additionally, due to continuing technological development reflected in the wording of the Proposal as well as in the context of the broad powers available to the Commission, it would be highly recommendable to expressly define the technological neutrality principle in the text of the Regulation. Such a principle would be of great importance not only for the EU legislator during work on the Package and its reform, but also after the adoption of the Regulation, in particular for the Commission, in the context of its broad powers to adopt secondary legislation. The Package, as well as discussion concerning it, should – in the opinion of the authors of this study – also concentrate on the issue of re-use of public information, since currently there are serious obstacles with regard to such re-use in the light of data protection regulation.

### Internal market dimension

The Proposal has a high potential for improving the internal market and creating a level-playing field for all businesses active in the EU (including businesses which are not established within the EU). Key elements are:

- the shift of the legislative instrument (from directive to regulation);
- the 'one-stop shop' principle regarding the competent supervisory authority in cross-border cases;
- the marketplace principle (which makes EU data protection standards also applicable to businesses based outside the EU, if they are active within the EU);
- the general principle of accountability (which replaces the obligation of data controllers or processors to make a general notification about their processing to their national regulator: *ex-post* supervision is being replaced by instruments that increase the probability of *ex-ante* compliance). The principle of accountability includes, *inter alia,* the duties:
    - to appoint a data protection officer;
    - to adopt mutable policies and measures to demonstrate compliance;
    - to carry out data protection impact assessments;
    - to install systems of "privacy by design" and "privacy by default".

Possible improvements regarding the effect on the internal market include, *inter alia*:

- the strengthening of the tools for a regular monitoring of the actual implementation and enforcement in all Member States (also in order to reduce incentives for shopping for a more 'business friendly' jurisdiction);
- the creation of EU-wide databases on legal practice in order to ensure uniform application;
- the refinement of the provisions on the territorial scope and the one-stop-shop principle;
- the further elaboration of concrete examples for privacy 'by design' and 'by default' (e.g. anonymisation and pseudonymisation of data, pre-settings of browsers).

### Strengthening the rights of the consumer

As for strengthening the rights of consumers, it seems that the balance of competing interests such as consumer awareness, autonomy, protection and the internal market has been struck through the promotion of transparency. Consumers are not wholly prevented from revealing data, as could be the case under a very strict data protection regime, however, the reform seeks to provide the consumer with the tools to know what data is transferred and how it is used.

Improvements have been made especially in relation to the notion of consent as one of the legitimating factors for the processing of personal data, the right to be forgotten and to erasure and the right against profiling. A new right of portability has been created which is very encouraging. Although in general clarity has been improved there remain many areas of the Proposal which require further refinement and clarification. This is particularly the case with behavioural advertising, the practicalities of implementation particularly in relation to the right of portability. This makes it difficult to make a full evaluation as it is sometimes not clear what is intended by the Proposal. This ambiguity must be resolved and the majority of recommendations are therefore mainly directed towards calls for further clarity in the Proposal.

The following elements require attention:

- Further clarification as to what constitutes data which is 'manifestly made public' which operates to dispense processors of sensitive personal data from seeking the consent of the data subject;
- Clarify in article 17 that once informed by a data controller that a data subject has exercised the right of erasure, the data held by the third party data controller must also be deleted;
- From the perspective of strengthening the rights of consumers, behavioural advertising should be included in the legal characterisation of profiling;
- Clarify whether the right to portability in article 18 moves the home of the data or whether the data merely finds a second home;
- A key political decision needs to be taken in article 18 on whether the harmonisation or adoption of 'commonly used formats' is compulsory for the creation of a true right of portability.

To take account of the realities of the business model upon which many processors of personal data are based, that is to say that consumers pay for seemingly "free" services with their personal data, there should be express mention in the preamble that the regulation does not deal with or prejudice remedies of non-performance which would be otherwise open to the consumer.

### International data transfers

International data transfers are one of the main aspects that require review and improvement when reforming the current EU data protection regime and reforming the Data Protection Package, as well, especially in the context of such phenomena like cloud computing. Cloud computing solutions create special problems for the current regulation of cross-border data transfers, which is basically based on protecting data in a given physical infrastructure in a defined location. This is one of the reasons why it is necessary to implement new and streamlined legal instruments in the field. Some of them have been proposed within the Package, and may better serve the main purposes: on the one hand, data controllers (EU-based) should not be relieved of their responsibilities with respect to data processing and – on the other hand – the cloud providers (especially those from "third countries") should be encouraged to protect the data at the highest level, "adequate" to the EU-level.

While some developments may be acclaimed in this context (e.g., the possibility of recognising particular territory or processing sectors as "adequate"; attempts to "centralise" the process of adequacy assessment; general rule under which transfers based on standard data protection clauses or BCRs do not require any further authorisation; the explicit recognition the BCRs), there is, however, room for further improvement, to better serve the basic purposes. In order to improve the international data transfers regime, and to reform the Package in this regard, it would be recommended, especially, to:

- Further refine the Commission's adequacy decisions scheme, in particular by introducing into the preamble to the Regulation of a more precise definition of the scope of the term "processing sectors";
- The "logistics" of how adequacy decisions are to be issued and used under the Proposal need to be addressed, in order to make them a tool that will be more frequently used in practice. Especially the following should be defined:
    - rules of conducting the assessment, including its initiation, the involvement of the national supervisory authorities and the European Data Protection Board;
    - rules of further "handling" of adequacy decisions, in particular in the context of the requirement to carry out periodic assessments;
    - increased financial and organisational support by the Commission and the authorities involved would also be required in this regard.
- Explicitly define in the Package the consequences of the so-called negative adequacy decisions issued by the Commission (the so-called "black list"), i.e. whether in such case the transfer of personal data to a 'black-listed' third country is totally prohibited or allowed under some conditions;
- The rule under which any transfer based on standard data protection clauses or Binding Corporate Rules does not require any further authorisation should apply to the so-called 'ad hoc clauses', as well;
- Explicitly emphasise within the Package the possibility of using standard data protection clauses also by data processors ('processor-to-(sub)processors model clauses');
- Delete Article 42(5) of the Proposal (except for the last sentence), which provides for the possibility of basing data transfers on non-binding instruments (the reference in Article 34 will require to be changed accordingly);

- Further increase the flexibility of the regulation regarding Binding Corporate Rules, which requires, in particular:
    - to specify whether that institution could be limited to a part of a group of undertakings;
    - to introduce of facilitation as regards adoption and approval of Binding Corporate Rules by smaller entities, especially SMEs.
- Explicitly define the basic and crucial, in this regard, term of “data transfer”.

The Regulation should also explicitly emphasise that entities that chose to transfer data to “third countries” are still accountable to ensure that personal data remain protected when transferred to such countries. Such a solution requires, however, further in-depth analysis, especially as to how far the responsibility of data exporters, if any, should stretch in the context of such instruments as Binding Corporate Rules and other tools facilitating trans-border data flows.

The new legal framework should also focus much more on risk assessment by the data controllers/processors before the data transfer takes place. Some other mechanisms, like the development of an accreditation system or the dedicated Cloud Safe Harbour Programme, as well as self-regulatory instruments and industry standards, could also be taken into account when reforming the current European data transfer regulation. The new legal instrument concerning cross-border data flows should also focus much more on international standards issues.

# INTRODUCTION

## Background

The current European regulatory framework on data protection is primarily based upon Directive 95/46/EC.[2] This directive sets out the basic principles in relation to data protection. The directive is, however, supplemented by other directives in more specific areas such as Directive 2003/98/EC on the re-use of public sector information,[3] Directive 2002/58/EC dealing with inter alia cookies in the context of e-privacy[4] and Directive 2009/136/EC on citizens' rights.[5]

The European Commission is currently in the process of reviewing the whole of the EU legal framework on the protection of personal data with an aim to:

- modernise the EU legal system for the protection of personal data, in particular to meet the challenges resulting from globalisation and the use of new technologies;
- strengthen individuals' rights, and at the same time reduce administrative formalities to ensure a unhindered flow of personal data within the EU and beyond;
- improve the clarity and coherence of the EU rules for personal data protection and achieve a consistent and effective implementation and application of the fundamental right to the protection of personal data in all areas of the Union's activities.

Responding to the European Commission's Communication[6] on 6 July 2011 the European Parliament adopted a resolution on a comprehensive approach to personal data protection in the European Union.[7] On 25 January 2012, the European Commission presented proposals of a new regulation[8] and directive[9] on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

---

2 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.

3 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.

4 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).

5 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

6 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', COM(2010) 609 final.

7 Personal data protection in the European Union. European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)).

8 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 final; hereinafter referred to also as "General Regulation".

9 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, COM(2012) 10 final.

## Limitations

First of all, it is necessary to note that the Proposal consists of two legal instruments, a directive and a regulation. The objectives of these two legal instruments are very different. The proposed directive is restricted to the 'processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.'[10] The proposed directive treats a very specific use of personal data – its exchange between Member States in the area of crime. Since, the directive does not affect the rights of EU citizens in their quality as consumers, nor does it affect the internal market, it will not be treated in this Study. The proposed regulation, on the other hand, is of a more general nature covering the 'processing of personal data and rules relating to the free movement of personal data.'[11] It is therefore this part of the proposal which will have the greatest effect upon the internal market and the rights of consumers. As a result, only the proposed regulation will be discussed in this Study and all references to "the Proposal" refer to the proposed General Data Protection Regulation.

Due to the vastness of the field, this Study does not profess to be comprehensive, but instead seeks to focus on some of the most important aspects of the Proposal made by the Commission.

## Aims

This Study aims to provide background information and advice for the Members of the Committee on Internal Market and Consumer Protection on priority measures and actions to be undertaken in the reform of the data protection package. The Study is based upon four aspects: mapping new technologies and services which impact on data protection; analysing the internal market dimension; strengthening the rights of the consumer in the area of data protection; and international data transfers discussing the benefits and threats as well as impact on European consumers and businesses.

Reform of the Data Protection Package should take into account modern technologies while ensuring a very high level of protection in order to increase legal certainty, consistent levels of privacy in order to boost e-commerce while ensuring the users' trust. This reform should be focused, among other factors, on facilitation of development of Digital Single Market and consumer protection.

Within the Study actual legal as well as practical (business) discussion has been used, together with achievements of legal doctrine and, when appropriate, relevant case law. Each of the four chapters are summarised with main findings and recommendations with the aim to present the priority measures and actions to be undertaken in the reform of the data protection package.

[10] Article 1, 'Proposal for a Directive' COM(2012) 10.
[11] Article 1, 'Proposal for a Regulation' COM(2012) 11.

# 1. MAPPING NEW TECHNOLOGIES AND SERVICES WHICH IMPACT ON DATA PROTECTION

First chapter is divided into two parts:

- In the first part, **new technologies with specific relevance to data protection** will be briefly presented, in order to provide for an insight of the most important developments in the field, like e.g., geo-location services and the actions of a few of the biggest market leaders, such as Google, to collate and assimilate data from all of the various sources which have been previously mentioned. Newer developments that will be also presented include smart metering, which has been employed successfully by the energy industry,[12] face recognition technologies, social networking services, or RFID technologies;
- In the second part, **the regulatory responses to new technologies in the Proposal** will be dealt with. Based on the analysis of new technologies, including the responses of some of the Data Protection Authorities and legal as well as practical discussion within the EU, the following legal issues which are "technologically sensitive" will be discussed and assessed with some proposals and recommendations as how to reform the Proposal, i.e.:
    1. Definition of "personal data"
    2. Data anonymisation and pseudonymisation
    3. Actors involved: "data controllers" and "data processors"
    4. "Household exception"
    5. Measures based on 'profiling'
    6. Purpose limitation principle and further processing.

Due to their ever growing importance – in the context of new technologies – two further legal issues will be also dealt with, i.e. principle of technological neutrality and re-use of public information.

## 1.1. New technologies with specific relevance for data protection

The plethora of new technologies, services and social media which provide exchange of information services can be classified according to their function. Several market leaders, such as Google and Facebook, have infiltrated most, if not all of these sub-markets. These general categories, including examples from each, are:

- **publishing:** wikipedia, wikia, twitter, wetpaint, over-blog etc.
- **sharing:** youtube, daily motion, deezer, flickr, vimeo, digg, slidesshare, iLike, scribd etc.
- **discussing:** phpbb, gravity, disqus, quora, aardvark, 4chan, IntenseDebate, Mahalo etc.
- **commerce:** e-shops, e-banking, e-insurance, online brokers, e-payment services;
- **geo-location:** Yelp.inc, Whrrl, booyah, mig33, eventful, plancast, socializr etc.

[12] Dutch Data Protection Authority (College beschermingpersoonsgegevens, CBP), see further 3.2.3 and information on MiData.

- **networking:** xing', ning, mylife, plaxo, orkut, myspace, copainsdavant, linkedin, hyves, tagged, hi5, viadeo, badoo, KickApps etc.
- **games:** zynga, pogo, harbo, playdom, playfish, ngmoco:), playfirst etc.

The vastness of the available business models, new technologies and services have resulted in a spectrum of data protection issues ranging from those which hardly touch upon data protection to others which could have very serious or even potentially devastating consequences for the use of personal data.

### 1.1.1. Geo-location services (including mobile)

New technologies based upon the localisation of consumers may provide distinct benefits; however, there are often corresponding issues of data protection and privacy. On the internet, location services include Yelp.inc and Whrrl which combine information on where the user can find a particular service such as a restaurant, or a point of interest with reviews on the quality of the various possibilities within a certain geographical location. Others include Eventful of which the particularity is that users can declare their 'demand' in a particular location for an event or performance, such as a concert by their favourite artist. The idea is that sufficient demand will encourage the artist or organisation to supply. Other geo-social networking models allow users to see where their friends are located and what they are doing in real time through maps on mobile phones such as the iPhone, devices with Google's Android system or Blackberry. Non-internet based location technologies, widely used, include: speed safety cameras and radio-frequency identification (RFID). The former are used to identify cars which exceed the speed limit, and through identification of the car also its owner. The latter is effectively a tracking device which can be used on toll roads, for example, for the automatic recognition of the driver to bill for the use of the road. Another example, of a strictly private law nature, is tracking devices woven into clothing as an anti-theft device but which continue to function months after purchase (see also 1.1.7 below). Both of these non-internet based new technologies impact on data protection, since information on the geographical location of persons is gathered.

The most important data protection aspects, in the context of such phenomenon, include: the concept of "personal data" and its meaning, the anonymisation and pseudonymisation of data and the purpose limitation principle or profiling.[13] Their importance can be well illustrated by an interesting case investigated by the Dutch DPA.[14] In this case, TomTom gathered geolocation data from users of satellite navigation devices used in vehicles. The data was obtained both from the devices operating offline (i.e. requiring no Internet access) and devices operating online (all types of "LIVE" services, which use online connections with TomTom servers). In the devices, the geolocation data was stored as encrypted. In the opinion of the authority, however, this did not mean that TomTom was unable to decrypt the data relatively easily and link it to such data as the user's e-mail address or surname, which TomTom also had in its possession (and, as a result, to treat them as personal data). The data could then be made available to external entities, such as airports, for marketing purposes (e.g., to identify the geographical area from which the people using the airport come from). All these aspects demonstrate, e.g., that data of users of various geolocation services – even sensitive data – could be used for different purposes, especially those not notified to the data subjects at the moment the data have been gathered.

---

[13] Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices', WP 185 (16.5.2011).

[14] Report of findings. Official investigation by the CBP in to the processing of geolocation data by TomTom N.V.', available at: http://www.dutchdpa.nl/downloads_overig/en_pb_20120112_investigation-tomtom.pdf

### 1.1.2. Assimilation of data from different sources

Other situations are becoming increasingly frequent in which data from different sources is being assimilated and further processed. A particularly well-known case is Google's practices of assimilating user data obtained from various Google' services used by the users of these services. This allows, for example, for more and more advanced marketing activities suited to users' behaviour. For example, a person using a smartphone featuring the Android system can receive, as part of the YouTube service, advertisements related to the user's phone use activity (e.g. phone call times and dates) or location data. Thanks to such practices, Google offers users, for example, the possibility to automatically fill in a user's diary when a message sent through the Gmail electronic mail service contains the word 'meeting' (which requires filtering messages) or, for example, the possibility of using a user's Gmail contact list to automatically invite people to work on a document using Google Docs.

The case of assimilating data from different sources became well known in connection with changes to Google's Privacy Policies, in early 2012, and is currently being scrutinised by the French DPA, since it raises many doubts in the privacy context.[15] Besides, the modified (simplified) policies of Google arouse some other doubts, e.g. within the context of delivering precise information on the purposes and scope of data processing or the possible data recipient, as part of Google's different services. The information obligation is even more important particularly within the context of assimilating user data from different services without the users being aware of this taking place, and the Package – rightly – pays great attention to transparency principle and information obligations.

### 1.1.3. Cloud computing

One of the fastest growing technical phenomenon, broadly defined as 'cloud computing' (i.e. on-demand access to various computing resources),[16] could be beneficial for businesses and their client as well as consumers (due to, e.g., cost savings, greater competitiveness of IT industry) and, at the same time, creates new risks, also in the area of privacy and data protection. The most common models of cloud computing use 'virtualisation' and concentrate data from various resources (clients, consumers) on a common cloud infrastructure, which poses threats to the confidentiality and privacy of data. Security measures and transparency, especially in their negative aspects (i.e., lack of security and transparency) are also of great importance, and prevent many entities from using cloud services. There are also ambiguities as to the role of the cloud computing providers, who – in some cases – can be treated not only as pure data processors, but also as data controllers, given their impact on how the data is being processed 'in the cloud'.

[15] French Data Protection Authority (Commission nationale de l'informatique et des libertés, CNIL), 'Google's new privacy policy raises deep concerns about data protection and conformity to the European law', available at: http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-raises-deep-concerns-about-data-protection-and-the-respect-of-the-euro/

[16] Directorate-General for Internal Policies. Policy Department, 'Cloud Computing. Study', 2012, p. 5.

Due to its novelty, it is currently still uncertain how cloud computing services will evolve. However, as projected "their availability and capacity are likely to continue to increase (…) [and] while some services are likely to move to the public cloud given the potential cost savings, other services will still remain in a private environment."[17] From the legal as well as the practical perspective, few aspects can be identified which could stop the cloud computing sector from rapid development, i.e.: security threats, lack of uniform standards, uncertainty about the location of the data centres, problems with one-sided provider agreements, not only for consumers, the roles of actors involved, including their responsibilities, data transfers issues, etc.

### 1.1.4. Smart Metering

In the power engineering sector, previously unknown problems are related to the use of so-called smart grid meters which are devices designed for metering electricity consumption and for transmitting measurement information using an IT system. Such meters, which are part of smart metering systems, are expected to be of benefit to both electric energy producers (e.g. by reducing the amount of energy stored by them) and consumers, while having a positive effect on the natural environment. In the European Union, Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC (Article 13), obliges Member States to provide consumers with meters that accurately reflect their energy consumption and provide information on actual time of use.

Use of smart grid meters impacts, however, quite seriously on data protection, since information on the use of electricity and particular devices, behaviors and practices of persons is gathered and subsequently processed. Within this context, one specific legal issue which arises is whether the data measuring electricity consumption according to the hour/time of day of use etc. should be considered as personal data. In the opinion of the Article 29 Data Protection Working Party and national supervision authorities, data such as an individual's smart meter ID and/or unique property reference number, including other data, particularly data regarding message content (alerts, meter register read etc.) and billing data, enables that individual to be singled out from other consumers.[18] This results in increased risks for individuals, on the one hand, and in legal obligations regarding privacy protection for the entities using such solutions, on the other hand.

### 1.1.5. Face recognition technologies (biometric technologies)

Biometric technologies such as face recognition technologies are increasingly popular. This growing popularity is *inter alia* the result of considerable technological development (e.g. the speed and accuracy of applied technologies) and availability (attributable to low prices of certain solutions). Such technologies are applied in both the public sector (public security) and the private sector, including for such purposes as automatic recognition of individuals in photographs placed on social networking websites, staff working time control, surveillance, fraud prevention, or even for purposes related to marketing and promotion.

[17] Directorate-General for Internal Policies. Policy Department, 'Cloud Computing. Study', 2012, p. 10.
[18] Article 29 Data Protection Working Party, 'Opinion 12/2011 on smart metering', WP 183 (4.4.2011).

Such technologies allow for the recognition of both an individual's physical appearance, and also his or her psychological or physiological features such as emotions, mood or even, in a way, the individual's … intentions. For example, so-called smart monitoring systems, used in selected places in the world, and based on neuron networks, allow images transmitted from surveillance cameras to be analysed. Based on "observations" using cameras and specialist detection devices, the system can predict certain types of behaviour, e.g. based on eyeball movement, eyelid blinking, heartbeat rates, breathing speed or voice trembling. This allows private entities and public security sector institutions to analyse behaviour of individuals that deviates from the accepted standards and to predict, for example, the planning of a criminal offence.

All this considerably affects the protection of privacy and personal data. This is the result of, in particular, the special nature of such data, as such practices may lead to the disclosure of highly sensitive information such as an individual's ethnic origin, race or health. Biometric technology needs to be appropriately evaluated in terms of compliance with the principle of proportionality as well as in terms of the objectives pursued through the use of such data, because using biometric technology (e.g. as part of conventional CCTV systems) significantly increases the possibilities and, in consequence, the objectives that can be achieved using such data. The ease of reproducing and making the gathered data available also affects the importance, within this context, of the principle of being bound by a goal and of achieving a goal which goes beyond the original purpose of processing the data. Biometric technology may also be used for profiling purposes, particularly that which is based on the specific behaviour of individuals.[19]

### 1.1.6. Google's collection of WiFi data

As part of its investigation, the Dutch DPA found that from March 2008 to May 2010 using vehicles for taking photographs for the Street View service, Google collected data regarding approx. 3.6 million WiFI routers in the Netherlands alone, which accounted for approx. 63% of all such devices used by households and companies in the Netherlands.20 The data collected by Google included both data regarding the device itself (its existence and location), as well as data obtained from the device (e.g. web traffic, email addresses, some other files, including video and audio files). The relevant authorities of other countries, e.g. Germany and Ireland, also decided to look into this matter.

As part of the investigation by the Dutch authority, it was held that when combined with geolocation data, MAC (Medium Access Control) addresses constitute personal data because the data can provide information about the router's owner. The matter also showed other potential risks for privacy and concerned other significant legal issues, such as the qualification of the entity processing such data as a data controller. In this respect, Google claimed inter alia that it could not be considered as a data controller because there was no purpose whatsoever for the processing of personal data on its side. Google's position, based on its subjective realisation of specific objectives or intentions, was rejected by the authority, which emphasised the importance of objective assessment in this regard. The authority also found Google in breach of regulations regarding the basis for data processing, the obligation to provide information to the subjects of such data and the obligation to notify the national authority of the data processing.

---

[19] See in detail Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies', WP 193 (27.04.2012) as well as 'Opinion 02/2012 on facial recognition in online and mobile services', WP 192 (22.03.2012).

[20] Dutch Data Protection Authority (College beschermingpersoonsgegevens, CBP), 'Final findings.Dutch Data Protection Authority investigation into the collection of Wifi data by Google using Street View cars', available at: http://www.dutchdpa.nl/downloads_overig/en_pb_20110811_google_final_findings.pdf

### 1.1.7. RFID - radio-frequency identification

Also increasingly popular is the use of Radio Frequency Identification (commonly known as "RFID technology") for different purposes by both private and public entities. This technology uses radio waves to transmit data, which allows "reading" an electronic label (consisting of a passive electronic system and an antenna) through a special reader (containing a transmitter, a receiver, a decoder and an antenna). As a result, it is possible to identify a particular object, e.g. a parcel being shipped (logistics) or a product offered by a shop (sales and distribution), to a much greater extent than is possible with the use of other technologies, i.e. those based on barcodes.

In addition to the unquestionable benefits of using this technology (e.g. by shops for theft protection, or to enhance consumers' shopping experience, or to improve control access to restricted areas), there are areas with a significantly higher risk of interfering with the privacy or dignity of individuals. For instance, due to the use of RFID technology individuals may be "followed" where they are, e.g. at airports, shops or in other public places. This technology also enables recognition of what clothes a particular individual is wearing, what devices he or she is using or even what medicines or other such objects, even if very personal and sensitive, he or she has. This results in the processing of data that can be used to identify a particular individual (i.e. personal data), including so-called sensitive data. It is often the case that such data processing is achieved without any legal basis, without valuable information for the individuals concerned, and in violation of the applicable rules.

### 1.1.8. Social networking services

Social networking websites, where users can not only view content, but also generate their own content (known as User Generated Content), seem to change the weight of many of the existing legal concepts, increasing – at the same time – the threats to privacy, at a mass scale (given, e.g., the number of the users of such sites). The issue that arouses particular doubts is whether the so-called household exception will be applied to the activity of users of social networking websites and, therefore, such activity will not be governed by the legal provisions on personal data protection, weakening the level of data protection.

Moreover, the status of users placing materials (including personal data) on such websites which belongs to third parties is not wholly clear. It is claimed that such users should be considered as data controllers, while drawing attention to the practical difficulties in this respect: i.e. it is not clear how such individuals would perform the obligations imposed on data controllers by law. A matter of difficulty is also the classification of social network providers, as they operate as either data processors or data controllers, depending on the activities they are involved in. As social network websites are becoming increasingly popular with children, the problems of processing data regarding children is gaining significance. Such problems include, in particular, the appropriate bases for such processing (the consent of the parents or legal guardians, the disclosure requirement etc.). All these issues have been addressed by the Regulation, however with not always satisfactory results.

### 1.1.9. Scanning electronic mail

Electronic mail scanning is another popular practice with providers of electronic mail services and involves scanning e-mails for the presence of specific content for marketing communication profiling purposes. The profiling of online advertising requires scanning the content of incoming electronic mail for the presence of keywords with the aim of making advertising messages better "suited" to the needs of users. Admittedly, the process of scanning electronic mail is a fully automated process and does not require disclosing any information that would allow individual users to be identified or, in particular, the content of electronic messages to be disclosed to third parties (especially advertisers). However, there are serious doubts surrounding this process.

These doubts also exist within the context of personal data regulations. This concerns the processing of data of a personal nature. Moreover, the data processed as part of filtered electronic mail accounts also includes sensitive data disclosing, for example, the political views, religious or philosophical beliefs of the account users. One of the main problems in this respect is to indicate the appropriate bases for such data processing. It seems that such a basis should be provided in the form of the user's consent. Such processing is not necessary to perform the contract, nor can it be explained by the legally justified objectives pursued by the data controller. Such technology can also be used for profiling purposes, without individuals' awareness.

### 1.1.10. Online gaming

As regards online gaming, an issue of particular significance is the protection of children whose data is often used for different purposes, including marketing purposes, without the children being aware of such use. Within this context, it is important to make laws and regulations that would be technologically neutral to such an extent as to be able to "keep up with" the changes taking place. Today, online games are not limited to games using computers and online browsers: video game consoles are designed to support playing games online (networked gaming) and mobile phones are offering increasingly advanced features, which results in greater capacity to assimilate data from different sources and use it with unprecedented potential. New solutions, such as a voice and motion-control sensor system for the X-box (Microsoft), allow faces and movements to be recognised, which makes the devices suitable for recognising individual players.[21]

[21] Microsoft Corp., 'Kinect Fact Sheet' (2010), available at: www.microsoft.com/presspass/presskits/xbox/docs/KinectFS.docx.

### 1.1.11. Summary table

| New Technology phenomenon (discussed in section 1.1.) | Degree of influence on data protection (law / medium / high) | Legal issues influenced (defined in the Proposal and discussed in in section 1.2.) |
|---|---|---|
| Geo-location services | High | 1. Definition of "personal data"<br>2. Data anonymisation and pseudonymisation<br>3. Purpose limitation principle and further processing |
| Assimilation of data from different sources | High | 1. Purpose limitation principle and further processing<br>2. Definition of "personal data"<br>3. Actors involved: "data controllers" and "data processors" |
| Cloud computing | High | 1. Actors involved: "data controllers" and "data processors"<br>2. Purpose limitation principle and further processing<br>3. Transfers of personal data |
| Smart Metering | Medium/High | 1. Definition of "personal data"<br>2. Purpose limitation principle and further processing<br>3. Data anonymisation and pseudonymisation |
| Face recognition technologies (biometric technologies) | Very high | 1. Definition of "personal data"<br>2. Measures based on 'profiling'<br>3. Data anonymisation and pseudonymisation<br>4. Purpose limitation principle and further processing |
| Google's collection of WiFi data | Medium | 1. Definition of "personal data"<br>2. Actors involved: "data controllers" and "data processors" |
| RFID - radio-frequency identification | High | 1. Measures based on 'profiling'<br>2. Purpose limitation principle and further processing<br>3. Definition of "personal data" |
| Social networking services | High | 1. "Household exception"<br>2. Actors involved: "data controllers" and "data processors" |
| Scanning electronic mail | Medium | 1. Measures based on 'profiling'<br>2. Purpose limitation principle and further processing |
| Online gaming | High | 1. Measures based on 'profiling'<br>2. Purpose limitation principle and further processing |

## 1.2. Regulatory responses to new technologies in the Proposal

### 1.2.1. Definitions of "data subject" and "personal data": Articles 4(1) and 4(2); online identifiers

The definition of "personal data" applicable to date (Article 2(a) of Directive 95/46/EC) – which is of key significance to the entire regulation and especially in the context of new technology developments – has been carried over, to a material extent, and incorporated into the definition of "data subject". Pursuant to Article 4(2) of the Proposal, *"'personal data' means any information relating to a data subject"*, whereas *"'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person"* (Article 4(1) of the Proposal). According to the Commission, preservation of the current method of defining the term "personal data",*has the advantage of providing a high degree of flexibility and the possibility to adapt to various situations and future developments affecting fundamental rights"*.[22] As a result – in spite of the difficulties of interpretation and varying implementations of the definition in the different Member States – the Commission believes that *"it would seem counterproductive to change the definition of personal data"*.[23] The adopted (*de facto* maintained) regulatory method should be, in principle, accepted as it allows for implementation of the goals that underlie the regulation analysed. However, it seems that this area lacked certain careful reflection, particularly as regards relevance of this fundamental definition to modern conditions, including in particular those arising from technological progress. Moreover, some of the changes in the definition of "personal data" cast substantial doubt, which may weaken the anticipated effect of harmonisation.

The concept of "personal data" has been somewhat improved by the proposed General Regulation through the addition of the phrase "**means likely reasonably to be used**" (see recital 23 of the preamble to the Proposal), which is a borrowing from recital 26 of the preamble to Directive 95/46/EC. This component was carried over to the same definition, but not without some faults, which gives rise to doubts as to the objectives that guided the Commission in this regard: Article 4 (1) of the Proposal mentions "means reasonably likely to be used", which may cause problems of interpretation, and even change the meaning of that wording. Proper use of this definitional component should allow in practice for taking into account, in particular, the different means and factors that permit identification, as well as the degree to which the possibility of identification does not exist or is negligible.

Also, there are concerns about the passage of the definition according to which the measures which may lead to the identification of a natural person may be used "**by the controller or by any other natural or legal person**". Although the current law (recital 26 of the preamble to Directive 95/46/EC) contains the above provision, to date it has had no material effect on how the term "personal data" was interpreted.[24] There is concern that this situation may change after the adoption of the definition in the proposed form. This may result in weakening or even abandoning the so-called **"relative approach"**, under which certain information may constitute personal data for a specific

[22] Commission Staff Working Paper, 'Impact Assessment', SEC(2012) 72 final, Annex 2. Evaluation of the Implementation of the Data Protection Directive, p. 14.

[23] Commission Staff Working Paper, 'Impact Assessment', SEC(2012) 72 final, Annex 2. Evaluation of the Implementation of the Data Protection Directive, p. 16.

[24] See in particular Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data', WP 136 (20.06.2007). In this opinion no proper attention was paid to the element indicated here.

entity, while the same information – for another entity – will not constitute personal data as it does not allow this particular entity to identify the data subject. The proposed change – as noted in the European literature – *"would suggest that if party A has non-identifiable data and party B has an index which can correlate that data with the identity of a person then this automatically means that the non-identifiable data is personal data – even if there is no relationship between party A and party B"*.[25] The effect of such a solution may be a significant extension of the definition of "personal data", and thus expansion of the obligations of entities involved in the processing of different types of information. In this respect, it seems necessary to clarify which persons (natural or legal) that passage of the definition refers to, which could be achieved through, for example, an explicit identification of the relationship (e.g. legal relationship) between the controller and such persons, so that they are not just any persons; otherwise, any information regarding a natural person would constitute personal data to each and every entity processing personal data.

In the context of modern technologies, in particular those which are Internet-related, it is of fundamental importance how a variety of **online identifiers**, such as IP addresses or cookies, are qualified.[26] At the same time, legal regulation should be expected to provide as clear a qualification as possible. Unfortunately, the Proposal does not meet these expectations. On the one hand, the amended definition clearly indicates that the identification of a natural person may be made by reference to "location data" or an "online identifier". Such an approach might suggest that location data as well as online identifiers may – in itself – constitute personal data, with all resulting consequences. On the other hand, however, recital 24 of the preamble to the Proposal notes that online identifiers *"may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances"*. This passage of the preamble suggests, therefore, that – firstly – online identifiers cannot in themselves constitute personal data, because they may be used only in conjunction with other information to identify individuals; and secondly – that such a qualification will always depend on the particular circumstances of its processing (the text of the Proposal does not indicate, however, even by way of example, any such circumstances, therefore the significance of the quoted passage is greatly reduced).

It will be necessary, therefore, to explicitly clarify – possibly in the Regulation, not only in its preamble – how online identifiers should be treated, bearing in mind that *"an overly inclusive definition of personal data could effectively require data controllers to identify individuals in borderline cases so that they could comply with other legal requirements, and would thus be counterproductive"*.[27] However, it does not seem necessary to remove the reference to location data or online identifiers from the proposed definition of "data subject". There should, in fact, be no doubt that a natural person may be identified not only by reference to "traditional" identification numbers (such as ID number), but also against various online identifiers. The key is, however, to define, as precisely as possible, the situations in which online identifiers should be treated as personal data and other sitautions in which they will not be subject to such a qualification. Of the proposals submitted in this

---

[25] A. Winton, N. Cohen, 'Proposed EU Framework – Online Advertising, E-Commerce and Social Media', (2012), available at: http://www.whitecase.com/articles-04172012

[26] As noted by the Commission, *"broad and flexible definition [of personal data] leads to some diversity in the practical application of these provisions. In particular, the issue of objects and items ("things") linked to individuals, such as IP addresses, unique RFID numbers, digital pictures, geo-location data and telephone numbers, has been dealt with differently among Member States"* (Commission Staff Working Paper, 'Impact Assessment', SEC(2012) 72 final, Annex 2. Evaluation of the Implementation of the Data Protection Directive, p. 14).

regard, attention should be paid to that raised by the UK Data Protection Authority, the Information Commissioner's Office, which indicates the role that may be played in this regard by the **intentions of entities processing personal data**. As suggested by the ICO, *"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"*.[28]

### 1.2.2. Data anonymisation and pseudonymisation

The new data protection framework should encourage entities processing personal data to anonymise personal information, which allows data to be processed without reference to information which could identify the data subject. Given the broad definition of "personal data" adopted in EU law, anonymisation allows for the implementation of numerous projects that involve personal information without adversely affecting the privacy of natural persons. Thus, data processing entities have been showing significant and growing interest in this phenomenon, e.g. in the context of marketing activities or making certain information available online. Also, as regards the legal aspect, anonymisation provides certain advantages: e.g. it allows for the reinforcement of the principle of "data minimisation", which only permits processing of personally identifiable data when the data must be personally identifiable in order to fulfil the purpose for which it is being processed. Moreover where it is not necessary to pursue a particular purpose, such data should– if possible – be subject to anonymisation. However, given the current realities of technological and legal development, there is no certainty as to when one is dealing with fully effective anonymisation. The use of anonymisation by entities from the European Union is also hindered by the broad definition of "personal data", which is interpreted differently (sometimes very narrowly) by the national data protection authorities.[29]

**An incentive to use anonymisation** is to be found in recital 23 of the preamble to the Proposal, according to which *"[t]he principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable"*. However, it would definitely make more sense if this were incorporated into the text of the Regulation itself (e.g. into Article 5 or 10), together with a precise definition of the legal institution. Prescribing precise **conditions for successful anonymisation** would also be highly recommendable – or even necessary – for insertion in the text of the new law. Those conditions should include:

1. requirements for anonymisation itself, and
2. requirements for the processing of anonymised data.

---

[27] Ch. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', Privacy & Security Law Report, 11 PVLR 06 (2012), p. 5.

[28] UK Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' (2012), p. 5.

[29] Cf. document Commission Staff Working Paper, 'Impact Assessment', SEC(2012) 72 final, Annex 2. Evaluation of the Implementation of the Data Protection Directive, p. 15-16, which contains a short review in that respect.

### Anonymisation-related requirements

In the context of conditions associated with rendering data anonymous, consideration must be given, in particular, to the requirement to obtain the consent of the persons concerned to carry out such operations on their data. This seems particularly important in the context of the broad understanding of the term "data processing" and the modified definition of consent (Article 4(8) of the Proposal), which requires, on each occasion, explicit indication of the data subject's wishes. "Data processing", which involves *"any operation or set of operations which is performed upon personal data or sets of personal data"* – including "erasure or destruction" – (Article 4(3) of the Proposal), also applies to the operation of anonymisation, for which it is necessary to identify the required legal basis. At the same time, this aspect should take into account – and precisely define in the legal text – both situations where consent is required (if any) and situations where consent is not required.

Issues that need to be taken into account should also include:

- leaving the "original" data in possession of the entity rendering them anonymous and the implications thereof for its effectiveness;
- (possible) requirement for data protection impact assessment;
- opposition of the persons concerned – reported already at the stage of conducting anonymisation;
- specific regulations that may apply, for example in relation to public bodies, or regulations on health;
- technical issues (requirements), on which, to a large extent, the effectiveness of the process of anonymisation, its irreversibility, etc. depends.

### Requirements for the processing of anonymised data

Among the conditions associated with the processing of anonymised data, the following will require particular consideration:

- the aspect of security of the data as well as of the key used to re-identify the data;
- the need to conduct periodic evaluations, which is associated with levels of the effectiveness of anonymisation changing over time, caused, among other things, by the risk of re-identification of data that are, for example, published online and which increases over time;
- the possibility of withdrawing consent by the person concerned due to, for example, an increased risk of data re-identification.

It should also be discussed, whether, in some circumstances, the law could not even oblige the organisations to anonymise data (obligation of anonymisation). The introduction of such a requirement is advocated by, for example, Article 29 Data Protection Working Party, noting that this requirement could apply to situations "where feasible and proportionate *according to the purpose of processing"*[30] (such a general provision would be then elaborated on within the data protection impact assessment).

[30] Article 29 Data Protection Working Party, 'Opinion 01/2012 on the data protection reform proposal', WP 191 (23.03.2012), p. 11.

Such an obligation could be of particular relevance in the context of the principle of "privacy by design", and would also contribute to reinforcing the obligation to reduce the processed data to the necessary minimum and the prohibition articulated in Article 10 of the Proposal, according to which *"if the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation"*.

The emerging modernised European data protection framework should also implement the **concept of pseudonymisation**. Article 29 Working Party, in its Opinion on the concept of personal data, defined "pseudonymisation" as *"the process of disguising identities"* on a temporary basis by using *"correspondence list for identities"* and "pseudonyms" for individuals.[31] In this regard, it would be desirable, in particular, to precisely define the term "pseudonymised data" and to identify the conditions that are required in this regard, in particular the conditions for the pseudonymisation process itself (e.g. requirements for the pseudonyms used). However, given the fact that "pseudonymised data" will continue to constitute "personal data", it will be necessary to determine the benefits that may be associated with its pseudonymisation, such as exemption from specific legal obligations or facilitation of certain elements related to such data, for example as regards measures based on profiling (cf. 3.2.4 below). Otherwise, the idea of pseudonymisation would not be attractive to data processors.[32] This seems particularly important in the context of the broad definition of "personal data", which involves a wide range of obligations the meeting of which – particularly in the context of new technologies – does not always seem to be possible or advisable. A properly constructed concept of pseudonymisation would also allow for addressing the calls of certain stakeholders, indicating the need to go beyond the present "bipolar" system based on a dichotomous division into "personal data" and "non-personal data", which does not conform fully with the requirements of the current social and technological development.[33]

Given the role that is played in the context of anonymisation and pseudonymisation by certain technological conditions, various soft-law instruments and initiatives may be of relevance here, including in particular **codes of conduct**.[34] Unfortunately, the text of the Proposal – in particular recital 23 of the preamble – contains no express reference to that type of instrument, similar to the provisions contained in recital 26 of Directive 95/46/EC, whereby *"codes of conduct (…) may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible"*. The Proposal needs to be completed in that respect as well.

---

[31] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data, WP 136 (20.06.2007), p. 18.

[32] Article 29 Data Protection Working Party pointed that *"the risks at stake for the individuals with regard to the processing of such indirectly identifiable information will most often be low, so that the application of these rules will justifiably be more flexible than if information on directly identifiable individuals were processed"* (see 'Opinion 4/2007 on the concept of personal data, p. 18).

[33] See in particular American Chamber of Commerce to the European Union, 'Response to the Commission communication on a comprehensive approach on data protection in the European Union, 14.01.2011, p. 26.

[34] See for example UK Information Commissioner's Office, 'Draft Anonymisation code of practice', May 2012.

### 1.2.3. Actors involved: "data controllers" and "data processors" (Articles 4(5) and 4(6))

The Proposal for a Regulation retains the **traditional division of entities involved in the processing of personal data**, i.e. into data controllers and data processors, introducing only minor changes in their definition (such as the definition of "controller" also draws attention to the "conditions" that may be – in addition to the purposes and means of processing – established by that entity). Proper classification of "actors" – as presented in 1.2.3. above – is not easy in practice, but has far-reaching consequences: it determines the scope of responsibility for the processed data (the fundamental portion thereof being imposed on the controller), affects how the rights of data subjects are exercised, defines the law applicable to data processing operations, etc. According to the "traditional" division, the former group of entities decides on the processing of personal data and initiates the processing, carrying out operations on data in-house or through an external entity (data processor). With this approach, data processors act as "passive" parties which do not have any impact on the way data are processed.

Such an assumption and this simple duality is no longer valid in the light of current commercial practices, and it is increasingly complex to apply this distinction in practice. For example, in cloud computing and e-commerce, "data processors" may exercise significant influence over the way the processing takes place. In particular, data processors influence – and even "decide" – about the technical and organisational measures to be used for data processing.

Moreover – as noted by Article 29 Data Protection Working Party – the *"tendency towards organizational differentiation"*, both in the private sector, where it may take the form of "corporate diversification", and in the public sector (e.g. decentralisation of policy departments and executive agencies), is intensifying.[35] It is not surprising, therefore, that often the largest market players (e.g. Google, see section 1.1.5.), and even data protection authorities, have problems with the proper evaluation and qualification of the roles of the different actors involved in the processing of personal data.[36] Thus, the risk of inappropriate qualification increases in the context of smaller entities, particularly SMEs. Moreover, it is noted that the role of entities such as cloud providers and Web 2.0 service providers is often reduced to the provision of a specific infrastructure (e.g. on-line platforms and servers for "cloud computing"), which is used for personal data processing, and, therefore, it *"is not always evident that they are themselves involved in such processing"*.[37]

---

[35] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', WP 169 (16.02.2010), p. 6; see also Ch. Kuner, 'European Data Protection Law. Corporate Compliance and Regulation', Oxford University Press, 2007, p. 70-72.

[36] Cf. the case regarding SWITF (Society for Worldwide Interbank Financial Telecommunication), where SWIFT was convinced that it was acting as data processor, however, as a result of the investigation, it was qualified as data controller; cf. also Article 29 Data Protection Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Woldwide Interbank Financial Telecommunication (SWIFT)', WP 128 (22.11.2006).

[37] P. De Hert, V. Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', Computer Law & Security Review 28 (2012), p. 134. See also W.K. Hon, Ch. Millard, I. Walden, '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, (p. 14 and subs.), who propose that cloud providers who provide only hardware and software supply services be not treated as 'data processors', but rather as 'neutral intermediaries'.

On the basis of the currently applicable regulation and the definitions adopted, in order to somehow "adjust" them to the changed conditions, various interpretive measures are taken, including but not limited to:

- the adoption of a broad understanding of the term "means" (*""means" does not only refer to the technical ways of processing personal data, but also to the "how" of processing, which includes questions like "which data shall be processed", "which third parties shall have access to these data", "when data shall be deleted", etc."*);[38]
- the possibility of deciding about the "purpose" of processing is granted solely to the controller (*"Determination of the "purpose" of processing is reserved to the "controller""*), while permitting delegation of the possibility of deciding about the "means" of data processing to a data processor (here, however, "means" shall be understood in the narrow sense, *"as far as technical or organisational questions are concerned"*);[39]
- as a result, the current condition contained in the definition of "data controller" may be interpreted – contrary to its literal wording – as *"determines the purposes or means of the processing of personal data"* (rather than *"determines the purposes and means of the processing of personal data"*).

The preceding discussion shows that an unequivocal distinction between data controller and data processor is no longer tenable, given the complex relationships that exist between entities involved in the processing of personal data. Those difficulties have been spotted both by Article 29 Working Party[40] and by the Commission, failing, however, to see the need to depart from the current model. Instead, Article 4(5) of the Proposal adds to the definition of "data controller" the requirement to **determine also the conditions of the processing of personal data**, which, however, raises additional complications and doubts. First of all, it is unclear how to understand the term "conditions", and, in particular, whether it would answer the question "how" the data is being processed (which is, at the moment, reserved for the term "means") or whether it should be interpreted in a different way. Second, and even more problematically, the definition still uses the conjunction "and". Thus, the qualification of an entity as data controller will require cumulative satisfaction of the condition to determine the purposes, the means and the conditions of processing. In this context, a question may also arise as to whether it will be possible to "delegate" the right to determine not only the "means" of processing but also the "conditions" thereof to the data processor. However, even if this were possible, the proposed wording of the definition would not allow for a clear identification of what the basis of such a "delegation" and its scope would be. It, therefore, seems that the solution proposed in the Proposal – with the other elements of the definition remaining unchanged – may cause additional difficulties and uncertainties of interpretation, rather than eliminate them.

---

[38] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', WP 169 (16.02.2010), p. 14.

[39] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', WP 169 (16.02.2010), p. 15.

[40] Article 29 Data Protection Working Party *"recognises the difficulties in applying the definitions of the Directive in a complex environment, where many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility (…) [h]owever, it has not found any reason to think that the current distinction between controllers and processors would no longer be relevant and workable in that perspective"* ('Opinion 1/2010 on the concepts of "controller" and "processor"', WP 169 (16.02.2010), p. 33).

Instead of the above, a different solution may be proposed: reducing the factors decisive in the qualification of a data processing entity as data controller to **purposes of data processing**. Such a solution seems to be less revolutionary, permitting the developments generated on the basis of the present definition to be taken into account, in particular those of the Article 29 Working Party. Such a solution would mean abandoning the factor of "means", but it seems that this would help to avoid at least some of the difficulties emerging today. Abandoning "means" is advisable because:

- there are substantial doubts as how to understand the term "means";
- greater importance is already assigned to the factor of "determining the purposes" rather than "determining the means" of processing;[41]
- Article 29 Working Party even permits the possibility of "delegation" of the competence to determine the means to the processor (at least as defined by the narrow meaning of that term);
- moreover, the general importance of "purposes" of processing is much higher in the personal data protection regulation because – as the legal literature reasonably notes – *"the finality pursued by (a set of) processing operations fulfils a fundamental role in determining the scope of the controller's obligations, as well as when assessing the overall legitimacy and/or proportionality of the processing"*.[42]

Another proposal in this respect advocates departing from the current dichotomy and to completely **abandon the structure of "data processor"**.[43] In particular, solutions adopted in foreign law systems, such as in Canada, are indicated, whose solutions are based on the Personal Information Protection and Electronic Documents Act (PIPEDA).[44] Under the PIPEDA, entities involved in the processing of personal data are considered to remain responsible for data even when data is transferred to third parties who conduct some processing operations. Such solutions, however, also entail certain far-reaching consequences in the form of, for example, making the positions of all entities involved in data processing equal and distributing all the obligations evenly, without taking into account their individual position, the scope of their tasks, or the expectations of data subjects. Therefore, the possible adoption of such solutions requires far-reaching prudence. Moreover, it seems that, on the basis of the dichotomy adopted in EU law, one can – with proper interpretation – achieve results similar to those found in regulations such as PIPEDA.[45]

---

[41] As noted by B. Van Alsenoy, *"[o]f these two elements, the Working Party appears to place greater weight on the controller's determination of finality (purpose) than upon his determination of means"* (in: 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC', Computer Law & Security Review 28 (2912), p. 31).

[42] B. Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC', Computer Law & Security Review 28 (2912), p. 31, footnote 55.

[43] P. De Hert, V. Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', Computer Law & Security Review 28 (2012), p. 134; similarly W.K. Hon, Ch. Millard, I. Walden, '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, p. 24.

[44] B. Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC', Computer Law & Security Review 28 (2912), p. 41.

[45] In any case, the Canadian regulation – and its 'accountability chain' approach – is criticised (see the literature referred to by B. Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC', Computer Law & Security Review 28 (2912), p. 42, footnote 161).

It also seems difficult to accept the proposals that entities which provide services to a limited extent (e.g. cloud computing infrastructure providers) are treated neither as "data controllers" nor as "data processors". In the context of the broad definition of personal data "processing" (maintained in the Proposal for a Regulation; Article 4(3)), any data operations – including its storage or processing with the use of the IT infrastructure owned – are subject to the regulation in question. Removal of such an important class of entities from the regulation could result in a weakening of the level of data protection, and could undermine the effects of such practices and institutions as "privacy by design" or specific requirements for data security.

In addition to definitional issues, the Proposal should elaborate on a **precise division and determination of the obligations and responsibilities** of data controller and data processor. Due to the fact that data processors generally perform only tasks assigned to them by the data controller, the question arises about the validity of the adoption of solutions according to which the data controller may expect the support of the processor in satisfying such obligations as the obligation to provide information, to conduct data protection impact assessment, etc. In that respect, verification should include but not be limited to the following: Article 33, Article 34, and Article 75 of the Proposal.

### 1.2.4. "Household exception": Article 2(2)(d)

The definition of "purely personal or household activities" (the so-called "household exception") has been somewhat changed by the Proposal. The Proposal, in Article 2(2)(d), excludes from its scope the processing of personal data *"by a natural person without any gainful interest in the course of its own exclusively personal or household activity"*. The current scope of the exemption under Article 3(2) of Directive 95/46 (*"by a natural person in the course of a purely personal or household activity"*) is **supposed to be too broad**, because it could exempt, in practice, such activities as the still growing processing of personal data online, especially by online social networks. For example, Article 29 Working Party in its document "Future of Privacy" has pointed out that:

> *"Increasingly, individuals upload their own personal data into the internet (social networks, cloud computing services, etc). However, Directive 95/46/EC does not apply to the individual who uploads the data for 'purely personal' purposes or 'in the course of a household activity'. Arguably it does not apply either to the organization that provides the service, i.e. hosts and makes available the information uploaded by the individual (unless the service processes data for its own purposes) insofar as the service provider may not be deemed to be a controller. The result is a situation of lack of safeguards which may need to be addressed, particularly given the increase in the number of such situations. In this context, whoever offers services to a private individual should be required to provide certain safeguards regarding the security, and as appropriate the confidentiality of the information uploaded by users, regardless of whether their client is a data controller".*[46]

[46] Article 29 Data Protection Working Party, 'The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data', WP 168 (1.12.2009), para. 71, p. 18. See also Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking', WP 163 (12.06.2009), p. 5-7.

The proposed text, however, still raises some concerns – especially when compared to the interservice version of the Regulation (dated 29.11.2011), which contained an additional restriction of this exemption (*"unless personal data of other natural persons is made accessible to an indefinite number of individuals"*). The restriction proposed in the previous version of the Proposal reflects the judgement of the European Court of Justice in the case Lindqvist[47] and Satamedia.[48] In the Lindqvist case, the court, in responding to the question of whether the activity of Ms Lindqvist is subject to the exemption referred to in Article 3(2) of Directive 95/46, ruled that:

> "*That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.*"

The solution ultimately adopted by the Commission in the Proposal dated 25.01.2012 should, however, be accepted. It does not seem that the introduction of additional restrictions in that respect – in the text of the law – would help avoid interpretational difficulties and practical issues. References to data "**made accessible to an indefinite number of individuals**" gives rise to questions such as: what circumstances should determine whether the circle of potential recipients of such data is "definite" or "indefinite", in particular whether any significance should be given to the nature of profiles on social networks ("private" or "public" profiles")[49] or to some other circumstances? It seems that ultimately it will be necessary to refer to whether a given activity is an "exclusively personal or household activity".[50] Therefore, it should be recommended to take into consideration the circumstances of rendering data available "to an indefinite number of individuals", but not in the normative text (i.e. in the provision itself), but in the preamble to the Regulation (now – recital 15). However, that circumstance (like the rest indicated in the preamble) should not be decisive in whether to use or not the exemption, and should be treated only as one of the circumstances to be considered in assessing a given case.

Any possible additional restrictions of the "household exception" should be adopted **with regard to their impact on other values**, in particular freedom of expression, which is especially important in the online community (blogs, entries on social networking sites, etc.). In this context, there may be doubts about the extension of the proposed wording of Article 2(2)(d) to include the condition: "without any gainful interest", as well as about the condition: "without any connection with a professional or commercial activity" contained in recital 15 of the preamble to the Proposal of a Regulation. As rightly pointed out by the UK Data Protection Authority, the former restriction *"might give the impression that only non-commercial activity can benefit from the exemption"*.[51] Also, the latter condition – the lack of "any" connection with a professional or commercial activity – seems to be formulated too categorically and broadly.

---

[47] Case C-101/01 [2003] ECR I-12971.

[48] Case C-73/07 [2008] ECR I-9831

[49] According to B. Van Alsenoy, J. Ballet, A. Kuczerawy, J. Dumortier, this does not seem appropriate. The authors *"would argue that the mere 'public' or 'private' setting of a profile by itself is too arbitrary a criterion, especially when considering the potentially great number of recipients even when the user set his profile to private"* (B. Van Alsenoy, J. Ballet, A. Kuczerawy, J. Dumortier, 'Social networks and web 2.0: are users also bound by data protection regulations?', Identity in the information society, 2009, vol. 2, no. 1, p. 75).

[50] Also B. Van Alsenoy, J. Ballet, A. Kuczerawy, J. Dumortier, 'Social networks and web 2.0: are users also bound by data protection regulations?', Identity in the information society, 2009, vol. 2, no. 1, p. 75.

[51] UK Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' (2012), p. 4.

### 1.2.5. Measures based on 'profiling': Article 20

The Proposal sets forth rules for a special type of data processing, known as "profiling". Profiling activities, intended to evaluate certain personal aspects of natural persons, are commonly used in the online environment, e.g. to filter search results, to provide shopping suggestions or for the purposes of direct marketing advertisements (see, for example, sections 1.1.6. and 1.1.8. of this study). Operations that use various kinds of "profiling" are performed commonly in many other cases and situations in many sectors of the economy or in legal relations, for example in the financing business (such as assessment of creditworthiness) and the insurance business, in employment relationships, in the marketing business, in science, and for the purpose of prevention of organised crime, terrorism, etc.

Article 20 of the Proposal builds upon the existing Article 15 of Directive 95/46/EC, dealing with "automated individual decisions", but significantly extends its scope to **all types of "measures"** which produce legal effects concerning natural persons, not only to "decisions". In addition, the scope of application of the provision has been extended by making the prohibition specified therein applicable not only to processing operations intended to evaluate certain personal aspects, but also to those activities that are performed solely to analyse or predict those aspects. As a result, it is believed that it *"will likely cause many companies to re-evaluate their data processing practices, particularly in the online sphere"*,[52] and as regards the latter, *"it is likely that information society service providers are likely to move the point at which users must be registered and "logged in", so that more of the site is only available to users who are logged in. This will result in more data being collected about users rather than less and the debate then becomes whether the profiling and other related services are "necessary" for the performance of the information society service"*.[53] Furthermore, the provision uses the term "natural person", rather than "data subject", which may suggest that it will be applied regardless of whether we are dealing with personal data or information of other nature (the term "personal data" does not appear in Article 20(1), which reinforces the suggestion).

Discussion of the various forms of "profiling" and how they should be regulated has generated all kinds of opinions, ranging from the most critical (perceiving this type of activity as "pure evil") to the other extreme, pointing to many benefits of "profiling", both in the context of economic development or better customer service. Advocates of the former opinion point to the risks associated with such operations, which often cannot be predicted and properly assessed. They may be related, for example, to concerns of the citizens about ubiquitous tracking of their behaviour, building extensive personal profiles, and using the results of such an activity for purely economic purposes. Also, emphasis is placed on the risk of infringement of the principle of non-discrimination, for example due to *"unjustifiably depriving her or him from accessing certain goods or services"*.[54] On the other hand, advocates of the latter view point to the consequences that may result from reducing the possibility of profiling, such as limiting economic growth, shifting costs to consumers (which may be related to, for example, restrictions on marketing activities), and weakening the competitiveness of European businesses.

---

[52] Ch. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', Privacy & Security Law Report, 11 PVLR 06 (2012), p. 7.

[53] A. Winton, N. Cohen, 'Proposed EU Framework – Online Advertising, E-Commerce and Social Media', (2012), available at: http://www.whitecase.com/articles-04172012

[54] Council of Europe, 'Recommendation CM/Rec(2010)13 of the Committee of Ministers to Member Stateson the protection of individuals with regard to automatic processing of personal data in the context of profiling', available at https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM

In the Proposal, the Commission seems to be leaning towards the former group of opinions. **Profiling operations are being dealt with rigorously** in the proposed Article 20 of the Regulation, with much wider scope of application and many restrictions. It, therefore, seems necessary that further works take into account the broader context, including the consequences resulting from overly restrictive regulation in this area. Those decisions – for the most part – are of political nature, but should be based on a much more **thorough analysis** than that presented by the Commission. Such an analysis should include, in particular, the differences that emerge in the context of "profiling" in different economic sectors, in different situations or legal relations. As it has been noted, *"marketing profiling means something different than in the risk management department of an insurance company, or in the psychology department supporting crime investigations by the police"*.[55] In addition, account should be taken of the fact that there are different levels of risk associated with profiling and disparate types of impact on the privacy of individuals.[56] As a result, it is impossible to agree with the solution proposed in the Proposal, which deals equally with all possible situations and cases of "profiling", introducing universal far-reaching restrictions in this regard, and a more suitable balance needs to be established as regards profiling activities, particularly in the online sphere. One way to deal with that would be to include data protection impact assessment and steer the entire profiling model towards a more risk-based approach.[57] However, the Proposal provides for no explicit relationship between data protection impact assessment and the profiling phenomenon, which should be changed in the wording of Article 20.

In addition, the provisions of Article 20 need to be clarified, particularly in the context of such key – but at the same time imprecise – phrases as "**produces legal effects**", "**significantly affects**", etc. The former of those phrases may be justified under Directive 95/46/EC, which applies to decisions, however it raises fundamental concerns in the context of all kinds of "means", which itself offers a wide range of possible interpretations. As regards the latter phrase, questions arise as to whether "significance" should be assessed from the perspective of the individual or in a more objective way; of what nature the "effects" may be (in particular whether they can be purely economic); etc. Moreover, the conditions proposed in Article 20(2) contain a number of ambiguities, raising serious questions of interpretation and resulting in different approaches to the problem in different EU countries. In this regard, concepts such as "suitable safeguards" and "suitable measures" in particular require clarification. Also, extending the catalogue of the conditions that permit profiling to include the case of using pseudonymised data could be considered.

Due to the wide practical application of profiling, involving many different business sectors and industries, soft-law instruments, in particular **codes of conduct**, may be of great importance in this regard. They may serve as "guidance" on how to interpret and apply the prescribed rules when it comes to profiling in a specific context, particularly in order to ensure that unfair and unlawful profiling is not taking place.

---

[55] Federation of European Direct and Interactive Marketing, 'FEDMA submission on the Comprehensive Strategy on Data Protection in the European Union', 15.01.2011, p. 5.

[56] Some authors also point to the need to take account of the inter-disciplinary aspect, bearing in mind the specific nature of computer science, especially the mechanisms governing data analysis, because at present *"data mining community (adept at spotting application issues) and the legal community do not co-operate enough"* (B.W. Schermer, 'The limits of privacy in automated profiling and data mining', Computer Law & Security Review 27 (2011), p. 49). According to the author, this is one of the reasons why *"the concept of privacy and its application in data protection law does not provide adequate protection from the risks associated with automated profiling"* (ibidem, p. 49).

[57] UK Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' (2012), p. 15. See also N.J. King, P.W. Jessen, 'Profiling the mobile customer – Is industry self-regulation adequate to protect consumer privacy when behavioural advertisers target mobile phones? – Part II', Computer Law & Security Review 26 (2010), p. 596.

### 1.2.6. Purpose limitation principle and further processing: Articles 5(b) and 6(4)

One of the core principles of Directive 95/46 – **the purpose limitation principle** (Article 6(1)(b) of the Directive) – has been retained in the Proposal (Article 5(b)), with no changes. The new Package introduces, explicitly, the possibility of further processing of data for incompatible purposes, but only if another legal basis can be found, except for a legitimate interest pursued by the controller (Article 6(4) of the Proposal). According to Article 6(4):

> "*Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract*."

There is an ongoing debate on whether this restriction should be eliminated or – on the contrary – strengthened, which could be of great importance for the Internet/online and other new technology-based industries. Today, many activities use the resources stored in databases for further processing and creating a certain "added value" (profiling, data mining, etc.), such as when the data has been collected in connection with and for the purpose of performance under an agreement, and is then used for other purposes, for example analytical purposes, to improve the quality of services (see, e.g., sections 1.1.2. and 1.1.4. of the study). The problem analysed here also shows strong links with the problems of "profiling", and the decision on the solution to be adopted in the final text of the Regulation will be largely political, in particular taking into account any conflicting values (including those specified in Article 21 of the Proposal). This issue is also particularly relevant in the context of the public sector's activities and re-use of public resources (cf. further comments in section 3.2.4).

In the legal context, **legitimate interest of the data controller** – like other grounds which justify processing – seems to be capable of forming the basis for further processing if the purpose for which the data were collected has changed. Giving the controller the possibility of such processing, upon prior assessment – by the controller – of whether the conditions set out in Article 6(1)(f) of the Proposal (in particular in terms of meeting the criterion of "necessity")[58] had been satisfied, would be associated with full legal responsibility for incorrect assessment in this regard. Any further processing of data would also be fully subject to the remaining rules of processing, in particular to the transparency principle, which requires notification of any change in the purpose of processing. Data subjects should also have the right – full and without any restrictions – to express opposition to such (contrary to the original purpose) processing of their data.

In this context, however, quite different views are also presented, for example the European Data Protection Supervisor, in his opinion on the data protection reform package, has stated that:

> "*the requirement of compatible use and the requirement of lawfulness are two cumulative locks which aim at ensuring a compliant processing of personal data. The requirement of compatibility cannot be lifted simply by referring to a condition of lawfulness of the processing. This would also be contrary to Article 5 of Council of Europe Convention 108. It is rather Article 21* [of the Proposal] *which should ensure that a change of purpose is done only under strict conditions*".[59]

[58] Which condition in inself may significantly limit the practical usefulness of this solution.

[59] European Data Protection Supervisor, Opinion on the data protection reform package (2012), [123].

In this regard, additional precision would be required as well, e.g. concerning the notion of "compatible use". This follows from the fact that at present the Member States interpret this notion in different ways, sometimes too liberally.

### 1.2.7. Principle of technological neutrality

In the context of new technologies, a principle such as technological neutrality could be of great importance. In its communication from 2010, the Commission underlined the need *"to ensure that individuals' personal data are actually effectively protected, whatever technology used to process their data"*. Much earlier, in 1999, the Commission pointed out that:

> "*Technological neutrality means that legislation should define the objectives to be achieved, and should neither impose, nor discriminate in favour of, the use of a particular type of technology to achieve those objectives.*"[60]

Most believe that **Directive 95/46/EC satisfies the principle of technological neutrality**. As noted by one of its authors:

> "*It is immediately apparent that all technologies which might be used to process data automatically, most obviously computers but extending to older technologies such as punched card readers (…) and new technologies not yet invented, are covered by this drafting* [i.e. by the Directive]. *Similarly, the key terms used in the Directive are either defined in technology neutral language (…) or are left undefined. (…) The obligations imposed upon controllers and processors are non-technological and focus on behaviours such as fair and lawful processing (…), taking reasonable security precautions (…), providing information to data subjects (…) and the like. Overall, it is not possible to identify any provision of the Directive which does not apply to current technologies for processing personal data, or which would not apply to any such technology whose future development can currently be envisaged.*"[61]

In the current text of the Proposal, this principle has been mentioned only in the preamble: in recital 13 (*"The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention"*) and recital 66 (*"When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation (…)"*). At the same time, however, the Proposal contains provisions and **solutions that raise some doubts** as to their compliance with the principle in question, in particular:

- the definition of "data subject" (cf. section 3 above) lists "online identifiers", and furthermore recital 24 of the preamble mentions specific technological solutions, such as Internet Protocol addresses and cookie identifiers, in spite of the fact that the Commission itself stated that *"[d]etailed references to specific technologies would jeopardise the proven technological neutrality of the Directive and risk gaps when technology advances"*;[62]

---

[60] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, 'Towards a new Framework for Electronic Communications Infrastructure and Associated Services: The 1999 Communications Review', COM (1999) 539 final, p. 14.

[61] Ch. Reed, 'The Law of Unintended Consequences – embedded business models in IT regulation', Journal of Information, Law & Technology, 2007, available at SSRN: http://ssrn.com/abstract=1017290, p. 4-5. See also report from the European Commission, 'First report on implementation of the Data Protection Directive (95/46/EC)', COM(2003) 265 final, p. 20, and Commission Staff Working Paper, 'Impact Assessment', SEC(2012) 72 final, Annex 1. Current EU Legal Instruments for the Protection of Personal Data', p. 10.

[62] Commission Staff Working Paper, 'Impact Assessment', SEC(2012) 72 final, Annex 2. Evaluation of the Implementation of the Data Protection Directive, p. 16.

- also the concept of the "right to be forgotten" is not devoid of certain specific technological "influences", related, for example, to deleting links (cf. Article 17(1) and 17(9)(b) of the Proposal);
- there are also certain doubts about the provision of Article 32(3) of the Proposal, which refers to *"technological protection measures [that] render the data unintelligible to any person who is not authorised to access it"*;[63]
- furthermore, on several occasions, the Proposal makes references to the electronic format, for example in Article 12(1) or, in particular, in Article 18(1), concerning the "right to data portability".

As emphasised in the legal literature – based on the example of the "right to be forgotten" and "data portability" – *"through the introduction of these two rights* [...]*the Commission seems to be particularly engaged with social networking websites and, indeed, the current internet state of play. As such, this may prove a risky law-making option: legislating in a constantly evolving field risks making the law seem outdated and irrelevant"*.[64]

It seems, therefore, to be highly recommended to expressly **define the technological neutrality principle** in the text of the Regulation (e.g. in Article 5).[65] Such a principle would be of great importance not only for the EU legislator during work on the Package, but also after the adoption of the Regulation, in particular for the Commission, in the context of its broad powers to adopt secondary legislation elaborating on such issues and concepts as privacy by design (Article 23(4)), data portability (Article 18(3)) or the right to be forgotten (Article 17(9)), which have been introduced by the Package, and include references to such conditions as "electronic format", "structured format which is commonly used" or "technical standards". Also, the provisions of the Proposal, in particular those identified in this analysis, require appropriate adjustment to the principle of technological neutrality.

### 1.2.8. Re-use of public information

The principle of access to public information, including official documents, especially in the context of re-use of such information, has not been expressed in the text of the proposed General Data Protection Regulation, although it was mentioned in recital 18, which reads as follows:

> "*This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation*."

The Package should **concentrate on re-use of public information**, since there are currently serious obstacles with regard to such re-use in the light of data protection regulation. They are related to the fact that Directive 2003/98/EC ("PSI Directive") does not exclude the application of data protection provisions, on the contrary, in recital 21 it notes that the PSI Directive *"should be implemented and applied in full compliance with the principles relating to the protection of personal data"*, and in Article 1(4) it declares that the PSI Directive *"leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data"*.

---

[63] See UK Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' (2012), p. 18.

[64] P. De Hert, V. Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', Computer Law & Security Review 28 (2012), p. 138.

[65] See also European Data Protection Supervisor, 'Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"' (14.01.2011), para. 39, or American Chamber of Commerce to the European Union, 'Response to the Commission communication on a comprehensive approach on data protection in the European Union' (14.01.2011), p. 13-14.

The main obstacles with regard to re-use of public information, especially for commercial purposes, are connected with:

- indication of the basis for personal data processing for re-use purposes: if no consent is obtained from data subjects (which is the rule), such a legal basis should be sought in legitimate interests pursued by the controller, which is very difficult;
- additional difficulties are associated with the processing of sensitive data: as regards re-use for commercial purposes, it is almost impossible to find a legal basis in Directive 95/46/EC;
- purpose limitation principle, which is in this context the key obstacle, fundamentally impossible to overcome: as noted by Article 29 Working Party, *"[i]f personal data are to be re-used for commercial purposes, this secondary purpose may be considered as incompatible and thus the information not be disclosed"*;[66]
- transparency obligations: they require both public entities (which render data available) and private entities (re-using the data) to properly notify all data subjects.[67]

[66] Article 29 Data Protection Working Party, 'Opinion 7/2003 on the re-use of public sector information and the protection of personal data', WP 83 (12.12.2003), p. 9.

[67] See detailed analysis in this respect, B. van der Sloot, 'Public Sector Information & Data Protection: A Plea for Personal Privacy Settings for the Re-use fo PSI', 2011, available at: http://www.ivir.nl/publications/sloot/Public%20sector%20information%20and%20data%20protection.pdf

The Proposal, in its current form, does not at all facilitate any re-use of public information, especially for commercial purposes, apart from minor exceptions. For example, Article 14(5)(b) of the Proposal waives the notice (information) obligation where the data is not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort (similarly, Article 11(2) of Directive 95/46/EC). The application of this exception, however, is problematic and, as a general rule, should be limited. The fact that there is no regulation, or even discussion, in this regard prevents the possibility of realising the full potential of public information, and ultimately the development of EU businesses, including SMEs, innovation, open data projects,[68] and, consequently, the economic growth of the European Union. This discussion needs to take account, in particular, of the purpose limitation principle, as indicated by the European Data Protection Supervisor:

> "*In particular, it is not easy to implement the principle of purpose limitation effectively in case of PSI reuse. On the one hand, the very idea and driving force for innovation behind the concept of 'open data' and PSI reuse is that the information should be available for reuse for innovative new products and services, and thus, for purposes that are not previously defined and cannot be clearly foreseen. On the other hand, purpose limitation is a key data protection principle and requires that personal data that have been collected for a specific purpose should not at a later stage be used for another, incompatible purpose, unless certain additional conditions have been met. (…) It is not easy to reconcile these two concerns (open data and data protection).*"[69]

## 1.3. Recommendations

In the context of new technology, and key concepts of personal data protection that are "technology sensitive" and have been dealt with in the Proposal (e.g., the definition of "personal data", the so-called "household exception", "measures based on profiling"), there are a number of recommendations which can be made, also relating to policy:

1. The method of defining the key concept of "personal data" should not be changed, as it allows – due to the flexibility and wide range of applications – implementation of the objectives of the Regulation, related, in particular, to the protection of individual rights. However, the proposed definition of "personal data" requires refining and clarifying as follows:
    - its further streamlining,
    - preservation of the "relative approach",
    - explicit qualification of online identifiers.
2. Further legislative work should pay greater attention to the issues of anonymisation and pseudonymisation of data, in particular in terms of:
    - creating a system of incentives for initiation of those processes,
    - determining the conditions for effective anonymisation,
    - clarifying the requirements for data pseudonymisation, in conjunction with the "benefits" that may be associated with that process.

---

[68] See in particular Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Open data. An engine for innovation, growth and transparent governance', draft, 2011, available at: http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive_proposal/2012/open_data.pdf

[69] Opinion of the European Data Protection Supervisor on the 'Open-Data Package' of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the reuse of Commission documents, 18.04.2012, para. 20.

3. In terms of defining the term “data controller” (Article 4(5) of the Proposal), there are doubts about the added provision that data controllers also determine the “conditions” of data processing. It seems that the definition of “data controller” should be limited to determining the “purposes” of data processing.

4. The Proposal should be refined as regards precise division and determination of the obligations and responsibilities of the data controller and data processor.

5. The text of Article 2(2)(d) of the Proposal (the so-called “household exception”) should be limited to the condition of “exclusively personal or household activity”. Any possible additional restrictions and reservations regarding the exception (e.g. making data “accessible to an indefinite number of individuals”) should be adopted solely in the preamble to the Regulation, taking account of their impact on other values, in particular freedom of expression.

6. Article 20 of the Proposal (“measures based on profiling”) and the underlying regulatory approach require fundamental rethinking, taking into account the broader context, the differences in “profiling” in the different sectors of the economy or legal relations, as well as taking into account the consequences of overly restrictive regulation in this area.

7. The wording of Article 20 also requires clarification, particularly as regards such key phrases as “produces legal effects”, “significantly affects”, “suitable safeguards”, and “suitable measures”.

8. Detailed analysis and decision (mostly political) is required as regards the issue of permissible further processing of data for purposes incompatible with the one for which the personal data have been collected, also on the legal basis of legitimate interest pursued by the controller (Article 6(4) of the Proposal). In this context, additional precision would also be required in the case of the notion of “compatible use”.

9. Due to continuing technological development reflected in the wording of the Proposal as well as in the context of the broad powers available to the Commission, it would be highly recommendable to expressly define the technological neutrality principle in the text of the Regulation (e.g. in Article 5).

10. The Package, as well as discussion concerning it, should also concentrate – in the context of new technologies – on the issue of re-use of public information, since currently there are serious obstacles with regard to such re-use in the light of data protection regulation.

# 2. ANALYSING THE INTERNAL MARKET DIMENSION

The purpose of this chapter is to explore the internal market dimension of the proposal for a Data Protection Package.[70] This will be achieved through an evaluation of key elements such as the shift of the legislative instrument (from directive to regulation), the 'one-stop shop' principle regarding the competent supervisory authority in cross-border cases or the marketplace principle (which makes EU data protection standards also applicable to businesses based outside the EU, if they are active within the EU). Further attention is given to new strategies for implementing data protection standards such as 'privacy by design' and 'privacy by default'.

## 2.1. EU-wide level playing-field as a result of modernisation of the legal framework

### 2.1.1. Change of legislative instrument: Regulation instead of directive: a single law with fewer differences in cross-border cases.

The proposal for a Data Protection Package[71] consists of two legislative proposals, one of them being a regulation, the other a directive:

- 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.

Both measures are intended to replace the centrepiece of existing EU legislation on personal data protection, Directive 95/46/EC.[72] Internal market aspects are only concerned by the legislative proposal for a General Data Protection Regulation. In this field there is thus a fundamental change of the legislative instrument. Instead of a directive, a regulation will be passed. Following the passing of a regulation, there would no longer be several individual transposition laws of the Member States, but an EU single data protection law (i.e. the General Data Protection Regulation) would apply across the whole EU. This would in particular disburden businesses from dealing with the individual transposition laws of the Member States which currently vary quite significantly.[73] This would be an improvement of the functioning of the Internal Market since the same set of rules would apply throughout the EU irrespective of where business and client are based. Businesses will not any more have to take care of the differences of the national transpositions of EU law. A regulation provides greater clarity through uniform definitions and provisions aimed at ensuring a more harmonised application of the law, thus facilitating the free movement of data.

---

[70] COM (2012) 9: Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century.

[71] COM (2012) 9: Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century.

[72] 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 ofsuch data, OJ L 281, 23.11.1995, p.31.

[73] See the rich materials collected by the Commission on the transposition of Directive 95/46/EC, e.g. COM(2007) 87 on the follow-up of the Work Programme for better implementation of the Data Protection Directive and the further materials available at: http://ec.europa.eu/justice/policies/privacy/lawreport/index_en.htm#ep_report

However, the argument is often brought forward that even under a regulation it is likely that there will be differences in the way in which the regulation is interpreted and enforced in practice. Such differences will in particular arise because of the principle-based style of legislation. It is important to note that such a principle-based approach has enormous advantages, since it is flexible, adaptable and hard to circumvent. It also makes the regulation prospective in outlook, or future-proof, with regard to the development of new technologies or practices of data controllers or processors. The approach is, however, inherently uncertain. Open-textured norms and broad concepts in the style of general clauses (such as the "legitimate interest test") are very likely to be interpreted and applied differently given a backdrop of many different legal cultures and traditions.

It should be noted, however, that under the Proposal differences of interpretation and enforcement will have less importance for businesses than under the current system of 27 transposition laws. The main reason for this is that the one-stop-shop principle ensures that the same national supervisory authority always interprets and enforces the Regulation against a certain data controller or processor. Differences in the way in which the regulation is interpreted and enforced in practice should not occur in cases where the one-stop-shop principle applies (see also below 2.1.2). Both the uniform set of rules and the interpretation of these rules by the competent supervisory authority under the one-stop-shop principle may in particular contribute to the further development of the internal market in the area of e-commerce. In the example of an e-shop which targets all Member States, these measures should facilitate the setting up and running of a uniform business model which is lawful relating to data protection standards in all Member States. Insofar the new legislation creates uniform rules and their uniform application by supervisory authorities and courts, the e-shop owners will be disburdened from the necessity to accommodate their e-shops to specific rules or administrative practices of individual Member States.

There are, however, still some remaining differences of the national laws. The Proposal allows Member States to autonomously pass additional measures on matters such as health, employment and professional secrecy.[74] Moreover, the sanctions for any breach of the provisions of the regulation are, as long as they are effective, proportionate and dissuasive, at the discretion of the Member States.

Finally, the organisation, the resources and the attitudes of national regulators and administrations may vary. There is a concrete risk that, despite the uniform regulation in all Member States, the "law in action", meaning the actual level of enforcement, will differ considerably. This risk has an influence on the actual level of data protection. It also has implications for the functioning of the internal market, since data controllers or processors, who are based in an EU Member State where enforcement standards are low, may be at a competitive advantage. Gaps will remain in the intended level playing-field for as long as a certain minimum standard of enforcement is not ensured throughout the EU.

[74] Articles 80-85.

The tools in the regulation for a regular monitoring of actual implementation and enforcement in all Member States should therefore be strengthened. Moreover, the risk of a different interpretation or application, in particular of wide concepts and open-textured norms, could be minimised by EU-wide databases on the legal practice under the Regulation. A model could be the obligation of Member States in the proposal for a Common European Sales Law to communicate judgements to the Commission which must set up a public database on such judgements.[75] Following the model of the already existing database on cases in consumer law (the 'Consumer Law Compendium') such judgements, of at least an abstract and the operative part, will have to be translated into several working languages in order to be useful to as many users in Europe as possible.[76]

### 2.1.2. Jurisdiction and competence of supervisory authorities (one-stop shop)

The provisions on the competence of the supervisory authorities in Article 51 contain an important innovation. Article 51(1) provides for the competence of each supervisory data protection authority on the territory of its own Member State. This is the traditional general rule, similar to Article 28(6) of Directive 95/46/EC. This general rule is complemented by Article 51(2) which states that the supervisory authority of the Member State where a controller has its main establishment is competent for the supervision of processing activities in all Member States ('one-stop shop') where processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union,and where the controller or processor is established in more than one Member State.

The one-stop shop of art. 51 (2) principle may have enormous advantages for businesses who make use of the internal market since they only have to deal with one authority instead of many under the current legislation. This reduces costs, ensures unity of application and increases legal certainty.

However, the current draft of the Proposal contains several gaps or ambiguities which might be improved in further stages of the legislative process. Firstly, the definition of main establishment in Article 4 (13) and in recital 27 is not very clear and therefore there is a lack of clarity in establishing the competent authority in cross-border cases. A clear understanding of the term 'main establishment' is crucial, as it is decisive for determining the competent authority in the meaning of Article 51(2).[77]

Secondly, the one-stop shop principle in Article 51(2) only applies to the situation where the controller or processor has more than one establishment within the EU. Seemingly, it does not apply to the situation where there is no establishment in the EU at all, but where the processing activities of an extra-EU business are related to the offering of goods and services to data subjects in the Union or the monitoring of their behaviour, according to Article 3(2). In this case, each supervisory authority in each Member State affected by

---

[75] Cf. Article 14 (Communication of judgments applying this Regulation) of the Proposal (COM(2011) 635) which reads: (1) Member States shall ensure that final judgments of their courts applying the rules of this Regulation are communicated without undue delay to the Commission. (2) The Commission shall set up a system which allows the information concerning the judgments referred to in paragraph 1 and relevant judgements of the Court of Justice of the European Union to be consulted. That system shall be accessible to the public.

[76] As for the methodology see H. Schulte-Nölke, 'The EC Consumer Law Compendium: A Pan-European Knowledge Base for Politicians, Businesses and Consumer Organisations', European Business Law Review 20 (2009) 383-389; cf. also the accompanying database, which displays core information on many hundreds of consumer law cases in English, French and German. The database is accessible via the homepage of the European Commission at: http://ec.europa.eu/consumers/rights/cons_acquis_en.htm#comp

[77] Cf. eg, the criticism of the Art. 29 Working Party, 'Opinion 01.2012 on the data protection reform proposals' (23.03.2012) WP 191 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf (p. 10).

processing operations is competent under to Article 51(1). The effect is that the privilege of the one stop shop is only granted to businesses which are established in the EU. If such discrimination of businesses without any establishment in the EU is not wanted, a provision on criteria for determining the competent supervisory authority should be inserted for cases where there is no establishment in the EU.

Thirdly, it is rather unclear how the competence of the competent authority in the meaning of Article 51(2) relates to the consistency mechanism. It is in particular not clear to what extent it is exclusive. It seems that the competence of the competent authority in the meaning of Article 51(2)is subject to the obligations to cooperate, provide and accept mutual assistance, and make use of the consistency mechanism, as stipulated in Chapter VII on consistency and cooperation. This could be clarified in the proposal. The more market friendly approach would be the exclusive competence of one supervisory authority of one Member State.

Moreover, it has been argued that the rule on the one-stop-shop (Article 51) should be amended so that groups of businesses should also have the privilege of only being subject to the monitoring of one single data protection authority. The reason for this seems to be that a company based in one country which has only non-independent branches without legal personality in other countries is only subject to the control of the data protection authority in the country where it is established. In contrast, a group of businesses, where, for instance, a controlling company has sub-entities or other subsidiaries with legal personality, has to face measures of all national data protection authorities and regulators of the Member States where such subsidiaries have their seat. It is of course true that such amendment of article 51 could be beneficial to such groups of businesses since they may standardise their data-protection strategies and practices across the EU without needing to communicate with several Member State regulators.

It should be noted that the Proposal contains a definition of the term “group of undertakings” in art. 4 (16). This definition is supplemented by recital (28), which reads:

> (28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.

It should further be noted that the Proposal only contains a few provisions by exception on groups of undertakings, in particular relating to the data protection officer (art. 28) and binding corporate rules (art. 43). These are cases where the proving of the fact that the undertakings form a group in the sense of the Regulation depends on the co-operation of the members of the group which will usually have an interest in establishing their nature as a group.

In contrast to these exceptions, the main addressee of data protection rules in the Proposal is a concrete individual (natural or) legal person,[78] not a group of persons. The reason for this is evident, since any legal action of supervisory authorities must also have a clear addressee, i.e. the (alleged) wrongdoer. It is hardly imaginable how an order to comply with data protection rules or a ban on processing under art. 53, or even administrative sanctions including fines under art. 79 could be enforced against a group of undertakings. In these cases the undertakings which form a group in the eyes of the supervisory authorities, do not have an interest in co-operating to prove that they form a group. Moreover, if parts or the group, usually including the controlling undertaking, are based outside the EU, the enforcement, in particular fines of up to 2% of the annual turnover of the whole group, may be too high to bear for the members of the group based within the EU.

A broadening of the rule on the one-stop-shop (Article 51) along the lines that groups of businesses also have the privilege to only be subject to the monitoring of one single data protection authority would have to be a double-edged sword for such groups.

It would only be acceptable if a group of undertakings irrevocably,

- declared itself a group of undertakings in the sense of the Regulation also for the purposes of being jointly monitored and penalised under the Regulation;
- accepted a joint and several obligation to comply with all provisions of the Regulation;
- accepted a joint and several obligation to fulfil to any sanction, including fines, to the full extent by any member of the group.

It is therefore recommended that art. 51 be amended in favour of groups of undertakings only if these requirements are inserted in the Regulation.

## 2.2. Enforcement Problems

Differences in the practical application of EU data protection rules by the different national supervisory authorities may cause enforcement problems. If it were true that regulators in some Member States are less pro-active than in others, data controllers or processors might utilise the single market provisions, in particular the one-stop-shop principle in art. 51 of the Proposal, by establishing a subsidiary in a Member State where one of the less active administrations is to be found and thereby avoid the more pro-active regulators.[79] For example, until now, the data protection authority of the Federal State of Hamburg had been rather active in enforcing European data protection standards against big US companies such as Google and Facebook. The one-stop-single market principle would allow such companies to avoid the Hamburg authority by establishing themselves in, say, Ireland.[80]

[78] Cf. also the definitions of controller and processor in art. 4 (5)(6).

[79] Allegedly Ireland could be an example for a "friendly jurisdiction within the European Union" where data controller might establish in order to avoid some of the more enthusiastic national regulators; see a newsletter of the law firm Linklaters on Technology Media and Telecommunications, p.9 (to be downloaded under http://www.linklaters.com/pdfs/mkt/london/January_2012_Newsletter_PDF.pdf)

[80] Cf. however the press release of the Hamburg Commissioner for Data Protection and Freedom of Information of 7 June 2012 on a halt of the legal action against the Facebook automatic face recognition function because of negotiations between Facebook and the Irish Data Protection authorities, http:www.datenschutz-hamburg.de/news/detail/article/verfahren-gegen-facebook-vorlaeufig-ausgesetzt.html

The Proposal already contains several instruments which could help to counter-act such strategies, e.g.:

- The right of supervisory authorities to participate in joint operations of supervisory authorities under art. 56;
- The consistency mechanism under art. 57 ss. (in particular the right of any supervisory authority or the European Data Protection Board to request that matters where a supervisory authority does not comply with its obligations in cross-border cases shall be dealt with under the consistency mechanism);
- The urgency procedure under art. 61 (under which any supervisory authority may adopt provisional measures with a specified period of validity);
- The right of each data subject to a judicial remedy obliging the supervisory authority to act on a complaint under art. 74 (proceedings have to be brought before the courts of the Member State where the supervisory authority is established).

Procedures under these rules which are aimed at preventing the evasion of the enforcement of pro-active data protection regulators may, however, become rather complicated and time-consuming. A more direct method of regulation would be to broaden the competences of the European Commission (possibly in co-operation with the European Data Protection Board) by creating:

- A right of any data subject and any supervisory authority to complain to the European Commission that the solely competent supervisory authority of the controller's or processor's main establishment responsible under art. 51 (2) is not properly fulfilling its tasks;
- A right of the European Commission (after a hearing of the European Data Protection Board) to publicly express the opinion that the solely competent supervisory authority of the controller's or processor's main establishment responsible under art. 51 (2) is not properly fulfilling its tasks.

Although it may be politically difficult to find support for such far-reaching competences of the European Commission in the Member States, the efficiency of the enforcement of data protection rules under the Proposal might be increased.

## 2.3. Securing competitiveness of EU-based service providers by the marketplace principle: extra-territorial application

A fundamental shift in comparison to the existing legislation in Directive 95/46/EC is the marketplace principle. The effect is that businesses not established in the Union will have to comply with the EU data protection standards (and not just with the often lower standards of the state in which they are established). This innovation is set out in the article on the territorial scope of the Regulation (art. 3). Under paragraph (1) of this article the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor of information in the Union.

This is still in line with the traditional approach of the current EU data protection legislation. The real innovation lies in paragraph (2) of the same article, under which the regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union where the processing activities are related to:

- the offering of goods or services to such data subjects in the Union, or
- the monitoring of their behaviour.

In particular, this scope also ensures that controllers not established in the Union have to apply EU-law.

### 2.3.1. Effect on the Internal Market: EU-wide level playing-field for all actors

This core innovation of the proposal will not only improve the data protection standard within the EU,[81] but also ensure the better functioning of the internal market. By making EU data protection legislation applicable to all providers active within the EU, potential disadvantages which are faced by service providers based within the EU due to its stricter data protection legislation will be ironed out. This would create an EU-wide level playing-field and could therefore improve the competitiveness of service providers based within the EU.

From the perspective of the functioning of the internal market, differences of the data protection regulation within the EU and outside of it may have the effect that the value of the main currency paid in exchange for services, i.e. personal data disclosed by the user, may vary. One aim of EU data protection regulation should therefore be to ensure a level playing-field also by regulating the value of such data given in exchange for services. A real level playing-field will only exist, if data given by data subjects in exchange for online services have the same value. If, however, differences in the level of data protection regulation result in varying levels of personal data on offer, online service providers are faced with different currencies in the same market. A level playing-field therefore requires a similar data protection level within and outside the EU in order to avoid differences of the main currency of many online services, i.e. personal data of data subjects.

The new draft legislation would therefore dramatically change the legal position of some of the very big data controllers established outside of the European Union, in particular the big US tech companies. Some of these companies may have kept much of their data processing in the US or in other third countries in the past to avoid becoming subject to EU data protection law under the current Directive. Those who intend to do business in the EU and want to collect personal data will also be subject to EU data protection legislation in the future even when their servers and headquarters are located outside the EU ('marketplace principle'). This change could remove a potential barrier to trade militating against the transfer of activities to the EU.

It is self-evident that enforcement of EU data protection rules on businesses based outside the EU may be faced with some problems. However, since at least the big data controllers and processors of data usually have an establishment within the EU, they are subject to enforcement measures by the EU Member States. It remains to be seen to what extent European supervisory authorities will be able to tackle infringements of data protection rules by controllers or processors based outside the EU and how they will find ways for enforcement.[82]

[81] See Chapter 3 of this study.

[82] See for example the proceedings of the Hamburg Commissioner for Data Protection and Freedom of Information against Facebook and Google: http://www.datenschutz-hamburg.de/pressemitteilungen-und-informationen/pressemitteilungen.html

### 2.3.2. The example of face recognition

The current proceedings of several European data protection authorities against the collection of biometric data by Facebook may serve as an example for the difficulties of deviating data protection standards and specific enforcement problems. In June 2012, the Hamburg Commissioner for Data Protection and Freedom of Information postponed an envisaged injunction against Facebook for its practice of biometric data-collection. Negotiations between the Irish Commissioner for Data Protection and Facebook concerning the use of the facial recognition function were allegedly soon to be settled. Following these negotiations Facebook announced to temporarily refrain from creating facial profiles of future users until a final solution is settled. However, the company refused to accept further obligations.[83] The already existing database containing biometric patterns of users is clearly in conflict with EU data protection requirements. Under EU standards, Facebook would be obliged to delete this data unless it obtains approval by all concerned users.

However, the existing EU data protection legislation only applies to Facebook because the company has establishments within the EU (among others in Hamburg and Dublin). If Facebook operated without any establishment within the EU, the existing EU data protection requirements would not be applicable to Facebook. The new regulation would close this loophole.

### 2.3.3. Applicability to personal data processed within the EU, but with no relationship to the data subjects in the EU?

The provision on scope in art. 3 (1) of the Proposal may have (as is already the case under the current EU regulation) a negative effect on EU-based data processors who want to offer their services to clients outside the EU. In the example of an US-based business with solely US clients (i.e. data subjects) which wishes to make use of the services of a data processor based in a EU Member State, the Proposal will probably apply to the EU-based data processor under art. 3(1). In particular, if the data protection standard of the countries where the data subjects are based is lower than in the EU, the applicability of the EU data protection regulation on the EU-based data processor may constitute a barrier to trade, since the EU-based data processor may have to fulfil data protection requirements that are not applicable to competitors outside the EU. Moreover, the Proposal may make the processing of personal data in the EU less attractive to non-EU entities. Therefore it has been suggested that article 3 (1) be amended in order to make clear that personal data of data subjects with no relationship to the EU which is processed in the EU will be exempted.[84]

---

[83] http://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/PressRelease-2012-08-15-Facebook_Proceedings.pdf

[84] See for example the response of the Association for Financial Markets in Europe (AFME) and the British Bankers' Association (BBA) of 6 March 2012 to a call for evidence of the UK Ministry of Justice, p. 3.; available at: http://www.bba.org.uk/download/7512

There is indeed some truth in the argument. It is important, however, that such an exemption does not lead to a lacuna in data protection. Disapplying the general data protection regulation for EU-based data processors that process the personal data of data subjects with no link to the EU could lead to the result that the activity falls completely out of the scope of monitoring by any data protection authority. This is the case where the regulators of the country where the data subjects are resident do not have the competence to take action against data processors based in foreign countries (or actually do not take action against them even if they have the competence). Such an exemption from article 3 (1) of the Proposal would allow businesses, which are based in countries which do not apply their national data protection legislation on data processors based outside their territory, to make use of a data protection gap. For this reason, the proposed amendment of article 3 (1) is not recommended.

## 2.4. Accountability instead of notification

The Proposal abolishes the obligation of data controllers or processors to make a general notification about their processing to their national regulator. The duty to notify is replaced by the more general principle of accountability.[85] Besides the duty to appoint a data protection officer, to adopt mutable policies and measures to demonstrate compliance and to carry out data protection impact assessments, data processors must install systems of "privacy by design" and "privacy by default".[86] The general idea is that tools for facilitating ex-post supervision are being replaced by instruments that increase the probability of ex-ante compliance with data protection rules. Although these innovative concepts and ideas are, in principle, introduced into the Regulation, the respective provisions are rather vague and give broad discretion to the data processors. The regulation could be improved by more precision, in particular giving some model examples of what such measures could look like.

### 2.4.1. Notion of "privacy by design" and "privacy by default"

The basic idea of "privacy by design" is to envisage data protection measures already when creating new technologies, services or social media. The emphasis of this concept is on the implementation of such measures during the development stage of the product and before any problems in relation to data protection occur after the product has been launched. The concept has been developed due to the common finding that new technological products import difficulties related to data protection which tend to appear after their development. Once a product has been fully developed, it is more difficult to correct and erase any security vulnerabilities. Privacy by design becomes relevant both in the phase of planning and of construction. It involves the principle of minimal acquisition of data ("data thrift").

The main advantage of this approach is the saving of resources and time which it would otherwise take in order to rework the product. Additionally, privacy by design takes preference by finding alternative solutions of preventing the emergence of problems related to data protection over trying to solve problems after they arise.

[85] Cf. Art. 22 of the Proposal.
[86] Cf. Art. 22 of the Proposal.

"Privacy by default" means that the basic implementation of data protection measures is provided by the producers of technologies, services and social media which typically deal with personal data. The crucial aspect of this idea is the existence of a presetting that is in favour of protecting the data of any user or third person possibly involved in the procession of the data. "Privacy by default" uses as a starting point the experience that many users are not aware of the (not very high) level of data protection they are subject to when using for example social media.[87] Therefore, they cannot be expected to take measures for the protection of their personal data by themselves. That is the reason why it is considered necessary to ensure that the presetting provided by the service provider at least secures a sufficiently high level of protection. As well as "privacy by design", "privacy by default" involves the principle of "data thrift", since this principle generally provides for a higher level of protection since it lowers the risk of security vulnerabilities due to the fact that the amount of data being recorded is restricted to a minimal amount from the beginning. An example for "privacy by default" would be a browser that is preset in a way either not allowing cookies to pop up at all or prompting users to give their consent before any cookies are allowed. For social media, it could mean a presetting that does not declare a user's profile generally public, but that leaves it to users themselves to determine whether their profiles are to be seen by the public or not.

### 2.4.2. Implementation of "privacy by design" and "privacy by default" in the Regulation

Article 23 clarifies the obligations of the controller in relation to privacy by design and default when stating the obligation to implement appropriate "technical and organisational measures" in order to meet the requirements set out by the Regulation. This must be done not only when personal data is being processed, but already when determining the means for processing. In addition, the provision reiterates the principle of data minimisation as set out in Article 5. Article 23 especially mentions the importance of a presetting to ensure that any personal data is not to be seen by an indefinite number of people. The provision does not further elaborate the aims and techniques of privacy by default.[88]

However, the obligation is qualified by adding "having regard to the state of the art and the costs of [...] implementation". This might be a gap for controllers through which they can try to escape the obligations as they are set out. The costs of IT-services and any measures related to them are often difficult to determine and may usually require professional knowledge.

Article 30 of the Regulation describes the obligations named in Article 23 in terms of ensuring the security of the processing of personal data. Again, any measures have to be taken "having regard to the state of art and the costs of their implementation".

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.[89] 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.

---

[87] See "Social Networking", a quantitative and qualitative research report into attitudes, behaviours and use page 51, available at: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/report1.pdf, recalled the 28th of June 2012.

[88] Opinion of the European Data Protection Supervisor on the data protection reform package, p. 29/30.

[89] Opinion of the European Data Protection Supervisor on the data protection reform package, p. 30.

Furthermore, the Regulation does not clearly state how a processor is to be bound by privacy of design[90] except indirectly through Article 27.

In general terms, the draft merely scratches the surface. Data protection by design is not elaborated in detail. In particular it does not refer to general principles of data protection through technology (most notably, there is no mentioning of anonymisation and pseudonymisation).[91] Under the Proposal, the practical effect of data protection by design will mainly depend on the delegated acts and technical standards enacted by the Commission under to Art 23 (3) (4) and Art 30 (3).

### 2.4.3. Example: Information on data automatically transferred by browsers

Internet browsers usually convey data in particular on technical aspects of the software on the data subject's computer to any service provider when entering its homepage. This data includes information on which browser is being used, which version of the browser and under which operating system the computer is running, as well as the IP-address, the fonts installed on the computer and the location where the data subject logged onto the internet. Such information may be very useful for the data subject, since it ensures that the service provider's homepage is properly displayed on the data subject's screen. For example, if the service provider detects that the data subject is using a mobile phone with a smaller screen, the format of the data provider's homepage can be adapted to this. Such data is usually stored in so-called logs and can be analysed later. Internet activists such as the US civil citizens' rights organisation Electronic Frontier Foundation (EFF) allow data subjects to check which information is automatically provided by their system.[92] Data protection regulation could oblige service providers to make the information which is being automatically stored in the data provider's logs more easily accessible to data subjects. Service providers could be obliged to offer a button or link on their site where data subjects could easily check which information is automatically provided by their browsers. Moreover, service providers could be obliged to inform the user of the possibility of presetting the data subject's browser so as not to deliver certain information (e.g. the place where the data subject has logged into the internet).

### 2.4.4. Example: Presetting "Do not track" feature of browsers

The new initiative, among others backed by the US government,[93] "Do not track" seeks to oblige providers of internet browsers to offer their customers a "Do not track" feature which would make it very easy for users to deliberately agree or disagree to tracking activities by service providers when visiting their homepage. In December 2010, the American Federal Trade Commission issued a privacy report that called for a "Do not track" system that would enable people to avoid having their actions monitored online. Several companies which provide frequently used browsers, such as Microsoft (Internet Explorer), Mozilla (Firefox), Apple (Safari), Opera and Google (Chrome) generally expressed support.

As development currently stands, the "Do not track" system accepts three values: 1 in case the user does not wish to be tracked (opt out), 0 in case the user consents to being tracked (opt in), or null if the user has not expressed a preference.

---

90 Opinion of the European Data Protection Supervisor on the data protection reform package, p. 29.

91 See below under point 2.6.

92 Cf. https://panopticlick.eff.org.

93 Cf. the CONSUMER PRIVACY BILL OF RIGHTS issued by the White House in February 2012, p. 12 ss, to be downloaded under http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

The principle of privacy by default would require that the presetting of such feature is "Do not track" (1) or no preference (null) instead of consenting to tracking by default (0). The latter is supposedly planned by the browser providers. The American Federal Trade Commission[94] and the European Commission[95] have raised objections against this. The proposed EU data protection regulation could clarify that – as an application of "privacy by design" – browsers should have such features and – as an application of "privacy by default" – the presetting should be "Do not track".

Moreover, under the current regulation, websites may not be required to comply with "Do not track" requests, neither by law, nor by broad social consensus, and therefore, very few websites might recognise and respect the privacy signal issued by setting the "Do not track" feature. The system would then just rely upon honour and etiquette on the part of the service provider. Under the Proposal an activated "Do not track" setting might be understood as refusing to give consent to the processing of data typically transmitted by web browsers. The Regulation could clarify this.

## 2.5. Recommendations

On the basis of the findings made in this chapter, the following recommendations can be made:

1. Strengthening of the tools for a regular monitoring of the actual implementation and enforcement in all Member States.
2. Adding precautions for the case that the solely competent supervisory authority of the controller's or processor's main establishment, responsible under art. 51 (2), does not properly fulfil its tasks, e.g. a right of the European Commission (after hearing European Data Protection Board) to publicly express the opinion that the solely competent supervisory authority of the controller's or processor's main establishment responsible under art. 51 (2) is not properly fulfilling its tasks.
3. Broadening the rule on the one-stop-shop (Article 51) with the purpose that also groups of businesses have the privilege to be subject to the monitoring of one single data protection authority (under strict conditions).
4. Creation of EU-wide databases on legal practice under the Regulation according to the model in the Commission Proposal for a Common European Sales Law.
5. Requiring that browsers offer a (preset) "Do not track" feature and clarifying that data controllers and processors must respect the data subject's wish for privacy, if the "Do not track" option is set.

---

[94] See the FTC Privacy Recommendations of March 2012, p. 53 available at: http://www.scribd.com/doc/86771514/FTC-Privacy-Recommendations

[95] Cf. letter of the Director-General of DG Information Society and Media Directorate-General Robert Madelin, to be downloaded under: http://lists.w3.org/Archives/Public/public-tracking/2012Jun/att-0604/Letter_to_W3C_Tracking_Protection_Working_Group.210612.pdf

# 3. STRENGTHENING THE RIGHTS OF THE CONSUMER IN THE AREA OF DATA PROTECTION

Chapter two explored the internal market dimension resulting from the problems faced in light of the developments in the area of IT and services explained in Chapter one. The purpose of this chapter is to explore the impact of the issues brought about by new technologies and services from the perspective of consumer rights. This will be achieved through an evaluation of measures for strengthening the rights of consumers in relation to the mapped multitude of new technologies. Before focus can be given to key elements in data protection that are important for adequate consumer protection it is necessary to re-contextualise the business model upon which the new technologies are based in relation to consumer protection.

## 3.1. The impact of new informational technologies and services on consumer protection

### 3.1.1. Consumer awareness about the data collected about them and its use

Establishing what data is collected by service providers and, perhaps more importantly, what they do with it is a difficult task.[96] It is complicated by the ever increasingly globalised nature of data flows. This translates into **a clear informational gap faced by consumers** caused in large part by a lack of transparency about what type of data and how much of it is being collected and commercialised through the use of internet services. Especially where the data collected about consumers concerns biographical information, information about political views and beliefs and other such sensitive information, known under the collective term of "personal life information", there is a real danger of violating consumers' fundamental right to privacy as well as more particularly the right to data protection.[97] It can therefore be stated as an important basic principle contributing to consumer protection that consumers should be made aware what information is being collected about them and how it is being used.

### 3.1.2. The balance between consumer autonomy and consumer protection

This state of affairs is intensified in the case of 'free' online services. It is a characteristic business model of online services, which are seemingly provided for free, that the online provider collects the data of the user and processes this data for commercial purposes (e.g. placing of advertisements, profiling, tailor-made offers). The more the service provider can make use of the data of the users of the service, the higher the value of the data will be. Often consumers are completely unaware that their data is being used to pay for the service they receive. Leaving aside the informational gap, **a balance must be achieved between two opposing interests, consumer autonomy and consumer protection**. On the one hand, consumers should have the choice to reveal as much or as little information about themselves as they wish. This would mean allowing consumers to choose their level of data protection freely. On the other hand, when it is considered that revealing certain information, or allowing its commercialisation, is prejudicial to the consumer *per se*, or when it is feared that the liberty of consumers would be abused, political decisions need to be made to provide limitations.

---

[96] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union' COM (2010) 609, p. 2.

[97] Article 8, EU Charter of Fundamental Rights.

One clear example of limiting data autonomy relates to the personal information of minors. Another relates to limiting the commercialisation of data where the data subject can be identified. Finding the right balance between the interests of autonomy and protection will strengthen the rights of the consumer.

### 3.1.3. The balance between consumer protection and the internal market dimension

The level of protection set by data protection regulation has a direct effect upon the commercial value of information provided by consumers, whether with their knowledge or not. Data protection characteristically affects the commercial value of consumer's data by prohibiting the commercialisation of certain types of data or at least subjecting it to further conditions. The data given in the course of online services is the currency of consumers in exchange for the service they receive. As a result, setting a higher level of data protection will be likely to devalue the currency of data subjects for online services. A strict data protection regime may therefore not always be to the benefit for the data subjects. A very strict data protection regime might even exclude data subjects from access to certain services usually only provided in exchange for providing personal data. **A balance must also therefore be struck between the internal market dimension and consumer protection**.

## 3.2. Fundamental elements of the reform

The new core elements of the Proposal, mainly taking the form of consumer rights, can be seen in the light of an attempt to find an acceptable balance between giving maximum currency to consumers to 'pay' for 'free services', on the one hand, and the protection of their data on the other hand. The new core elements of the proposal are:

- consent (Articles 4(8), 7 and 9);
- the right to be forgotten and to erasure (Article 17);
- the right to data portability (Article 18);
- The rights against "profiling" (Article 20);
- The duty of controllers not established in the Union to designate representatives in the Union (Article 25);
- The possibility of joined operations of supervisory authorities (Article 56).

Due to the limited space which can be devoted to these core elements, in-depth analysis will be restricted to important aspects of the first four issues and a cursory overview will be made of the latter two.

### 3.2.1. Consent

The requirement of consent can be seen as a part of the right not to be subject to the processing of personal data. It is also a part of ensuring that consumers are made aware of how their personal information is being used by data controllers.

### Comparison with the current legislation

The main elements of consent in the existing data protection framework and the Proposal are contained in the legislative definition of consent at the beginning of both legal instruments and the articles providing for **consent as a legal basis for processing data**. Under the existing legislative framework, consent is defined as 'freely given specific and informed.'[98] The 1995 Directive adds a distinction in the standard of consent dependent upon whether the consent relates to the processing of 'normal' personal data or special categories of personal data. The general standard of consent is that it is given 'unambiguously.'[99] This is the substance of Article 7 entitled 'criteria for making data processing legitimate.' On the other hand, for sensitive personal data, consent must be explicit. According to the Article 29 Working Party, explicit consent 'encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question.'[100] The 1995 Directive includes an exception to the principle of consent for the processing of sensitive personal data where the data subject makes the data 'manifestly public.'[101]

The greatest change effected in the notion of consent by the Proposal is the **generalisation of 'explicit consent' for all processing of personal data**, a qualification which is currently only reserved for sensitive personal data. In order achieve this, the Proposal removed the concept of 'unambiguous' consent for the processing of general personal data and moved the qualification that consent be 'explicit' for the processing of sensitive personal data to the definition of consent at the beginning of the proposed regulation. In addition, the proposed definition also specifies that consent may be given 'either by a statement or by a clear affirmative action.'[102] Furthermore, Article 6(a) of the Proposal subjects consent to the added condition of being directed towards 'one or more specified purposes.' However, this condition, although announced as a principle of the lawful processing of data in Article 6, is not carried over to the consent for the processing of sensitive data. The exception to the principle of consent for the processing of sensitive personal data where it is made manifestly public remains solely applicable to sensitive personal data in the Proposal and does not therefore apply to the processing of personal data in general.

The Proposal also introduces an article setting out further specific conditions for consent. The key conditions relevant for strengthening consumer rights are:

- laying the burden of proof on the controller, Article 6(1);
- making consent to data processing distinct from consent to other matters, Article 6(2);
- and vitiating consent where the controller is in a more powerful position, Article 6(4).

These conditions are entirely new in relation to the existing directive.

Article 8 of the 1995 Directive prohibits the processing of 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.' However, such categories of data can be processed with the consent of the data subject, unless the data subject makes them manifestly public.[103]

---

98 Article 2(h), Directive 95/46/EC.
99 Article 7(a), Directive 95/46/EC.
100 Article 29 Data Protection Working Party, 'Opinion 15/2012 on the definition of consent', WP 187 (13.07.2011)
101 Article 8(2)(e), Directive 95/46/EC.
102 Article 4(8), the Proposal, COM(2012) 11.
103 Article 8(2), Directive 95/46/EC.

In essence, the Proposal adds 'genetic data' and 'criminal convictions' to the categories of sensitive data.[104]

In effect, as regards consent, the only difference between normal categories of personal data and special categories is that Members States have the discretion to decide that the latter categories cannot be processed irrespective of the consent of the data subject.[105] This fundamental state of affairs would not change under the proposed reform.

### Application

Several examples can be made of the application of the rules on consent and how they affect the interests of consumers. Of particular interest are the methods for obtaining consent, distinctions between the two different types of personal data and the exceptions to the need for consent. First, as for the means of obtaining consent online, the most typical method is to provide for a box which consumers can tick to indicate their consent. However, unless accompanied by the necessary information about the processing in a comprehensible manner, the consent will not be informed. For example, if excessive jargon or even legal vocabulary is used, or the information is ambiguous or even excessively long, with the result that the average consumer will not find it readily understandable, then the consumer's consent will not be informed. Furthermore, if the box to be ticked is already ticked and the consumer would need to opt out of the processing, then this will not satisfy the requirements because there will have been no affirmative action on the part of the consumer. Additionally, the explicit method of requesting consumers to consent through ticking a box will be required for all types of personal data.

Second, the Proposal includes the need to specify the purpose for processing as for personal data in general. Purposes for which data could be processed include processing as necessary for the service requested by the consumer, transfer of data to the developer of the service for improvement, added value services, behavioural advertising and transfer of data to third parties.[106] The need to specify the purpose for processing does not apply expressly to sensitive personal data, although it could be inferred from Article 5. The derogation from the need to give consent where data is manifestly made public applies to sensitive personal data, but not personal data in general. These modalities and limitations on consent have important effects upon the consumer. As an illustration of a worst case scenario in the interpretation of the Proposal, it could be supposed that a social network site requested consent which was then given for the processing of all types of personal data, specifying that this included political opinions. The social network site would then be able to provide advertising to the consumer based upon the consumer's political opinions which is sensitive personal data. However, the social network site would not be able to provide advertising to the consumer based upon the consumer's age, an example of normal personal data, because that specified purpose of the processing of the consumer's age had not received the consumer's consent. As another illustration, three different situations relating to a person's participation in a social network could be envisaged. It is clear that where a consumer limited their profile to persons who they had expressly selected, whether pro-actively or by acceptance, then any sensitive personal data revealed by the consumer is certainly not 'manifestly made public.' There could be argument as to whether sensitive data was 'manifestly made public' when, although limited in principle, the consumer systematically allows any request to see the consumer's profile and the number of persons capable of reading the profile extended into the thousands. However, it is likely that since 'the public' is an indeterminate body of persons, the fact that the extensively accessible

[104] Article 9(1) , the Proposal, COM(2012) 11.
[105] Article 8(2)(a), Directive 95/46/EC and Article 9(2)(a), the Proposal.
[106] Many of these examples of purposes for processing are taken from Article 29 Data Protection Working Party, 'Opinion 15/2012 on the definition of consent', WP 187 (13.07.2011), pp. 18-19.

profile is nonetheless limited would not be interpreted by the courts as manifestly public. The legal position is, however, much more ambiguous where the profile is not 'limited' and is accessible to anyone who is a member of the social network which is open to the public. In this third case, the sensitive personal data is in most likelihood 'manifestly made public.' This would mean for the consumer that the social network site and any person extracting data from it would be able to process it for such purposes as transfer to third parties and behavioural advertising.

### Evaluation

The general tenor of opinions expressed concerning the proposed changes to the regime for obtaining consent are **inherently polarised** into two groups with data protection groups, enforcers and **consumer** organisations, on the one hand, and other organisations representing **business** interests, on the other hand. The former group sees the Proposal as contributing to strengthening the rights of consumers and is positive as to its content. The latter group is more hostile to the enhanced standard of consent and even interprets the changes as likely to be detrimental to consumers' interests. Thus, the UK Information Commissioner's Office welcomed the 'high standard of consent' provided for in the Proposal[107] and the Article 29 Data Protection Working Party found that 'the proposal addresses the notion of 'consent' in a comprehensive and suitable manner in order to further specify and reinforce these conditions.'[108] As hinted at in the Proposal itself, the interaction between unambiguous and explicit in the 1995 Directive is not entirely clear[109] This has now been rectified bringing all consent up to the standard currently used for sensitive data. The European Data Protection Supervisor and the Article 29 Data Protection Working Party welcomed the resulting clarification of the notion of consent.[110]

On the other hand, the Association for Financial Markets in European and the British Bankers' Association believe that the 'proposed conditions for consent is disproportionately onerous and will result in lengthy notices which will generally remain unread or ignored by individuals' as well as 'consumer confusion.'[111] Likewise, the Internet Advertising Bureau UK, representing the interests of digital advertising business, claims that the rules on consent would be 'a significant burden on businesses and a cumbersome online experience for users.'[112] The proposal has not, however, been shielded from criticism emanating from data protection enforcers as the UK Information Commissioner's Office expressed reservations concerning the unqualified invalidity of consent in cases of significant imbalance.[113] On balance, however, the higher standard of consent for all types of data processing certainly represents a strengthening of consumer rights.

---

[107] UK Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' (2012), p. 6.

[108] European Data Protection Supervisor, Opinion on the data protection reform package (2012), p.21.

[109] the Proposal, COM(2012) 11, p. 8; also, 'First report on the implementation of the Data Protection Directive (95/46/EC)' COM(2003) 265 final, p. 17.

[110] European Data Protection Supervisor, Opinion on the data protection reform package (2012), p.19.

[111] British Bankers' Association and the Association for Financial Markets in Europe, 'EU General Data Protection Regulation' (2012), p.4.

[112] Internet Advertising Bureau UK, 'European Commission General Data Protection Regulation: IAB UK response to Ministry of Justice Call for Evidence' (2012), p.3.

[113] UK Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' (2012), p. 7.

Concern has been expressed in the business sector that requiring separate consent for data processing is misleading because it suggests that consumers can receive a service without subjecting their data to processing when, in fact, the choice for consumers is rather whether they want to receive the service with its associated data processing or not at all.[114] From the perspective of consumer protection and particularly in relation to the informational deficient, however, the separation of consent to the processing of data from consent to other matters should increase consumers' awareness that their data is often being used to pay for the services they receive. In this regard, the requirements of consent can be seen as strengthening the position of consumers. This could also eventually be seen as an effort to allow consumers to determine the level on which they share their data.

There is, however, one aspect in the standard of consent which appears anomalous. This is the relationship between the protection of personal data in general and the protection of sensitive personal data as regards consent. It has been noted that in two areas the regime for sensitive personal data appears to be less protective than that for personal data in general. This is incoherent. First, it was already noted in criticism of the 1995 Directive that the restriction of manifestly made public exception for sensitive information is 'inconsistent.'115 It is therefore recommended that, either the manifestly public exception to consent be transferred over to personal data in general, or removed from the Proposal altogether. In the interests of strengthening the rights of the consumer, however, it is recommended that if this qualification is to be added to the processing of personal data in general that the concept of 'manifestly made public' be further specified. For example, it could be specified that publishing information on an internet homepage open to the public at large would be manifestly public, but that providing information through a social media network is not manifestly public unless the profile is freely accessible to the public at large. The highest level of consumer protection would be to remove the manifestly public exception from the Proposal altogether. Second, there is the lack of the express requirement that consent be directed towards 'one or more specified purposes' in relation to sensitive personal data. Although the 'principle' is stated in Article 5(b), if this requirement is used in Article 6(a) on the lawfulness of processing personal data in general it should also be carried over to Article 9(2)(a) for the sake of clarity. In fulfilling the aims of the purpose-related principle, it is essential that the consent to the processing of sensitive personal data be directed towards a specified purpose.

[114] Society for Computers and Law, 'SCL Data Protection Seminar – 22nd February 2012', available at: www.scl.org
[115] For example, DLA Piper, 'The future of online privacy data protection' (2009), p.40.

### 3.2.2. The right to be forgotten and to erasure

#### Comparison with the current legislation

Under Article 12(b) of Directive 95/46/EC "the 1995 Directive", the deletion of data was provided for where it was unlawfully retained. This was the case where the data was inaccurate or incomplete. The right of erasure has apparently been 'transformed' into, or at least renamed as, a right to be forgotten. Thus, according to article 17 of the Draft Regulation, the data subject shall have the right to erase personal data without delay under a number of grounds, such as withdrawal of the consent by which the data controller holds the data. Furthermore, where a data controller has authorised a third party to publish data, the controller is liable as if it had published the data itself.

#### Application

The obvious example to which this article could be applied is that of social network services. Certain social network services currently divest data subjects of the right to delete information which they give to data controllers, such as photos, contact details or messages posted on forums. For example, an employee might in the 'heat of the moment' post an hyperbolical message on a social network service about his or her employer relating to an incident at work without realising that the employer may have access to it. A further variation could then include the 'tweeting' or forwarding with the employee's identity of the possibly exaggerated message to a much wider circulation than originally intended. Another distinct example would be the posting of compromising photos which could be accessed by a third party user entrusted with the task by an employer of 'checking' the suitability of applicants.

In the first example, of the message to be deleted, the right to erasure should operate to allow the data subject to have the compromising message deleted. However, it is not entirely clear from the wording of article 17 what the consequences of simply informing third parties that a data subject requests them to erase the personal data which they hold. Given that the data may have fallen into the hands of the third party without the authorisation of the data controller, it is unlikely that there will be any consent from which to withdraw. As a result, there may be no strict ground from which to require the erasure of the data. In the second distinct example, article 17 would have no scope for application, since the data controller, i.e. the social network service, is unlikely to have authorised the third party to process the data, i.e. harvest and pass on to the employer.

#### Evaluation

The **right to be forgotten and to erasure** do represent a strengthening of the rights of consumers. These rights give consumers control over their own personal data in the sense that a clear mechanism is provided for allowing consumers to withdraw their consent to the retention and use of their data. Both rights can therefore be seen as allowing consumers to set their own level of data protection. However, **the effect of the rights would still be mitigated in practice if consumers are not aware of exactly what information is being held by data controllers and how it is being used**. In addition, the substance of the right to erasure is in one respect unclear and should be amended. It appears that the purpose of requesting third parties to erase data is its removal. It would therefore be clearer to explain that a request for erasure from one data controller counts as an exercise of the right to erasure to which the addressee must comply. Even clearer would be to simply state that once informed by a data controller that a data subject has exercised the right of erasure, the data held by the third party data controller must also be deleted.

There are two further critical comments of a non-political nature which can be made relating solely to legislative technique. Thus, the additional qualification to the application of the right to be forgotten as 'especially in relation to personal data which are made available by the data subject while he or she was a child' is at best of no practical effect and at worst a dilution of the content of the right. This is because the right to erasure can only be absolute in the sense that it is either fully applicable or not applicable at all.[116] It is therefore useless to say that a right is more applicable in relation to children than others. If, as appears to be the case, the inclusion of the example of minors is to make a political statement about the protection of children, then this should be moved to a recital. The exceptions to the right to delete without delay in article 17(3) have a very similar content to the general restrictions of article 21, especially 17(3)(b). Consequentially, it is unclear how the exceptions in article 17(3) relate to the general exceptions in article 21.[117] Given the legal principle that provisions of a more detailed nature regulate an issue exhaustively to the exclusion of other more general rules (*lex specialis derogate legi generali*), it might be thought that the general exceptions of article 21 do not apply to the right of 17(b). Instead, the content of 17(3) should be moved to article 21.

### 3.2.3. The right to data portability

#### Comparison with the current legislation

Under article 12(b) of the 1995 Directive, the data subject had a general right of access and erasure. This included the right to obtain a copy of the data held by the data controller 'in an intelligible form.' Also, as indicated above, the right to erasure was only available where the data held was inaccurate. Article 18 of the Proposal provides for a so-called right of portability so that the data subject can have 'data [transferred] from one electronic processing system to and into another, without being prevented from doing so by the controller.'[118] Instead of referring to data 'in an intelligible form', as the 1995 Directive did, Article 18(1) of the Proposal refers to data 'in a structured and commonly used format.' Article 18(3) bestows the power on the Commission to specify particular formatting standards.

#### Application

Two brief types of example of the potential advantages of the right of portability can be given. First, without portability data subjects are often 'locked-in to services'. For example, a social media user may have a whole collection of sentimental photos stored. Even if the data subject is unhappy with the standards of data protection exercised by that social media provider, the data subject cannot move those photos to another more data protection friendly social media provider. The right of portability should help in this regard and also stimulate competition in the market, and even possibly a market-led race to provide better data protection. The second type of example empowers data subjects, especially consumers, to make use of information held about them.[119] For instance, in changing energy suppliers, the data subject would be able to offer valuable consumption data collected by the data controlling energy to a competitor. Indirectly, portability could even be used to allow data subjects who are consumers to acquire credit rating information held about them in order to made autonomous decisions about whether to make consumer credit agreements.

---

[116] See also, UK Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' (2012), p.14.

[117] European Data Protection Supervisor, Opinion on the data protection reform package (2012), [149].

[118] COM(2012) 11 final, p.9.

[119] see further, http://www.bis.gov.uk/news/topstories/2011/nov/midata

### Evaluation

**If properly implemented without dilution of substance, the right to portability should have a significant impact on strengthening the rights of the consumer**. Portability of data has the purpose of empowering consumers by increasing the effectiveness of their autonomy. Instead of a choice between leaving their data in the hands of service providers to continue to benefit from the service, consumers would be able to remove their data and still benefit from a similar service online but provided for by a different service provider. There are, however, two main points of criticism as regards Article 18. The first mainly relates to coordination of legislative technique and the relationship between the right of portability to the right to be forgotten and to erasure in article 17. The second is of a more political nature and concerns the means in achieving a right of portability through standard formats of data.

First, it is unclear whether the right of portability is meant to effect an all out transfer of the data to another consequentially deleting the information held by the original data controller, or whether the right to portability is based upon the principle of duplication. Under the principle of duplication, the information would be copied from the first data controller to another with both controllers keeping the information after exercise of the right to portability. It therefore needs to be clarified whether the right to portability moves the home of the data or whether the data merely finds a second home. Recommendations in this direction have been made, for instance, by European Data Protection Supervisor.[120]

Second, it is **unclear** from article 18 whether the Proposal intends to **compulsorily harmonise** the formats for holding data. Paragraph (1) provides that

> *'[t]he data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain... [the data]'*

Under a strict interpretation of the wording, such a harmonising effort is not intended. The **standard format** appears only optional, and the right of portability is made subject to the condition that the data controller actually holds the data in a commonly used format. As a result, unless the data controller purposefully decides to hold its data in a commonly used format, the data subject will not have a right of portability. On a more purposive interpretation, upon which for example the Association for Financial Markets in European and the British Bankers' Association seem to base their analysis, the right of portability would necessitate harmonising standards of holding data. This is because portability presupposes the transferability of data, an aim which can only be achieved through standard formats. Even if the right of portability were made absolute, and therefore not subject to the aforementioned condition,[121] it is clear that unless the formats for holding data are harmonised, the right will, in many cases, be ineffective. For instance, a data subject may very well exercise the right of portability, but the data then transferred by the data controller could be given in an almost indecipherable format which would, in practice, hinder any portability.

[120] European Data Protection Supervisor, 'Opinion on the data protection reform package' (2012), para. [152].
[121] i.e. 'shall have the right, where...'

In its submission to the call for evidence on EU data protection of the Ministry of Justice of the United Kingdom, the British Banking Association, in conjunction with the Association for Financial Markets in Europe, claimed that harmonising the formats for holding data in order to facilitate the portability of data would be 'disproportionate' given the costs involved and that in some cases it would be 'technically impossible'.[122] Consumer Focus, a UK statutory consumer organisation, welcomed the introduction of the right of portability, however, evidenced the problem of the providing a standard for the interoperability of services. It is, nonetheless, noteworthy that the process of harmonising formats for holding data has already begun. For example, the MiData scheme launched by the UK government in conjunction with industry allows consumers to request data held about them in an accessible format.[123] The UK Information Commissioner seems to support establishing formatting standards in spite of the possible costs involved in such harmonisation.[124]

To conclude, a key political decision needs to be taken on whether the harmonisation or adoption of 'commonly used formats' is compulsory. If the harmonisation is optional, then the effectiveness of the right of portability will be limited to the extent that data controllers decide to hold their data in a commonly used format. If the harmonisation of formats is compulsory, then the right of portability will be optimally functional, but costs associated with standardising formats will be incurred by the data controllers.

### 3.2.4. The right against "profiling"

#### Comparison with the previous legislation

Profiling is the process by which information collected about identifiable persons is analysed, often through the use of complicated algorithms, in order to discover patterns of behaviour and preferences.[125] As mentioned above, data subjects may not be aware that a profile is being compiled about them and the results of profiling are often valuably employed in personalised advertising. Under Article 15(1) of the 1995 Directive, Member States were to

> *'grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.'*

[122] British Bankers' Association and the Association for Financial Markets in Europe, 'EU General Data Protection Regulation' (2012), p.6.

[123] http://webarchive.nationalarchives.gov.uk/+/http://www.bis.gov.uk/policies/consumer-issues/personal-data

[124] UK Information Commissioner, 'Initial Analysis of Revised EU Data Protection Legislative Proposals' (2012), p.14.

[125] Definition in 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 (2010): Profiling means 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.

In 2010, the Council of Europe recommended that a set of principles be put in place concerning profiling in order to protect fundamental rights.[126] Article 20 of the Proposal increases the level of protection from the 1995 Directive in particular extending the scope of protection by removing the limitations imposed by the words 'automatic' and 'decisions'. Thus, all measures which produce legal effects on a natural person fall under the scope of the article and not just decisions. As a result, it applies also to the processing of data with the aim of predicting the behaviour of consumers. Article 20(2)(a) removes the right of consumers to submit their point of view as is currently the case under Article 15 of the 1995 Directive.

### Application

A number of short examples may be given to the issues raised by the right against profiling:

- establishing through the processing of personal data that a particular person is more likely to buy a product at a higher price and then offering the product to them at a higher price will not be possible. Likewise, having established that a person is less likely to desire a product will not justify offering it to that person at a reduced price. Such practices which manipulate supply and demand is such a way constitute price discrimination;
- using profiling to predict performance at work is not possible;
- as for predicting what a consumer is likely to want to buy having established a profile based upon their personal data and then targeting advertising of their predicted preferences, i.e. behavioural advertising, it is unclear whether this falls within the scope of Article 20 of the Proposal.

### Evaluation

As has already been mentioned above, article 20 of the Proposal should provide a more comprehensive and stricter treatment of profiling. The Article 29 Working Party has, however, expressed concerns that the provisions on profiling do not go far enough.[127] In particular, one issue for clarification is whether behavioural advertising is an example of profiling which either has 'legal effects', such as for example infringing the fundamental right to privacy, or 'significantly affects' natural persons in other ways.

The Recommendation of the Council of Europe on profiling, of which the Proposal 'takes account',[128] explicitly refers to the fact that profiling 'is capable of having an impact on the people concerned by placing them in predetermined categories, very often without their knowledge.'[129] Nevertheless, despite the fact that recital 21 of the Preamble to the Proposal explicitly refers to 'analysing or predicting ... personal preferences, behaviours and attitudes', in the opinion of the UK Information Commissioner's Office, behavioural advertising does not fall within the scope of the right not to be subject to profiling because it does not produce legal effects or significantly affect consumers.[130] It is interesting to note

[126] 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.
[127] Article 29 Data Protection Working Party 'Opinion 01.2012 on the data protection reform proposals' (23.03.2012) WP 191, p.14.
[128] the Proposal, COM(2012) 11, p. 9.
[129] Recommandation 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 (2010).
[130] UK Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' (2012), p.15.

that the UK representative had 'reserved the right of her Government to comply with' the Recommendation of the Council of Europe.

The UK Information Commissioner's Office does, however, concede that the exclusion of behavioural advertising is not clear. The Article 29 Working Party believes that 'web analysing tools, tracking for assessing user behaviour, the creation of motion profiles by mobile applications, or the creation of personal profiles by social networks' should be included.[131] In light of that belief, the Article 29 Working Part submits that 'significantly affects' is imprecise.[132]

As noted by the UK Ministry of Justice's Summary of Responses to its call for evidence, opinions concerning the inclusion of behavioural advertising are divided between the 'advertising sector' and 'members of the public and rights groups.'[133]

First of all, it is curious to note that whilst when consumer's personal data is used in exchange for online services these services are nonetheless marketed as 'free' and yet when business is made to ask for the consumer's consent to commercialise personal data this is characterised as a cost to business. In any event, **from the perspective of strengthening the rights of consumers, it is clear that behavioural advertising should be included within the scope of the right against profiling**. This does not outlaw behavioural advertising, thus recognising its potential benefits, but simply subjects it to the prior consent of consumers. As a result, restricting behavioural advertising to the condition of prior consent strikes an appropriate balance between the internal market dimension and consumer protection as well as contributing to the awareness about practices which are 'largely invisible and unknown to consumers.'[134]

### 3.2.5. The duty of controllers not established in the Union to designate representatives in the Union

The designation of representatives in the EU is certainly a step forward for the practicalities of enforcing EU data protection regulations. However, it would be important that this requirement is not satisfied by simply having a '**post-box**' in the EU. In substance, the article must result in jurisdiction over issues concerning European data controllers being attributed to courts of the EU Member States. Jurisdiction should not be circumnavigated through the main activity of the data controller being situated outside of the EU.

### 3.2.6. The possibility of joined operations of supervisory authorities

This article is **potentially very beneficial**, although it could prove **complicated in practice**. Article 56 introduces the possibility of joined operations of supervisory authorities in the EU. This would allow for a more vigorous treatment of protection issues by pro-active supervisory authorities of Member States, where otherwise the competence would have been solely attributed to less pro-active supervisory authorities of other Member States.

---

[131] Article 29 Data Protection Working Party 'Opinion 01.2012 on the data protection reform proposals' (23.03.2012) WP 191, p.14.

[132] Article 29 Data Protection Working Party 'Opinion 01.2012 on the data protection reform proposals' (23.03.2012) WP 191, p.14.

[133] Ministry of Justice, 'Summary of Responses to Call for Evidence on Proposed EU Data Protection Legislative Framework' (June 2012), p.20.

[134] 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 (2010).

## 3.3. Recommendations

### 3.3.1. How the balance has been struck between consumer rights and other interests

It seems that the balance in the Proposal has been struck through the **promotion of transparency**. Consumers are not wholly prevented from revealing data, as could be the case under a very strict data protection regime, however, the consumer must be aware of what data is transferred and how it is used. This is particularly demonstrated in the provisions relating to consent. A tentative framework for allowing consumers to vote with their feet and switch the service provider which holds their data seems also to be found within the right of portability. As a consequence, this ultimately leaves the choice of what level of protection consumers choose based on their convictions concerning the level of transparency they want to give to their data (there are consumers who do not what to reveal their data and those who prefer total transparency) and what they may get in exchange for their data. **However, in many respects the Proposal leaves certain issues equivocal**. This is particularly the case with behavioural advertising, the practicalities of implementation and the right of portability. This makes it difficult to evaluate where the balance has been struck as it is not clear what is intended by the Proposal. This ambiguity must be resolved and the recommendations are therefore mainly directed towards calls for further clarity in the Proposal.

### 3.3.2. Remedies for the non-performance of “free” online services

There is a large gap in the legal framework which is not included in the data protection package and which could be filled by drawing the legal consequences from the fact that “free” online services are, in fact, paid for with the data of consumers. As a preliminary issue of general contract law, it is pertinent to ask whether consumers should not be able to exercise the normal remedies for non-performance. At this late stage in the legislative process, the most practical recommendation which can be made would be to make an **explicit reference to the possibility of general consumer remedies** in the national laws of the Member States.

As has already been mentioned, online services which are provided not in exchange for a price are usually not really “free” services. User data is given in exchange for making use of the service. Since making use of such a service is reciprocal, the issue arises whether the data subject should have remedies for non-performance in case the service is not being properly provided by the service provider. Moreover, often the service provider invites the data subjects to install certain software on their computer – or automatically installs software (such as cookies). In the event that the service is not properly provided, the user may wish to uninstall such software or to remove cookies and other software from his or her computer. Finally, software being installed in the course of the provision of such a service may damage the user’s computer. In all these cases, the user might ask whether he or she has remedies against the software provider. Such remedies could be, e.g. to terminate the contract and its unravelling (in particular the returning/erasure of all data provided), to require that any software be uninstalled from the user’s computer or to claim damages for loss caused by the non-performance, in particular to the users’ soft- or hardware. This would represent an important step in strengthening the rights of consumers in response to the recent developments of internet services.

It could be seen as one aim of data protection regulation to improve the position of data subjects as well as with regard to such contractual claims arising from the provision of defective services. Several models have already been proposed, the most important being some provisions in the European Commission's proposal for a Common European Sales Law.[135] It might be too complicated in the current stage of the legislative procedure of the data protection package to insert a fully fleshed out set of provisions on remedies of data subjects in such cases. It could, however, be useful to at least mention the problem within the data protection regulation, for example, in a recital. Such a recital could be useful for enforcing data subjects, in particular consumers' rights because of defective services under the applicable (EU or Member State) law. Such a recital could read:

> "This regulation does not deal with remedies a data user may have, because services promised or supplied in exchange for giving consent to the processing of personal data are not being provided in conformity with the contract or otherwise cause harm to the data subject, in particular their soft- or hardware. Remedies in such cases may, however, be available under the applicable laws of the Member States [or under the Common European Sales Law]." [136]

### 3.3.3. Specific recommendations

There are a number of recommendations which can be made, mainly of a technical nature, but also relating to policy decisions:

1. A key political decision needs to be taken in article 18 on whether the harmonisation or adoption of 'commonly used formats' is compulsory.
2. For the purposes of strengthening the rights of consumers, behavioural advertising should be included in the legal characterisation of profiling.
3. Either the manifestly public exception to consent be transferred over to personal data in general, or removed from the Proposal altogether. The latter option would strengthen the rights of the consumer. In any event, should the concept of 'manifestly made public' be maintained in the reformed data protection package then this concept needs to be further clarified.
4. Express mention in the preamble that the regulation does not deal with or prejudice remedies of non-performance which would be otherwise open to the consumer.
5. Clarify whether the right to portability in article 18 moves the home of the data or whether the data merely finds a second home.
6. Removal of the explicit reference to children from article 17 and (possibly) restatement in a recital of the preamble.
7. The requirement that consent to the processing of sensitive personal data be directed towards specified purposes should be carried over from Article 6(a) on the lawfulness of processing personal data in general to Article 9(2)(a).
8. Clarify in article 17 that once informed by a data controller that a data subject has exercised the right of erasure, the data held by the third party data controller must also be deleted.

[135] Commission Proposal COM(2011) 635 final, cf. Article 107 and others.
[136] When enacted.

# 4. INTERNATIONAL DATA TRANSFERS – BENEFITS AND THREATS AS WELL AS IMPACT ON EUROPEAN CONSUMERS AND BUSINESSES

One of the main field of application of international data transfers is cloud computing. The big providers of cloud computing such as Google, Amazon, Microsoft and Apple are based in the United States. Their servers are located and distributed across the entire world and data is routed where it is cheapest and easiest to process. The current European (EU and Member State data protection legislation) is therefore difficult to apply. Moreover, data subjects who make use of other services of the same provider may not be aware of the practice that all data related to a data subject is being collected in the different services and then joined to become part of a comprehensive user profile of the data subject. Such user profiles based also on data stored by the data subject in a cloud service make the data subject's user profile much more valuable, in particular for personalised advertising. Another problem is the storage of data of users who terminated the use of a cloud service. Up until now, it has been rather unclear whether such data will be deleted or continued to be stored and used for the purposes of the service provider. From an internal market perspective the limited effect of European data protection legislation on cloud service providers based in third countries may disadvantage providers which are based within the EU. The applicability of the General Regulation to all providers active within the EU would also create an EU-wide level playing-field for cloud computing and could therefore improve the position of cloud computing service providers based within the EU. Moreover, the protection of data subjects and consumer protection could be improved, because European authorities will be put in a better position to enforce EU data protection legislation against providers of cloud services based in third countries.

International data flows are one of the main aspects that require review and improvement when reforming the EU data protection regime, especially in the context of such phenomena like cloud computing. Cloud computing solutions create special problems for the current regulation of cross-border data transfers, which is basically based on protecting data in a given physical infrastructure in a defined location. This is one of the reasons why it is necessary to implement new and streamlined legal instruments in the field. As a general rule: using cloud computing services, on the one hand, should not relieve data controllers (UE-based) of their responsibilities with respect to data processing and – on the other hand – the cloud providers (especially those from "third countries") should be encouraged to protect the data at the highest level, "adequate" to the EU-level. The purpose of this chapter is to explore the proposed regulation of trans-border data flows and to present recommendations on how can it be further improved.

## 4.1. Increased role of the Commission: "adequacy assessment"

Currently, under Directive 95/46/EC, the Commission **decisions on the adequacy** of data protection legal systems of non-EU countries, together with Model Contractual Clauses, Binding Corporate Rules and some other mechanisms and instruments, facilitate data transfers outside the European Economic Area (Articles 25-26 of the Directive). There are, however, inconsistencies and growing problems in this regard. As regards the concept of adequacy of non-EU legal regimes, it is currently concentrated on the assessment of national legal systems ("the third country in question" – see the wording of Article 25(1) of the Directive), however, performed "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations" (Article 25(2) of the Directive).

Such an assessment approach requires modification and should be conducted also in relation to the specific recipients of personal data, not only to the whole "non-adequate" country the data recipients are located in. As one scholar has put it:

> *"It is not clear why at the present time the European Commission has been concentrating on adequacy decisions covering an entire country, which are necessarily more complex and difficult to reach than more limited decisions. In many countries there are specific laws covering data processing in different sectors, and the level of protection may differ substantially among different sectors. (…) Thus, greater use could be made of adequacy decisions covering a specific industry, a specific type of data processing, or a specific law or regulation. Examples of such decisions already exist, such as those concerning the US safe harbor system (which covers those companies that have voluntarily joined safe harbor) or the Canadian PIPED Act (which only covers data processing that falls under that Act). Such limited adequacy decisions would be quicker and easier to reach than those covering entire countries, and could be fine-tuned to cover types of data transfers and data processing where there is the greatest need for adequacy decisions".*[137]

The Proposal introduces – in Article 41(1) – the **possibility of recognising particular "territory", "processing sectors"** within a third country or an international organisation as ensuring an "adequate" level of protection. This direction is certainly correct, allowing assignment of higher importance to adequacy decisions, both in legal and practical terms. This line of development should be continued, and in particular, the introduction of a clarification in the preamble to the Regulation should be considered, stating that the term "processing sectors" may denote not only a certain sector of the economy (such as banking or telecommunications), but also a specific circle of entities subject to specific legal regulation of a third country, bound by a specific code of conduct, etc. It is also proposed in the Package to remove the discrepancy occurring under the Directive: **assessment criteria** no longer include the circumstances of a specific transfer (as under Article 25(2) of the Directive), but focus on the "rule of law, relevant legislation in force" and other similar circumstances of a general nature (Article 41(2) of the Proposal).

Another significant change proposed in the Package, in the field of cross-border data flows, concerns the **attempts to "centralise" the process of adequacy assessment**, by giving the Commission increased and exclusive powers to determine that the third country, territory, processing sector or international organisation ensures an adequate level of protection. Such a shift would ensure a more uniform and coherent approach within the EU. At the moment – under Article 25 of Directive 95/46/EC, which does not provide an explicit answer in that regard[138] – the issue is far from being explicit and the required level of legal certainty: some of the Member States allow data controllers themselves to conduct the adequacy assessment (e.g. the UK, Poland), other reserve it for national authorities (e.g. France), and finally, there are countries which leave the issue solely at the discretion of the Commission.[139] As a result, this entails significant risks, including those associated, for example, with the fact that a given third country may be considered by some Member States to meet the required level of protection, while in other Member States it will continue to be forbidden to transfer data to that third country.

---

[137] Ch. Kuner, 'Developing an Adequate Legal Framework for International Data Transfers', in: S. Gutwirth et al. (eds.), 'Reinventing Data Protection?',2009, pp. 263-273.

[138] Only Article 25(3) states that *"[t]he Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection"*, which suggests that assessment in this regard may be made by both Member States as well as the Commission.

[139] See the analysis carried out in this area by R. Marchini, S. Delon-Bouquet, O. Fasshauer, J.-Y. Steyt, B. Verdegem, 'Legitimising Cross-Border Data Flows by the "Self-Assessment" Method: Different Approaches Throughout Europe', World Data Protection Report, January 2007, pp.23-28.

The solution proposed in the Proposal is also justified for practical reasons: at present, few national authorities have the necessary personnel and financial resources, as well as the necessary facilities, to allow conducting the adequacy assessment process, which is complicated, cost- and time-consuming. For these reasons, *"authorities rather deal with specific transfers that do not however imply a general decision on adequacy of a third country"*.[140]

Additionally, this situation becomes more complicated in the context of "adequacy self-assessments" carried out by data controllers. Currently – even in the Member States where this is possible – data controllers are in practice not found to exercise that right often enough, therefore, it is assumed that only the export of data to third countries recognised by the Commission as providing an adequate level of protection does not require the additional responsibilities to be satisfied.

As regards adequacy assessment and decisions, in addition to the letter of the law, the actual practice will also be very important. The current practice is considered – based on the experience to date – insufficient. As noted in the legal literature, *"[i]f one assumes that future adequacy decisions will be approved at the same rate as they have been since the Directive came into force (namely at a rate of six countries approximately every ten years), then it would take approximately one hundred and thirty years for these 78 countries to be found adequate. While 130 years may be a reasonable timescale for building the Pyramid of Cheops or the Great Wall of China, it is clearly absurd with regard to passing adequacy decisions, and shows the flaws in the present system"*.[141] One should, therefore, expect **more frequent use of that tool in practice**, which will require, in particular, ensuring increased financial and organisational support by the Commission and the authorities involved. Additionally, given the current complex, lengthy and politically sensitive procedures involved in assessing adequacy, the **"logistics" of how adequacy decisions are to be issued and used** under the General Regulation needs to be addressed. In that respect, the following must be defined:

- rules of conducting the assessment, including its initiation (as at the moment it raises significant doubts), the involvement of the national supervisory authorities as well as the European Data Protection Board;
- rules of further "handling" of adequacy decisions, in particular in the context of the requirement to carry out periodic assessments that take account of changes, if any.

[140] 'Analysis and impact study on the implementation of Directive 95/46 in Member States' (Annex to the First Commission's report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final), p. 32.

[141] Ch. Kuner, 'Developing an Adequate Legal Framework for International Data Transfers', in: S. Gutwirth et al. (eds.), 'Reinventing Data Protection?',2009, pp. 263-273.

At this stage, it does not seem justifiable to completely forgo this legal institution, in spite of its obvious shortcomings and the still limited practical use. It may, in fact, continue to serve as an important instrument for increasing the level of protection of the rights of individuals both in the EU and worldwide, becoming – as one scholar put it – the *"engine of an emerging global data protection regime"*.[142] Furthermore, the adequacy assessment procedure still demonstrates certain flexibility, and even some openness to alternative solutions and legal philosophies, offering an interesting perspective in the context of transnational data transfers in the future. As noted in a report prepared at the request of the Commission:

> *"the recent Working Party 29 positive opinion regarding New Zealand may open new perspectives for the adequacy process in its political dimension. The recognition by the Working Party 29 of the compatibility, not to say adequacy, of the harm-based approach developed in New Zealand privacy laws surely sends a signal to APEC and member governments that the EU adequacy apparatus, despite being cumbersome and slow, is still operating and open to admit differing approaches"*.[143]

In this regard, however, attention should be paid to the wording of Article 40 of the Proposal and the possible resulting complications. Article 40 introduces an explicit requirement to take account of the specific rules of **onward transfer**, which may be a difficult condition to meet by certain third countries and regarding their adequacy decisions, where there is no specific provision on the protections and safeguards when personal data are transferred from those third countries to other third countries. It is, therefore, necessary to clarify how the following reservation under Article 40 should be understood: *"including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization"*, so that the required flexibility and openness of the procedure in question are not reduced.

In spite of the limited practical usefulness (for many reasons, including political),[144] the Proposal preserved the possibility of decisions by the Commission that a third country (and – in addition – a territory, a processing sector or an international organization) does not ensure an adequate level of protection (Article 41(5) of the Proposal; the so-called **negative adequacy decisions** or "black list"). There is fundamental doubt in this regard as to the consequences of such decisions. Recital 82 of the preamble to the Proposal suggests that the transfer of personal data to such third countries should be totally prohibited. On the other hand, the provisions of Article 41(6) do not seem to completely prohibit such transfers (*"transfer of personal data (…) shall be prohibited, without prejudice to Articles 42 to 44"*). The additional question is whether the prohibition on transfer in this situation will apply to the entire country (the second sentence of Recital 82 of the preamble to the Proposal mentions only a third country) or apply to a territory, a processing sector or an international organization where the Commission's decision applies to an area smaller than the entire country. Because of their importance, these issues require clear and explicit determination.

---

[142] M.D. Birhnack, 'The EU Data Protection Directive: An Engine of a Global Regime', Computer Law & Security Report 24 (2008) 6.

[143] CRIDS, 'Assessment of the application of Article 25 of Directive 95/46', 27.07.2011, p. 20; see also Article 29 Data Protection Working Party, 'Opinion 11/2011 on the level of protection of personal data in New Zealand', WP182 (4.04.2011), p. 9.

[144] Ch. Kuner, 'European Data Protection Law. Corporate Compliance and Regulation', Oxford University Press, 2007, p. 175.

## 4.2. Decreased role of the national Data Protection Authorities: no "further authorisations"

The Data Protection Package explicitly states that if specific data transfers have been approved by the Commission's decision or are based on Model Contractual Clauses ("standard data protection clauses", in accordance with the Proposal's terminology) or Binding Corporate Rules, then such transfers **do not require any further authorisation** (Article 41(1), second sentence, as well as Article 42(3) of the Proposal). Such pre-approvals by a number of national DPAs, even when parties of the Model Contractual Clauses do not deviate from the standard template, are currently the source of administrative burdens with only little value.

The above proposal should be welcomed as it is supported by sound legal arguments (to put it simply: what has already been accepted by the EU law should not require additional approval at the national level) as well as practical arguments, and may, for obvious reasons, contribute to facilitating transfers of personal data outside the European Economic Area. The current legal status is, in fact, far from satisfactory in this respect: some Member States already fully recognise adequacy decisions and Model Contractual Clauses; others recognise only the former of those instruments and require pre-authorisation in the latter case; and finally there are countries which apply the requirement of additional national approval with respect to all instruments approved at EU level.

The principle described in Article 42(3) of the Proposal concerns only the instruments referred to in Article 42(2) points (a) to (c); it does not, however, apply to "contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority" (Article 42(2)(d), the so-called **'ad hoc clauses'**). Thus, the application of such contractual clauses requires from the controller or processor to obtain prior authorisation from the supervisory authority (Article 42(4) of the Proposal). This solution does not seem appropriate as it may weaken the effect of proposals adopted in the Proposal. Quite frequently, entities involved in data transfer use individual non-standard provisions as those standard ones contain imperfections and limitations. In connection with the progressing economic and technological development, this trend is expected to increase, not decrease. In many cases, those agreements are so extensive and regulate such complex outsourcing operations and transactions, that their analysis and approval can take a long time, which may adversely affect the success of business projects, thus increasing the administrative burden and – ultimately – adversely affecting the development of international cooperation and economic development of the EU. Not without significance is also the empirical argument: data protection authorities (or at least not all of them) do not have adequate resources, knowledge and experience to engage in the assessment of complex business solutions and agreements.

The solution proposed in Article 42(3) of the Proposal should be applicable to both cases: where the data exporter is the data controller and where such exporter is the **data processor** (this follows from Article 42(1), which treats the two categories of entities equally). To date, there were significant doubts as regards data transfers by data processors, doubts which were resolved by different national authorities in various ways. In those situations, some of them required:

- first, to sign an appropriate transfer agreement (which, however, due to the limitations of the model contract solutions used to date, was signed not as a *processor-to-sub-processor* agreement, but as *controller-to-processor* agreement);
- second, to obtain authorisation from the respective DPA for such data transfer.

As the Danish DPA stated in the letter on the case regarding the Odense Municipality's use of Google Apps:

> *"If data centres in Europe – but outside of the EU/EEA - are to be used, Odense Municipality and the individual data centres may enter into an agreement based on the EU Commission's standard contractual clauses, or Odense Municipality may grant Google Ireland Limited a clear mandate to enter into agreements, in Odense Municipality's name and on behalf of Odense Municipality, based on the EU Commission's standard contractual clauses with the individual data centres. In addition, it would be necessary to apply for authorisation from the Danish Data Protection Agency pursuant to Section 27(4) of the [Danish] Act on Processing of Personal Data."*[145]

By explicitly excluding the permissibility of using further authorisations by the Member States, the Proposal **does not provide for the obligation of notification** either, both with respect to national authorities and the Commission. Such a solution is believed to be desirable. In the reality of mass and ubiquitous cross-border exchange of data, such an obligation would constitute an unnecessary administrative burden, without bringing the required benefits in return. It is already quite evident that obligations of this kind do not work properly in practice. For example, the obligation to inform the Commission and the other Member States of the authorisations granted pursuant to Article 26(2) of the Directive (as prescribed by Article 26(3)) was satisfied only sporadically. This was mentioned in the 2003 Commission report on the implementation of Directive 95/46/EC, by pointing out that *"this suggests that many unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection. Yet there is little or no sign of enforcement actions by the supervisory authorities"*.[146]

## 4.3. Data transfers by way of "standard data protection clauses"

The Proposal explicitly provides for **different types of contractual solutions** to facilitate personal data transfers, thus confirming the practice which is already in force. Article 42(2)(b)-(d) lists the following as instruments that may constitute the appropriate safeguards:

- standard data protection clauses adopted by the Commission;
- standard data protection clauses adopted by a supervisory authority;
- contractual clauses between the controller or processor and the recipient of the data (the so-called 'ad hoc clauses').

Approval of specific contractual clauses by the DPA from one Member State – in accordance with the consistency mechanism – will mean that it will no longer be necessary to take any measures by other Member States, in particular no additional assessment or approval of such clauses or granting consent for data transfer operations performed under such clauses will be required.

---

[145] Processing of sensitive personal data in a cloud solution', J.no.2010-52-0138 (3.02.2011), available at http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution

[146] 'Report from the Commission: First report on the implementation of the Data Protection Directive (95/46/EC)', COM(2003) 265 final, p. 19. In the 'Analysis and impact study on the implementation of Directive 95/46 in Member States' being an annex to the Report, the Commission has summarised this by stating that "[t]he extremely law number of notifications indicates either that Member States have failed to notify authorisations to the European Commission or that Member States are not granting authorisations as provided for in Article 26(2) of the Directive and national laws transposing it" (pp. 34-35).

The Proposal should also take into account such commonplace operations as "onward transfers", "sub-processing" (and even "sub-sub-processing") and the fact that there are numerous data exporters and importers on both sides. For these reasons, the instrument of standard data protection clauses should be improved, by introducing **processor-to-sub-processors model clauses** or clauses that could be used by a service provider in relation to many of its clients using similar services, e.g. cloud services. Article 29 Working Party, in its opinion, has already urged the Commission *"to develop promptly a new separate and specific legal instrument that allows international sub processing by processors established in the Union to sub processors in a third country. Such an instrument could for instance take the form of a new set of Standard Contractual Clauses, through which the controller and the processor established in the EU/EEA could provide for trans border sub processing, in accordance with the necessary and adequate guarantees for such transfers"*.[147] At the moment, the situation in this respect – even after a new set of model clauses for controller-to-processor transfers were adopted in 2010[148] – is far from simple and flexible: transmission of data from a processor in the EU to a sub-processor in a third country may occur:

- in cases where an agreement – based on the EU Commission's standard *controller-to-processor* contractual clauses – is entered into directly between the EEA-based controller and the sub-processor in the third country, or
- in cases where the processor in the EU is granted from the EEA-based controller a clear mandate to enter into an agreement (based on the EU Commission's standard *controller-to-processor* contractual clauses), in the controller's name and on its behalf, with sub-processor in third country, or
- by the use of ad-hoc agreements.[149]

As a result, it has been noted in the legal literature that:

> *"As the model clauses do not enable EEA cloud providers to transfer data to non-EEA sub-providers, this may incentivise EU customers to use non-EEA cloud providers, in order to achieve greater flexibility in terms of transfers to sub-processors. This seems to be a major limitation of the new model clauses and is a significant practical disadvantage as many EEA providers rely on the infrastructure or platforms of non-EEA IaaS and PaaS providers such as Amazon Web Services, Google App Engine or Microsoft Windows Azure"*.[150]

The Proposal creates a legal basis for adopting such missing legal instruments by providing for the possibility of using standard data protection clauses also by data processors (Article 42(1) read in conjunction with Recital 84). It would be desirable, however, to explicitly emphasise that possibility in Article 42(2)(b) and (c), as is done in Article 42(1)(d) of the Proposal.

---

147 'Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor)', WP 161 (5.03.2009), p. 3.

148 Commission Decision no. 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

149 'FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC', WP 176, (12.07.2010), pp. 4-5.

150 W.K. Hon, Ch. Millard, 'Data Export in Cloud Computing –How can Personal Data be Transferred outside the EEA? The Cloud of Unknowing, Part 4', Queen Mary University of London, School of Law, Legal Studies Research Paper No. 77/2011, p. 23.

Article 42(5) of the Proposal provides for the possibility of basing data transfers on **non-binding instruments** (*"appropriate safeguards (…) not provided for in a legally binding instrument"*). That possibility gives rise to some objection because, as rightly pointed out by Article 29 Working Party, *"bindingness has always been considered as an important requirement in existing tools framing international transfers (for example CCT, BCR, SH, adequacy of third countries)"*[151] The solution proposed by the Commission does, in fact, provide for the necessity to obtain authorisation for such transfers, but even such an authorisation will not remedy the lack of an appropriate binding instrument between the data exporter and the data importer. And such an instrument is of key importance in the context of responsibility of the data recipient from a third country, enforcement of that responsibility, and the measures available – in relation to such data recipient – to data subjects. Perhaps that gap could be filled by "provisions to be inserted into administrative arrangements", it seems, however, that they include "arrangements" to be entered into between the data exporter and the data protection authority (which is suggested by the use of the term "administrative"), rather than "arrangements" between the data exporter and the data importer. Therefore, given the risk of weakening the level of data protection, objections as to leaving decision-making within the competencies of national regulatory authorities (which may, in itself, result in a non-uniform approach in different countries), and serious doubts of interpretation, it is recommended to delete Article 42(5), except for the last sentence. Therefore, the reference in Article 34 of the Proposal will require to be changed accordingly.

## 4.4. Data transfers by way of Binding Corporate Rules (Article 43)

The Binding Corporate Rules ("BCRs") have been **explicitly recognised** in the Proposal, which could help to remove any remaining legal barriers in this regard. Currently, not all Member States and DPAs recognise the decisions taken by other DPAs and impose additional national requirements, like the requirement of obtaining additional authorisation for the use of BCRs, even though they have been approved by DPAs of other Member States. The so-called "mutual recognition procedure" – whereby BCRs are reviewed and approved only by the "lead DPA", assisted by two other concerned DPAs – has been accepted only by 16 Member States and additional 3 EEA countries.[152] In accordance with the Proposal, a data transfer based on Binding Corporate Rules does not require any further authorisation (Article 42(3)).

The main substantive as well as procedural elements and requirements for Binding Corporate Rules have also been defined, based generally on Article 29 Working Party's opinions on this subject. That instrument – in accordance with the proposed Article 43(1)(a) – could be applicable to both data controllers and data processors who, for example, are engaged in outsourcing activities (the so-called **'Binding Safe Processor Rules'** or 'Processor Binding Corporate Rules'). Article 29 Working Party has already taken appropriate measures in that respect by presenting a toolbox that describes the conditions to be met to facilitate the use of Binding Corporate Rules for Processors ("BCR for third party data").[153]

[151] Article 29 Data Protection Working Party, 'Opinion 01/2012 on the data protection reform proposal', WP 191 (23.03.2012), p. 22.
[152] Commission Staff Working Paper, 'Impact Assessment', SEC(2012) 72 final, p. 17.
[153] Article 29 Data Protection Working Party, 'Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules', WP 195 (6.06.2012).

Unfortunately, the Proposal does not provide for any facilitation as regards adoption and approval of Binding Corporate Rules by smaller entities, especially by SMEs. Therefore, in practice that mechanism should be expected to be limited to the largest international corporations with the necessary legal, financial and organisational resources. Neither does the Proposal clarify whether it would be possible to limit the instrument in question to a certain part of a group of undertakings, which could contribute to its increased flexibility. In practice, it is not always necessary to cover an entire group by Binding Corporate Rules, and such a conclusion follows from Article 43(1)(a) of the Proposal, according to which BCRs are *"legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings"*.

## 4.5. Other issues: definition of "data transfer"; derogations

The Proposal introduces additional solutions, desirable by both theorists and practitioners, for example, it elaborates that the rules on data transfers are applicable not only in relation to data controllers, but **also to data processors**. That issue, in the current legal environment, gives rise to doubts – therefore, its explicit resolution in the Proposal should be considered as a positive development. Regrettably, the Data Protection Package does not provide clear answers to other questions, even basic questions. The most important seems to be how **the term "data transfer"** should be understood and defined, because as the European Data Protection Supervisor stated in his opinion that:

> *"this has proved to be a problematic issue which has been specifically left by the Court of Justice to the legislator to resolve. (…) Defining what a transfer is and what it is not should be clearly addressed in the Proposal, especially with regard to the network environment, where the difference between actively transferring and making data available is becoming theoretic while the consequences in terms of applicable law are huge for data controllers and individuals".*[154]

As regards the so-called **"derogations"** (Article 44 of the Proposal), the introduction of an additional condition permitting data transfers – in the form of legitimate interests pursued by the controller or the processor (Article 44(1)(h)) – should be considered a positive development. At the same time, however, the possibility of applying that condition has been entrenched by far-reaching restrictions and burdens, including:

- no possibility of applying that exception to "frequent or massive" transfers;
- necessity to carry out assessment of "all the circumstances surrounding the data transfer operation or the set of data transfer";
- necessity to adopt "appropriate safeguards with respect to the protection of personal data, where necessary";
- requirement to precisely document the assessments and the adopted appropriate safeguards (Article 44(6));
- disclosure obligation towards the relevant supervisory authority (Article 44(6)).

[154] European Data Protection Supervisor, 'Opinion on the data protection reform package' (2012), [108].

The first of the above restrictions (transfer "which cannot be qualified as frequent or massive") has been derived from the work of Article 29 Working Party regarding data transfer rules.[155] However, neither Article 29 Working Party not the writers of the Proposal elaborate sufficiently enough on those terms, thus leaving a lot of room for arbitrariness and creating the risk of varying interpretations in the different Member States.[156]

There is concern that in some Member States the condition will not be applied in practice, because *de facto* all (or at least, the overwhelming majority of) transfer operations carried out at present can be treated as "frequent", and particularly as "massive".[157] It seems that in a situation where a data exporter performs the appropriate assessment of all the circumstances surrounding the data transfer operation, as well as "appropriate safeguards" ("where necessary") are applied, there is no justification for introducing such far-reaching restrictions in that respect. Also, abandonment of the information obligation referred to in Article 44(6) of the Proposal should be considered, at least in relation to SMEs, as well as it should be explicitly stipulated that the obligation cannot be understood as a *de facto* obligation to obtain prior authorisation for transfer.

It is rightly noted that the use of the term "appropriate safeguards" in Article 44(1)(h) raises concerns. An identical term is used in Article 42, and the essence of "derogations" is the lack of "appropriate safeguards". Therefore, one of the following solutions should adopted:

- the term should be defined more precisely or replaced with a different term, so that it does not give rise to additional complications;[158] or
- the restriction should be abandoned in favour of another restriction, e.g. regarding the nature of the data transferred, rather than their scope or frequency (taking into account e.g. sensitiveness of data); or
- incorporate the regulation proposed in Article 44(1)(h) into Article 42, so as not to suggest that we are dealing with a legal institution different to what it really is.

## 4.6. Other mechanisms and instruments; elements of the accountability principle

In its document titled "The Future of Privacy", Article 29 Working Party suggested that:

> *"a new provision could be included in the new legislative framework pursuant to which data controllers would remain accountable and responsible for the protection of personal data for which they are controllers, even in the case the data have been transferred to other controllers outside the EU".*[159]

---

[155] Article 29 Data Protection Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995', WP 114 (25.11.2005).

[156] UK Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' (2012), p. 21.

[157] According to Ch. Kuner, such a restriction will render the condition inapplicable in the case of cloud computing (in : 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', Privacy & Security Law Report, 11 PVLR 06 (2012), p. 10).

[158] European Data Protection Supervisor, 'Opinion on the data protection reform package' (2012), [228].

[159] Article 29 Data Protection Working Party, 'The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data', WP 168 (1.12.2009), para. 39, p. 12.

The Regulation should in particular explicitly emphasise that entities which choose to transfer data to third countries are still accountable to ensure that personal data remains protected when transferred to such countries (at present, elements of that rule are contained only in Recital 89 of the preamble, but not without ambiguity). It seems that this is the Commission's attempt to retain the current adequacy system and improve it by adding certain components of the so-called **'accountability approach'**.[160] Such a solution requires, however, further in-depth analysis, especially as to how far the responsibility of data exporters, if any, should stretch in the context of such instruments as Binding Corporate Rules and other tools used for the purpose of data transfer operations. As has been noted in the doctrine:

> *"The proposal by the Working Party seems to be leading to an accumulation of the requirements of two different systems to regulate cross-border transfers (…) [i.e.] systems which are based on a territorial approach for data transfers (based on "adequacy" of protection in countries) and systems which have chosen the organisational approach (based on accountability of organisations). (…) In any event the provision proposed by the Working Party seems more stringent than the accountability provision in respect of data transfers as included, for instance, in the APEC Privacy Framework. (…) I therefore recommend that EU legislators not follow the proposal of the Working Party 29."*[161]

The new legal framework should also focus much more on **risk assessment** by data controllers/processors before the transfer takes place. The proposed Package introduces data protection impact assessment obligations, but they should be much more clearly applicable to the data transfer processes. In today's reality with ubiquitous information and data exchange, it is also necessary to create suitable conditions so that entities which transfer personal data are aware of the restrictions and their obligations. In this respect, extra-legal actions, in particular informational or educational measures, will be also of importance.

Some other mechanisms, like the development of an accreditation system[162] or, for example, the dedicated **Cloud Safe Harbour Programme**[163] (similar to the current EU-U.S. Safe Harbour Programme), could also be taken into account when reforming the current European data transfer regulation. Such a system or programme, based on certification, internal and external auditing and enforcement, would entail non-EU cloud providers who voluntarily agree to adhere to EU data protection requirements, and could strengthen the level of personal data protection worldwide. The same effect could be achieved with much broader use of the **self-regulatory instruments** in the data transfer context.

---

[160] See in this regards, e.g., Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability', WP 173 (13.07.2012); The Centre for Information Policy Leadership, 'Data Protection Accountability: The Essential Elements. A Document for Discussion', 2009; Ch. Kuner, 'Developing an Adequate Legal Framework for International Data Transfers', in: S. Gutwirth et al. (eds.), 'Reinventing Data Protection?',2009, pp. 263-273.

[161] L. Moerel, 'Binding Corporate Rules. Fixing the Regulatory Patchwork of Data Protection', 2011, available at: http://arno.uvt.nl/show.cgi?fid=116138, p. 390-394

[162] 'The Information Commissioner's response to the European Commission's consultations on the legal framework for the fundamental right to protection of personal data', p. 6.

[163] "EC Considering Cloud Safe Harbour Program As Data Directive Amendment, Reding Says", Privacy & Security Law Report, 10 PVLR 780 (23.05.2011).

## 4.7. International standards

The new legal instrument concerning cross-border data flows should also focus much more on **international standards** issues. Such standards may have different meanings, but they have generally the same purpose, i.e. to strengthen the level of personal data protection globally, especially when the data are being transferred to different locations. Examples of current business as well as technological developments (e.g. cloud computing) prove that the data can be moved to the other site of a globe with ease, at no great cost.

International standards should be then elaborated and strengthened – with the active involvement of the European Union – as an instrument of an emerging global law in the area of privacy/data protection, with a goal to establish global-wide, basic data protection rules and principles (even in a form of a binding international convention or some other form of international law). At the same time, the EU should take an active part in the discussion concerning various technical (international) standards, especially IT and industry standards (e.g., in the area of security of data or default settings used by the Internet users in the online world). **Technical standards** are not legally binding and can be adopted by states or organizations on a voluntary basis. Among many initiatives and organizations for standardisation in this regard one can mention:

- International Organization for Standardization (ISO) with its standards for general information and private data;[164]
- International Telecommunications Union (ITU) and its widely recognised standards covering various fields of telecommunications (e.g., data communication over the telephone network; data networks, open system communications and security, etc.);[165]
- World Wide Web Consortium (W3C)that has created already over 100 technical standards for World Wide Web, many of them influencing also privacy issues;[166]
- initiatives of regional bodies, e.g. American National Standards Institute (ANSI), or European Committee for Standardization (CEN). [167]

Both standards – legal as well as non-binding/technical – could have a great role in securing personal data protection globally, especially when constantly transferring the data. For these reasons, Article 45 of the Proposal should be supplemented, in order to concentrate also on such "appropriate steps" that could help to develop different forms of international standards, with the aim to increase the level of personal data protection globally.

---

[164] For example: ISO/IES 18028-5:2006 which provides guidance on the security aspects of the use of IT networks; 23207:2008 that seeks to safeguard the privacy of people's financial data processed by automated, networked information systems; or the 27000 standards series.

[165] See at: http://www.itu.int/ITU-T/

[166] See at: http://www.w3.org/standards/

[167] See, for example, CEN's publications concerning various aspects of personal data protection: CWA 15499-01:2006 and CWA 15499-02:2006 (Personal Data Protection Audit Framework (EU Directive EC 95/46)); CWA 15292:2005 (Standard form contract to assist compliance with obligations imposed by Article 17 of the Data Protection Directive 95/46/EC (and implementation guide)).

## 4.8. Recommendations

Based on the findings presented above, there are a number of recommendations which can be made to further improve the European trans-border data flow regime:

1. Article 42(5) of the Proposal (except for the last sentence), which provides for the possibility of basing data transfers on non-binding instruments, should be deleted. The reference in Article 34 will require to be changed accordingly.

2. The rule under which any transfer based on standard data protection clauses or Binding Corporate Rules does not require any further authorisation (Article 42(3) of the Proposal) should also apply to the so-called 'ad hoc clauses'. Under the Proposal application of such contractual clauses still requires from the controller or processor to obtain prior authorisation from the supervisory authority (Article 42(4)).Therefore, the rule prescribed in Article 42(3) should be amended in order to apply it also to the 'ad hoc clauses'; Article 42(4) – consequently – needs to be deleted.

3. The direction of changes in the context of "adequacy assessment" is correct, especially an introduction of a possibility of recognising particular territory or processing sectors within a third country as ensuring an adequate level of protection. Attempts to "centralise" the process of adequacy assessment, by giving the Commission increased and exclusive powers, should also be continued. Further refinement of the Commission's adequacy decisions should be, however, considered. In particular introduction into the preamble to the Regulation of a more precise definition of the scope of the term "processing sectors", used in Article 41(1) of the Proposal, would be advisable.

4. The "logistics" of how adequacy decisions are to be issued and used under the Proposal needs to be addressed, especially the following should be defined:

   - rules of conducting the assessment, including its initiation, the involvement of the national supervisory authorities and the European Data Protection Board;
   - rules of further "handling" of adequacy decisions, in particular in the context of the requirement to carry out periodic assessments.

5. The new legal framework should also focus much more on risk assessment by the data controllers/processors before the data transfer takes place.

6. The Regulation should explicitly emphasise that entities who chose to transfer data to third countries are still accountable to ensure that personal data remain protected when transferred to such countries.

7. It would be advisable to explicitly emphasise within the General Regulation the possibility of using standard data protection clauses also by data processors ('processor-to-(sub)processors model clauses').

8. The regulation regarding Binding Corporate Rules requires further increase of its flexibility and corrections, in particular:

   - it should be specified whether that institution could be limited to a part of a group of undertakings;
   - introduction of facilitation as regards adoption and approval of Binding Corporate Rules by smaller entities, especially SMEs, should be considered.

9. The Data Protection Package should define the term of “data transfer”.

10. The so-called “derogations” (Article 44 of the Proposal) need to be further elaborated and clarified, especially as regards the derogation of the data controller’s legitimate interests.

11. It is necessary to explicitly define in the Package the consequences of the so-called negative adequacy decisions issued by the Commission, i.e. whether in such case the transfer of personal data to a ‘black-listed’ third country is totally prohibited or allowed under some conditions.

12. Some other mechanisms, like the development of an accreditation system or the dedicated Cloud Safe Harbour Programme, as well as self-regulatory instruments and industry standards, could also be taken into account when reforming the current European data transfer regulation.

13. The new legal instrument concerning cross-border data flows should also focus much more on international standards issues. For these reasons, e.g., Article 45 of the Proposal should be supplemented, in order to concentrate also on such “appropriate steps” that could help to develop different forms of international standards, with the aim to increase the level of personal data protection globally.

# CONCLUSIONS

The Proposal has been analysed in four chapters respectively relating to mapping new technologies and services, the internal market dimension, strengthening consumer rights and international data transfers. In general, it can be concluded that the Proposal represents a improvements in each of the aspects covered, however, there are a number of recommendations which can be made to improve its content and achieve the goals set. Each chapter contains a separate section making specific conclusions and a number of recommendations. In order to avoid repetition, reference is made to the conclusions and recommendations made in 1.3 on mapping new technologies and associated data protection issues, 2.5 on the internal market dimension, 3.3 on strengthening consumer rights and 4.8 on international data transfers as well as the priority mesures mentioned in the Executive Summary.

# REFERENCES

## Institutions and Organisations


- American Chamber of Commerce to the European Union, 'Response to the Commission communication on a comprehensive approach on data protection in the European Union, 14.01.2011.
- Analysis and impact study on the implementation of Directive 95/46 in Member States' (Annex to the First Commission's report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final).
- Article 29 Data Protection Working Party, 'Opinion 7/2003 on the re-use of public sector information and the protection of personal data', WP 83 (12.12.2003).
- Article 29 Data Protection Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995', WP 114 (25.11.2005).
- Article 29 Data Protection Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Woldwide Interbank Financial Telecommunication (SWIFT)', WP 128 (22.11.2006).
- Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data', WP 136 (20.06.2007).
- Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking', WP 163 (12.06.2009).
- Article 29 Data Protection Working Party, 'The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data', WP 168 (1.12.2009).
- Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', WP 169 (16.02.2010).
- Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability', WP 173 (13.07.2012).
- Article 29 Data Protection Working Party, 'Opinion 11/2011 on the level of protection of personal data in New Zealand', WP182 (4.04.2011).
- Article 29 Data Protection Working Party, 'Opinion 12/2011 on smart metering', WP 183 (4.4.2011).A
- Article 29 Data Protection Working Party, 'Opinion 01/2012 on the data protection reform proposal', WP 191 (23.03.2012).
- Article 29 Data Protection Working Party, 'Opinion 02/2012 on facial recognition in online and mobile services', WP 192 (22.03.2012).
- Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies', WP 193 (27.04.2012).
- Article 29 Data Protection Working Party, 'Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules', WP 195 (6.06.2012).
- Article 29 Data Protection Working Party, 'Opinion 15/2012 on the definition of consent', WP 187 (13.07.2011).

- British Bankers' Association and the Association for Financial Markets in Europe, 'EU General Data Protection Regulation' (2012), available at: http://webarchive.nationalarchives.gov.uk/+/http://www.bis.gov.uk/policies/consumer-issues/personal-data
- Centre for Information Policy Leadership, 'Data Protection Accountability: The Essential Elements. A Document for Discussion', 2009.
- Commission Decision no. 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.
- Commission Staff Working Paper, 'Impact Assessment', SEC(2012) 72 final.
- Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, 'Towards a new Framework for Electronic Communications Infrastructure and Associated Services: The 1999 Communications Review', COM (1999) 539 final.
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Open data. An engine for innovation, growth and transparent governance', draft, 2011, available at: http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive_proposal/2012/open_data.pdf
- CONSUMER PRIVACY BILL OF RIGHTS issued by the White House in February 2012, available at: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
- Council of Europe, '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', available at: https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM
- DLA Piper, 'The future of online privacy data protection' (2009).
- Dutch Data Protection Authority (College beschermingpersoonsgegevens, CBP), 'Report of findings. Official investigation by the CBP in to the processing of geolocation data by TomTom N.V.', available at: http://www.dutchdpa.nl/downloads_overig/en_pb_20120112_investigation-tomtom.pdf
- Dutch Data Protection Authority (College beschermingpersoonsgegevens, CBP), 'Final findings. Dutch Data Protection Authority investigation into the collection of Wifi data by Google using Street View cars', available at: http://www.dutchdpa.nl/downloads_overig/en_pb_20110811_google_final_findings.pdf
- European Commission, 'First report on implementation of the Data Protection Directive (95/46/EC)', COM(2003) 265 final.
- European Data Protection Supervisor, 'Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"' (14.01.2011).
- European Data Protection Supervisor, Opinion on the data protection reform package (2012).

- FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC', WP 176, (12.07.2010).
- Federation of European Direct and Interactive Marketing, 'FEDMA submission on the Comprehensive Strategy on Data Protection in the European Union', 15.01.2011.
- French Data Protection Authority (Commission nationale de l'informatique et des libertés, CNIL), 'Google's new privacy policy raises deep concerns about data protection and the respect of the European law', available at: http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-raises-deep-concerns-about-data-protection-and-the-respect-of-the-euro/
- FTC Privacy Recommendations of March 2012, available at: http://www.scribd.com/doc/86771514/FTC-Privacy-Recommendations
- Hamburg Commissioner for Data Protection and Freedom of Information against Facebook and Google: http://www.datenschutz-hamburg.de/pressemitteilungen-und-informationen/pressemitteilungen.html
- Hamburg Commissioner for Data Protection and Freedom of Information: http://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/PressRelease-2012-08-15-Facebook_Proceedings.pdf
- Internet Advertising Bureau UK, 'European Commission General Data Protection Regulation: IAB UK response to Ministry of Justice Call for Evidence' (2012).
- Letter of the Director-General Robert Madelin of DG Information Society and Media Directorate-General, available at: http://lists.w3.org/Archives/Public/public-tracking/2012Jun/att-0604/Letter_to_W3C_Tracking_Protection_Working_Group.210612.pdf
- Linklaters on Technology Media and Telecommunications, available at: http://www.linklaters.com/pdfs/mkt/london/January_2012_Newsletter_PDF.pdf
- Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor)', WP 161 (5.03.2009).
- Opinion of the European Data Protection Supervisor on the data protection reform package.
- Opinion of the European Data Protection Supervisor on the 'Open-Data Package' of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the reuse of Commission documents, 18.04.2012.
- Hamburg Commissioner for Data Protection and Freedom of Information of 7 June 2012 (press release), available at: www.datenschutz-hamburg.de/news/detail/article/verfahren-gegen-facebook-vorlaeufig-ausgesetzt.html
- Processing of sensitive personal data in a cloud solution', J.no. 2010-52-0138 (3.02.2011), available at: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution

- 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 (2010).
- Report from the Commission: First report on the implementation of the Data Protection Directive (95/46/EC)', COM(2003) 265 final.
- Response of the Association for Financial Markets in Europe (AFME) and the British Bankers' Association (BBA) of 6 March 2012 to a call for evidence of the UK Ministry of Justice, p. 3.; available at http://www.bba.org.uk/download/7512
- "Social Networking", a quantitative and qualitative research report into attitudes, behaviours and use page 51, available at: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/report1.pdf, recalled the 28th of June 2012
- UK Information Commissioner's Office, 'Draft Anonymisation code of practice', May 2012.
- UK Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' (2012).
- UK Ministry of Justice, 'Summary of Responses to Call for Evidence on Proposed EU Data Protection Legislative Framework' (June 2012).

## Individual Authors


- B. van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC', Computer Law & Security Review 28 (2012).
- B. van Alsenoy, J. Ballet, A. Kuczerawy, J. Dumortier, 'Social networks and web 2.0: are users also bound by data protection regulations?', Identity in the information society, 2009.
- M.D. Birhnack, 'The EU Data Protection Directive: An Engine of a Global Regime', Computer Law & Security Report 24 (2008) 6.
- P. de Hert, V. Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', Computer Law & Security Review 28 (2012).
- W.K. Hon, Ch. Millard, 'Data Export in Cloud Computing –How can Personal Data be Transferred outside the EEA? The Cloud of Unknowing, Part 4', Queen Mary University of London, School of Law, Legal Studies Research Paper No. 77/2011.
- W.K. Hon, Ch. Millard, I. Walden, '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.
- N.J. King, P.W. Jessen, 'Profiling the mobile customer – Is industry self-regulation adequate to protect consumer privacy when behavioural advertisers target mobile phones? – Part II', Computer Law & Security Review 26 (2010).
- Ch. Kuner, 'Developing an Adequate Legal Framework for International Data Transfers', in: S. Gutwirth et al. (eds.), 'Reinventing Data Protection?', 2009, pp. 263-273.
- Ch. Kuner, 'European Data Protection Law. Corporate Compliance and Regulation', Oxford University Press, 2007.
- Ch. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', Privacy & Security Law Report, 11 PVLR 06 (2012).
- L. Moerel, 'Binding Corporate Rules. Fixing the Regulatory Patchwork of Data Protection', 2011, available at: http://arno.uvt.nl/show.cgi?fid=116138.
- R. Marchini, S. Delon-Bouquet, O. Fasshauer, J.-Y. Steyt, B. Verdegem, 'Legitimising Cross-Border Data Flows by the "Self-Assessment" Method: Different Approaches Throughout Europe', World Data Protection Report, January 2007, p.23-28.
- Ch. Reed, 'The Law of Unintended Consequences – embedded business models in IT regulation', Journal of Information, Law & Technology, 2007, available at SSRN: http://ssrn.com/abstract=1017290.
- B.W. Schermer, 'The limits of privacy in automated profiling and data mining', Computer Law &Security Review 27 (2011).
- B. van der Sloot, 'Public Sector Information & Data Protection: A Plea for Personal Privacy Settings for the Re-use fo PSI', 2011, available at: http://www.ivir.nl/publications/sloot/Public%20sector%20information%20and%20data%20protection.pdf
- Winton, N. Cohen, 'Proposed EU Framework – Online Advertising, E-Commerce and Social Media', (2012), available at http://www.whitecase.com/articles-04172012

## Legal Materials

- 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 final.
- 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, COM(2012) 10 final.
- Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.
- 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.
- Case C-101/01 [2003] ECR I-12971.
- Case C-73/07 [2008] ECR I-9831.

EUROPEAN PARLIAMENT

CATALOGUE BA-31-12-929-EN-C

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

# POLICY DEPARTMENT A
## ECONOMIC AND SCIENTIFIC POLICY

## Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

## Policy Areas

- Economic and Monetary Affairs
- Employment and Social Affairs
- Environment, Public Health and Food Safety
- Industry, Research and Energy
- Internal Market and Consumer Protection

## Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.


ISBN 978-92-823-3860-5
doi 10.2861/45280

Publications Office

Reforming the Data Protection Package