EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY

COMPARATIVE STUDY

ON

DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES,

IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS

Contract Nr: JLS/2008/C4/011 – 30-CE-0219363/00-28

FINAL REPORT

Submitted by:

LRDP KANTOR Ltd (Leader)

In association with

Centre for Public Reform

20 January 2010

(final final version)

CONTENTS

RESEARCH TEAM:

	Title/Position:	**Institution(s):**	**Nationality:**
Core Experts:			
Douwe Korff	Professor of International Law	London Metropolitan University, London, UK	NL
Ian Brown	Senior Research fellow	Oxford Internet Institute, University of Oxford, UK	UK
Special Experts:			
Peter Blume	Professor of Legal Informatics	Faculty of Law, University of Copenhagen, Copenhagen, Denmark	DK
Graham Greenleaf	Professor of Law	University of New South Wales, Sydney, Australia	AUS
Chris Hoofnagle	Senior Fellow	Berkeley Center for Law and Technology, University of California, Berkeley, CA, USA	USA
Lilian Mitrou	Assistant Professor	Department of Information and Communication Systems Engineering, University of the Aegean, Mytilene, Greece	GR
Filip Pospíšil, Helena Svatošová, Marek Tichy	Researchers	NGO *Iuridicum Remedium*, Prague, Czech Republic	CZ
Advisers:			
Ross Anderson	Professor of Security Engineering	University of Cambridge, UK	UK
Caspar Bowden	Chief Privacy Adviser , Microsoft EME&A	Microsoft Corporation	UK
Katrin Nyman-Metcalf	Professor of International & Comparative Law	Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia	EST
Paul Whitehouse	Former Chief Constable (Head of Police Force)	Sussex Police (retired) now Chairman of the Gangmasters Licensing Authority	UK

GLOSSARY & INTERNET REFERENCES:

APEC : Asia-Pacific Economic Cooperation, see: http://www.apec.org/

APPA : Asia Pacific Privacy Agencies, see: http://www.privacy.gov.au/aboutus/international/appa

ASEAN : Association of Southeast Asian Nations, see: http://www.aseansec.org/

BBB : Better Business Bureau OnLine Privacy Seal, a US-based privacy seal, see: http://www.bbbonline.org/privacy/

BCRs : Binding Corporate Rules, self-regulatory rules to ensure data protection compliance within (multinational) companies, encouraged by the *WP29**, see WP29 documents WP153, 154 and 155, available from: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm

CCTV : Closed-Circuit Television

Charter of Fundamental Rights: The Charter of Fundamental Rights of the European Union, proclaimed in Nice in 2000 and which has become a binding legal instrument following the *Lisbon Treaty**. Unlike the European Convention on Human Rights (*ECHR**), the Charter includes a specific provision guaranteeing data protection, Article 8. See: http://www.europarl.europa.eu/charter/default_en.htm

Cloud computing: Computing in which the user's data and the applications s/he uses are no longer installed on the user's personal computer (PC), but hosted on servers and made available to him/her through browsers over the Internet

COE : Council of Europe, the oldest and broadest European organisation, parent to both the European Convention on Human Rights (*ECHR**) and *Convention No. 108** (among many other treaties).

COE Convention No. 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series (CETS) No. 108, adopted on 28 January 1981 (entry into force 1 October 1985), the first international treaty on data protection. An Additional Protocol to the Convention (CETS No. 181, adopted in 2001 and in force since 2004), stipulates additional requirements relating to supervisory authorities (*DPAs**) and transborder data flows.

(COE) CJ-PD : (Council of Europe) Project Group on Data Protection, operating under the *COE*'s* European Committee on Legal Cooperation (CDCJ), see: http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Steering_Committees/cdcj/

Dataveillance	:	The surveillance of individuals through the "data trails" they leave in the electronic/information society, e.g., on the Internet or through credit- or debitcard payments
DNA	:	Deoxyribonucleic acid, a nucleid acid that provides the code to genetic information, increasingly used for identification in forensic and other contexts, as well as for medical treatment
DPA	:	Data Protection Authority (also referred to as [Office of the] Information- or Privacy Commissioner, etc.)
EC	:	European Community, the original part of what is now the *EU**, and until the *Lisbon Treaty** (which abolished it) constituting the "*First Pillar*"* of the EU
ECHR	:	The European Convention on Human Rights, the most important European human rights instrument, enforced by the European Court of Human Rights (*EctHR**) (see there for link)
ECtHR	:	The European Court of Human Rights, responsible for upholding the European Convention on Human Rights (*ECHR**), see: http://www.echr.coe.int/echr/Homepage_En
ECJ	:	The European Court of Justice, full name: the Court of Justice of the European Union (*EU**), see: http://curia.europa.eu/jcms/jcms/Jo2_6999/
EDPS	:	The European Data Protection Supervisor, responsible for ensuring data protection compliance within the EU institutions and to advise on data protection law and policy; see: http://www.edps.europa.eu/EDPSWEB/
EEA	:	European Economic Area, a group of countries linked to but not members of the *EU**. Since the accession of Austria, Finland and Sweden to the EU, there are only three EEA States: Iceland, Liechtenstein and Norway. EEA States are required to implement the EC *acquis*, including the EC data protection directives, in the same way as the EU Member States. Hence the references in the text to "EU/EEA States"
EPR	:	Electronic Patient Record (also referred to as Electronic Health Record)
EU	:	European Union, see: http://europa.eu/
EuroPriSe	:	The European Privacy Seal, established with support of the EU Commission, see: https://www.european-privacy-seal.eu/
First Pillar	:	Another name for the European Community (*EC**), the original part of what is now the *EU**. There was also a Second Pillar, covering the EU's Common Foreign and Security Policy, and a *Third Pillar** covering Police and Judicial Cooperation in Criminal Matters. The pillars were abolished by the *Lisbon Treaty**.
FRA	:	The Fundamental Rights Agency of the European Union, see: http://fra.europa.eu/fraWebsite/home/home_en.htm

IP address	:	A numerical label, based on the "Internet Protocol" used for communications between devices linked to the Internet, that identifies the device (usually, a personal computer or PC) that is being used for the communication
Lisbon Treaty	:	The Treaty of Lisbon, signed at Lisbon, 13 December 2007, OJ 2007/C 306/01. The Lisbon Treaty amended (but does not replace) the Treaty on European Union (TEU) and the Treaty establishing the European Community (TEC, since renamed Treaty on the Functioning of the European Union or *TFEU**). The Lisbon Treaty streamlined the decision-making processes within the EU and abolished the previous three "pillars" of the EU (see *First Pillar** and *Third Pillar**).
MMS	:	Multimedia Messaging Service, used to send multimedia content with short messages ("texts"), usually by mobile phone (see also *SMS**)
NGO	:	A Non-Governmental Organisation (as opposed to a Governmental- or Inter-Governmental [IGO] one)
OECD	:	The Organisation for Economic Cooperation and Development, see: http://www.oecd.org/
P3P	:	Platform for Privacy Preferences, a privacy-enhancing technology (*PET*)* that seeks to allow users to know the privacy practices of websites and to choose the desired settings, see: http://www.w3.org/P3P/
PBD	:	Privacy By Design, a computer design approach, originally developed by the Ontario Privacy Commissioner, but also encouraged by (e.g.) the UK Information Commissioner, that supports the production and operation of privacy-friendly systems, see: http://www.privacybydesign.ca/ and: http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx
PETs	:	Privacy Enhancing Technologies
PIA	:	Privacy Impact Assessment, an assessment of products, services, policies or systems, carried out before these are implemented, to ensure they will be privacy-friendly, compulsory in several jurisdictions
PNR	:	The so-called Passenger Name Record, a list of information on passengers on international flights, the compulsory collection and disclosure of which to the USA caused a major data protection controversy. See the "Article 29 Working Party (*WP29**) Opinion 2/2004 of 29 January 2004 (WP87), available from: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_en.pdf (Cf. also the Council and Commission views and decisions on the issue, at: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm)
Prüm Treaty	:	An international police co-operation agreement, originally signed by Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria on 27 May 2005, which since the coming into force of the *Lisbon Treaty** has

		become part of the general legislative framework of the European Union and will be implemented in all Member States. See: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/803
RFID	:	Radio Frequency Identification, a tiny tracking device that can be attached to clothes, passports, etc. See EU Commission Recommendation C (2900) 3200 (final) of 12.5.2009, *on the implementation of privacy and data protection principles in applications supported by radio-frequency identification*, available from: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
SMS	:	Short Messaging Service, also known as text messages (or "texts"), usually sent by mobile phone (see also *MMS**)
SNS	:	Social Networking Site, such as FaceBook.
Solange	:	German for "as long as". The "*solange* problem" is the problem that arises when national (constitutional) courts refuse to accept the supremacy (or primacy) of EU law if they feel that that law does not comply with the fundamental human rights requirements of the relevant national constitution. The problem has mainly arisen in Germany, but also exists in other countries with strong constitutional human rights protection such as Italy.
SWIFT	:	The Society for Worldwide Interbank Financial Telecommunication, an inter-bank organisation that facilitates international bank transfers, involved in a major data protection controversy. See the "Article 29 Working Party (*WP29**) Opinion 10/2006 of 22 November 2006 (WP128), available from: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf
TFEU	:	The Treaty on the Functioning of the European Union, the new name of the Treaty establishing the European Community. The TFEU has been amended (but not replaced) by the *Lisbon Treaty**
Third Pillar	:	The part of the *EU** which used to cover Police and Judicial Cooperation in Criminal Matters. There was also a First Pillar, covering the *EC**, and a Second Pillar, covering the EU's Common Foreign and Security Policy. The pillars were abolished by the *Lisbon Treaty**.
TRUST-e	:	A US-based privacy seal, see: http://www.truste.com/
TrustGuard	:	A US-based seal that seeks to ensure customer privacy, customer information security and business identity protection at the same time, see: http://www.trust-guard.com/
ULD	:	The Independent State Centre for Data Protection (*Unabhängiges Landes-zentrum für Datenschutz*) of the German State of Schleswig-Holstein, which also administers the European Privacy Seal (*EuroPriSe**) system

VRM	:	Vendor Relationship Management, a customer-centred (and privacy-friendly) data management system (as opposed to business-centred, usually less privacy-friendly Customer Relationshop Management systems)
WP29	:	The "Article 29 Working Party" (or Working Group/*Groupe de Travail*) established under the main *EC** Directive on Data protection (Directive 95/46/EC), that provides important opinioins and guidance on the application and interpretation of that directive and the other data protection directives. See:http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm
WTO	:	The World Trade Organisation, see: http://www.wto.org/
Qui tam	:	An abbreviation from the Latin "*qui tam pro Domino rege quam pro sic ipso in hoc parte sequitur"* meaning "who as well for the King as for himself sues in this matter." It is currently used to refer to a special provision of the US Federal Civil False Claims Act that allows private citizens to file a lawsuit in the name of the US Government charging fraud by government contractors and others who receive or use government funds. If succesful in the lawsuit, the citizen in question receives a share of any money recovered.
Safe Harbor	:	An EU-USA arrangement under which US corporations can declare their compliance with European data protection principles, and are then supervised by the US Federal Trade Commission (FTA), see: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/adequacy-faq1_en.htm

For the definitions of core concepts in the Data Protection Directive, see Article 2 of the Directive. This covers:

–	"personal data "	(Article 2(a))
–	"processing [of personal data"	(Article 2(b))
–	"personal data filing system"/"filing system"	(Article 2(c))
–	"controller"	(Article 2(d))
–	"processor"	(Article 2(e))
–	"third party"	(Article 2(f))
–	"recipient"	(Article 2(g))
–	"the data subject's consent"	(Article 2(h))

The report also refers to several EU projects or programmes, on which further information can be found at the websites below:

EuroPriSe	:	https://www.european-privacy-seal.eu/
PRIME	:	https://www.prime-project.eu/
PRISE	:	http://www.prise.oeaw.ac.at/

For various Internet applications referred to in the text, see the relevant websites:

Amazon	:	http://www.amazon.com/ and national sites, such as: http://www.amazon.co.uk/
Boing Boing	:	http://boingboing.net/
Facebook	:	http://www.facebook.com/
Flickr	:	http://www.flickr.com/
Google	:	http://www.google.com/ and national sites such as: http://www.google.co.uk/
MySpace	:	http://www.myspace.com/
YouTube	:	http://www.youtube.com/

- o – O – o -

I. Introduction

1. This is the Final Report on a study commissioned by the European Commission's Directorate-General for Justice, Freedom and Security and carried out under the guidance of its Data Protection Unit between October 2008 and August 2009. It follows on from an Inception Report, submitted in December 2008, an Interim Report, submitted in March 2009 (as revised in the light of the Commission's comment), and a Draft Final Report, submitted in August 2009. It takes into account the Commission's final comments.

2. The study was carried out by Prof. Douwe Korff of London Metropolitan University and Dr. Ian Brown of the Oxford Internet Institute of Oxford University, assisted by the following European and non-European experts: Prof. Peter Blume (Denmark), Prof. Graham Greenleaf (Australia), Prof. Chris Hoofnagle (USA), Prof. Lilian Mitrou (Greece), Filip Pospíšil, Helena Svatošová, Marek Tichy (Czech Republic); and advised by: Prof. Ross Anderson (UK), Caspar Bowden (UK/France), Paul Whitehouse (UK), and Prof. Katrin Nyman-Metcalf (Estonia). (For full details see page 2, above)

3. The purpose of the study was to identify the challenges for the protection of personal data produced by current social and technical phenomena such as:

   - ✓ *the Internet;*
   - ✓ *globalisation;*
   - ✓ *the increasing ubiquity of personal data and personal data collection;*
   - ✓ *the increasing power and capacity of computers and other data-processing devices;*
   - ✓ *special new technologies such as RFID, biometrics, face- (etc.) recognition, etc.;*
   - ✓ *increased surveillance (and "dataveillance"); and*
   - ✓ *increased uses of personal data for purposes for which they were not originally collected, in particular in relation to national security and the fight against organised crime and terrorism -*

   and to produce a report containing a comparative analysis of the responses that different regulatory and non-regulatory systems (within the EU and outside it) offer to those challenges, and that provides guidance on whether the legal framework of the main EC Directive on data protection (Directive 95/46/EC) still provides appropriate protection or whether amendments should be considered in the light of best solutions identified. This is that report.

4. As requested by the Commission, the team closely analysed all major aspects of the way in which the legal systems in several selected EU Member States have implemented the Directive (in terms of both substantive norms and formal procedures and oversight), and addressed the question of overlapping jurisdictions (conflicts of law) within the EU. We also examined the regulatory system on these matters in the United States of America, at both Federal and State level, in two States providing a representative picture; in two further non-EU countries which are members of the OECD, and in two countries outside the Economic European Area which are not members of the OECD. The study thus looked at more than a dozen widely different legal systems.

   This resulted in a series of Country Reports, submitted with this Draft Final Report, covering the following countries and jurisdictions:

COUNTRIES AND JURISDICTIONS COVERED:

A. European countries:

- Czech Republic
- Denmark
- France
- Germany
- Greece
- United Kingdom

B. Non-European countries and jurisdictions:

- USA:
  - Federal level
  - California
  - New Jersey
- Australia
- Hong Kong
- India
- Japan

5. In accordance with the contract and the wishes of the Commission, the present (final) report, as such, has been kept short and focused on the main topics of the study. Further information and analysis is provided in separate reports and papers, submitted with this Final Report (see list of attachments at the end of this report). Most of these were submitted earlier as part of the Interim Report, but have been expanded in the light of comments from the Commission. Specifically:

- **Section II** of this Draft Final Report provides an overview of the challenges we identified as stemming from the phenomena listed in para. 3, above.

  For further detail, see: Working Paper No. 1: The challenges to European data protection laws and principles - An overview of the global social and technical developments and of the challenges they pose to data protection.

- **Section III** provides our overall summary and assessment of the current EU data protection regime and of the difficulties it has in facing the above-mentioned challenges, with reference to similar (or contrasting) issues in the non-EU countries and jurisdictions, as further discussed in Section V (see the indent on that section, below, for references).

- **Section IV** very briefly notes certain wider but fundamental matters that must be taken into account in any review of the data protection regime in the EU.

  For further detail, see: Working Paper No. 1 (already mentioned); Douwe Korff, *Paper No. 4: The Legal Framework*, in: Ian Brown & Douwe Korff, Privacy & Law Enforcement, study for the UK Information Commissioner, 2004, (included in the material submitted with this report); and the Country Reports (including in particular the Country Report on Germany).

– **Section V** contains our more specific conclusions and recommendations. They are based on the overall assessment set out in Section III, and take account of the fundamental requirements noted in Section IV. This section seeks to identify, from the wealth of comparative information obtained in the course of the study, the most appropriate and effective answers to the different challenges, including both best legal approaches and best practices, and alternative, innovative solutions to the challenges (including in particular solutions not yet fully tried in Europe), with suggestions on how these could be used to preserve and strengthen the EU data protection regime.

For further detail (especially also of the underlying analyses), see: Working Paper No. 2: Data protection laws in the EU - The difficulties in meeting the challenges posed by global social and technical developments, and the Country Reports.

– Finally, with this report, we provide a **Glossary** of technical terms (above, p. 3), a **Comparative Chart** (attached) and an **Executive Summary**. The Executive Summary is submitted as a separate document, for easy dissemination.

- o – O – o -

II. Overview of the Challenges[1]

6. In broad terms, there are two (interwoven) strands to the developments addressed in this study. The first strand consists of challenges caused by technical developments; the second of challenges resulting from social and political changes and choices. They are interwoven, in that many new technologies both in themselves make the effective application of data protection more difficult (although some may help in this), and drive new, more intrusive policies, or are eagerly used to further them.

7. We have seen dramatic technological change since the European Commission first proposed the Data Protection Directive in 1990. The Internet has moved out of the university lab into 56% of European homes and 95% of OECD businesses. Computer processing power has continued to follow Moore's Law, with transistor density doubling every 18-24 months – around one thousand-fold in the last two decades. Computer storage capacity and communications bandwidth have both been increasing even more quickly, doubling every 12 months and hence a thousand-fold each decade. These exponential increases have radically increased the ability of organisations to collect, store and process personal data. The physical environment is now saturated with sensors such as CCTV cameras and mobile phones, with biometric and electronic identifiers used to link data to individuals. In the digital world almost every communication and Web page access leaves behind detailed footprints. The Internet and mobile information appliances allow large quantities of personal data to be trivially moved between jurisdictions. Data mining tools attempt to find patterns in large collections of personal data, both to identify individuals "of interest" and to attempt to predict their interests and preferences. New multinational companies have sprung up around these technologies to service a global customer base, with smaller enterprises outsourcing employee and customer data processing to developing world companies.

8. Governments are increasingly analysing and exchanging information on their citizens in response to fears over terrorist attacks. Individuals are using social networking sites to share information about themselves and their family, friends and colleagues. The ubiquity of personal data and of data gathering means that the default position is shifting from state and private bodies having to decide to collect data to one in which they have to make an effort not to collect (increasingly sensitive) data.[2]

9. This technical development feeds into the major social and political trends of the day. We all worry about terrorism, child pornography and serious international organised crime. The State also worries about exploding budgets for health care, education and social welfare. Governments want to encourage "good" behaviour, and discourage "bad" behaviour (in a much wider sense than "non-criminal" vs. "criminal"). In some countries – in the EU, in particular, the UK – the authorities believe that the more information its officials can get, and share, the better it can tackle social ills, be this teenage pregnancy, obesity or "extremism" that may lead to terrorism. E-government

[1] For full details and full references, see Working Paper No. 1: The challenges to European data protection laws and principles - An overview of the global social and technical developments and of the challenges they pose to data protection. This section is essentially just a short summary of the issues discussed in detail there.

[2] We are using the words "default position" here to describe a social-organisational attitude, not a technical setting. The issue of default settings for applications (including Internet-based applications) is addressed in Section V, sub-section V.8, below. See also section V, sub-section V.2(ii), para. 35.

systems typically contain large quantities of sensitive personal data on entire populations, shared between government departments using specific "gateways" contained in legislation. "Back office" systems focus on the more effective processing of data and the enabling of new services (including fraud detection and prevention related to benefit payments and tax returns) out of the citizens' gaze. "Portals" enable citizens to interact online with the government, supplying information such as tax returns and applying for services without the cost to either party of face-to-face or telephone conversations and manual form processing. Electronic Patient Records (EPRs), digital versions of medical records, are being nationally specified in countries including France, the US, Canada, Germany and the UK. Most of these projects are focusing on interoperability standards that allow different healthcare providers (public and private) to exchange medical information as patients receive treatment at different locations. Plummeting costs mean that the sequencing of patients' genomes is likely to become routine. The ageing of the baby boomer demographic in North America and Europe is likely to produce strong cost pressures for the out-patient treatment of chronic health conditions in older citizens, and we are therefore likely to see much more detailed information automatically gathered on physiological indicators and more general lifestyle data for the elderly and the less well. Law enforcement and intelligence agencies have been eager to gain access to the wide range of personal information that has become available from information systems created for very different purposes. This trend has intensified since 2001 under the rubric of "national security" and anti-terrorism purposes – including monitoring of financial transactions to reduce money laundering. Many governments have taken powers to require that Internet Service Providers make their networks "wiretap-capable" and retain data about customers' communications for later access by officials. Data protection is seen as an obstacle to State policies of this kind.

10. As retailers have moved online and new e-businesses such as Amazon have captured significant percentages of global markets, they have taken advantage of their servers' ability to gather detailed transactional histories of their customers' activities. E-commerce stores can see not just their customers' purchasing behaviour, but every product customers consider and for how long before deciding whether or not to buy. Advertising networks can track individuals' browsing behaviour across thousands of web sites. Service providers such as search engines can store all information provided by a user, such as search terms. It took pressure from the Article 29 Working Party for companies such as Google to limit the time for which this information was stored, but many online business models are dependent on advertising revenue and there will be continued pressure to target adverts more effectively using information on users' interests. It is difficult if not practically impossible for ordinary consumers to prevent such monitoring.

11. "Web 2.0" technologies allow users to create and share text, audio and video on blogs, photo and video sites such as Flickr and YouTube, and the now-ubiquitous social networks such as MySpace and Facebook. Combined with the still and video cameras present in most mobile phones, this has allowed individuals to share information about themselves and those around them to an unprecedented degree. Social networks now have hundreds of millions of members around the world, while high-profile blogs like BoingBoing have readerships to rival national newspapers.

12. In addition, both technology and government policies have tended to globalise data collection and dissemination, and to diffuse data storage. Ordinary citizens as well as criminals and terrorists physically travel to, and act in, many countries. Recent International Civil Aviation Organisation passport standards require that fingerprint and facial images be included on chips within new "e-passports". The EU now requires this data to be included in Schengen state passports, partly in response to US threats to otherwise withdraw Europeans' visa waiver status. Large-scale trials have found significant difficulties in registering and verifying fingerprints and iris scans, especially for disabled individuals. Personal data travel much more, over the Internet, through social networking sites and e-shops –- but also in the context of international cooperation between public authorities aimed at identifying suspected football hooligans, illegal or trafficked migrants, subversives, terrorists and paedophiles. Being given any of the above labels by any authority, or even on a social Web site, in any country, can quickly lead to such a stigma becoming all pervasive, without it being possible to challenge the body that initially made the mark (or even to identify that body). The European Court of Human Rights recently found that the indiscriminate nature of the UK DNA database breached the right to privacy in the European Convention – yet under the Hague "principle of availability" and the Prüm Treaty, we are seeing increasing sharing of such data by law enforcement agencies – without "fully satisfactory" data protection, according to the European Data Protection Supervisor.

13. Finally, there are the constraints on technology that should be considered. There are serious, often inherent limitations on many of the technologies in question. Face and gait recognition are far from perfect. Biometric data are not as conclusive as often thought. "Profiling" suffers from inherent limitations. The US National Research Council recently published a report on counter-terrorism technologies that concluded: "*there is not a consensus within the relevant scientific community nor on the committee regarding whether any behavioral surveillance or physiological monitoring techniques are ready for use at all in the counterterrorist context given the present state of the science.*" This is a fundamental difficulty based on the extremely high number of false positives thrown up by searches for potential terrorists and the ease with which terrorists can adapt their behaviour to mask their intentions. There are also concerns that data mining can lead to automated discrimination, where individuals are treated unfairly based on assumptions made about their behaviour based on previous transactional data.

14. Any consideration of the implications of technological developments should seriously consider these constraints. Over-reliance on technologies, marvelous though they may seem, is likely to result in serious injustice and bad governance. Effective data protection creates not just privacy in a narrow sense, but also protection against such trends and outcomes.

- o – O – o -

III. The difficulties in facing the challenges: Summary & Overview[3]

15. The basic data protection principles, rules and criteria, as developed in Europe by the COE and the EU, and as also broadly endorsed globally, in particular by the OECD, as such, have stood the test of time, even if they may need strengthening in some respects. It is a testimony to their wide acceptance that they are increasingly adopted as the basis for legislation in many parts of the world, including Asia and Africa.[4]

    They have had less impact on privacy laws in the USA: some US privacy laws incorporate some of the basic principles of data protection, but the scope of these laws are very limited, leaving much information collection to be regulated by other rules, such as the rules against unfair or deceptive business practices.[5] However, this has, if anything, served to underline the overall weakness of the USA model (to the extent that one can speak of a single model there). The basic European principles should therefore be re-affirmed and, if anything, strengthened; and efforts to obtain their adoption world-wide should continue.

    This is further discussed (with reference to Working Paper No. 2 in particular) in Section V, sub-section V.1.

16. However, their specific application and enforcement has been much less successful, and the new technological developments – ubiquitous, and more intrusive computing and personal data collection and use; "profiling"; ubiquitous internationalisation of such processing; user-generated web content; etc. – threaten to make the application of the principles yet more difficult, even on paper (although some new technologies can help in their application).

---

[3] For further discussion of the matters noted in this section, see Section V, below. For full detail (in particular also of the underlying analyses) and full references, see Working Paper No. 2: Data protection laws in the EU - The difficulties in meeting the challenges posed by global social and technical developments, submitted with this report. Note that this is a new, expanded version of the same paper submitted as part of the Interim Report.

[4] The COE Convention on data protection (CETS No. 108) and the EC Directive (Directive 95/46/EC) are undoubtedly the main inspiration for all European data protection laws, including the laws in aspirant-Member States and other countries such as Russia. For the Asia-Pacific region, see the comparative overview by Graham Greenleaf, Twenty-one years of Asia-Pacific data protection, Privacy Laws & Business International, Issue 101, October 2009, and in particular his comment that "*The influences on data protection principles [in the Asia-Pacific region] are principally the OECD Guidelines and the EU Directive, but the APEC Privacy Framework has not yet had any direct influence. The influence of the EU Directive is, if anything, strengthening over time.*" (Conclusions, p. 11). The law in Macau SAR, in particular, is being closely modelled on the Directive (via the Portuguese legislation), the Bill under consideration in China in 2006-7 was also strongly EU-influenced, as was the South-Korean legislation. Modest progress is also being made in the introduction of data protection in Africa, with help from the French data protection authority, the CNIL, in particular. Because of this help, the emerging laws in that continent, too, are clearly inspired by the European instruments. For argument that the new South-African Bill is designed to be compliant with the Directive, see the article by Iain Currie in Privacy Laws & Business International, Issue 101, October 2009. Mention should also be made of the recently-launched work by the International Conference of Data Protection and Privacy Commissioners to set global standards, based on the European ones, in the "Barcelona Initiative", and of the response by a broad coalition of civil society organisations in engaging with that initiative through their "Madrid Declaration", launched on 3 November 2009.

[5] See the *Country Report on the USA*, sections 2 and 4.

17. The following are the main areas posing challenges to EU data protection law, which are all further discussed in Section V (as indicated):

✓ Some matters are not subject to the Directive or the national laws implementing it; and these exclusions will become more problematic in the new "Web 2.0" environment in particular.

This is further discussed (with reference to Working Paper No. 2 in particular) in SectionV, sub-section V.2.

✓ There are still major conflicts of law, even within the EU/EEA, but especially in relation to controllers in non-EU/EEA countries; and these conflicts will grow strongly.

This is further discussed, again with reference to Working Paper No. 2 in particular, in Section V, sub-section V.3.

✓ There are still wide differences in the application and interpretation of even basic data protection concepts and rules, even within the EU/EEA, and wider differences still between EU/EEA and other countries; in a generally-internationalised world of data processing, these differences will be increasingly problematic.

These differences are partly due to inadequate or deficient implementation of the Directive by the Member States, and partly to differences in interpretation and application of the Directive. The mechanisms for ensuring full, and more harmonised implementation of the Directive have not been fully used. Specifically, in our view:

– The European Commission has not sufficiently forcefully pursued enforcement action against Member States that have not properly implemented the Directive; and

– The mechanisms in the Directive aimed at greater harmonisation have not been sufficiently used. To some extent, the procedures aimed at achieving greater harmonisation are also deficient in themselves, and need revision.

This is further discussed, with reference to both Working Paper No. 2 and to another Commission study, on the Article 29 Working Party, in Section V, sub-section V.4.

✓ The European Commission has used the procedure to issue "adequacy findings" in only a limited number of countries. Globally, the procedure has therefore had a more limited impact than could have been hoped for; and the development of strong data protection laws in non-EU/EEA countries has consequently been less strongly promoted than might have been the case.

This is further discussed in Section V, sub-section V.5.

✓ Even in the EU/EEA, enforcement by the national Data Protection Authorities (DPAs) is often not strong or comprehensive. With some notable exceptions (in particular, New Zealand and to some extent, for the private sector, South Korea), enforcement in most non-European countries, including the USA, is even weaker. Yet enforcement will

become both more important and more difficult in the new global-technical environment (although here too technology can sometimes be helpful).

This is further discussed in Section V, sub-section V.6, with reference, as far as the practices of the EU/EEA DPAs are concerned, to a study commissioned by the EU Fundamental Rights Agency, and as concerns enforcement outside the EU/EEA, to the Country Reports on non-EU/EEA countries.

✓ The assertion of data subject rights, either individually or with the help of NGOs, is often difficult and hampered by several matters, in Europe and elsewhere. However, some non-European countries, and in particular the USA, while generally providing less substantive data protection, do offer some special remedies, which could be used as examples to strengthen the powers of individuals in respect of their data in the EU/EEA.

This is further discussed in Section V, sub-section V.7.

✓ Supplementary and alternative means to enhance data protection, including technical means such as encryption, anonymisation, identity management tools and other (supposedly) Privacy-Enhancing Technologies (PETs), are still rather under-developed, often weak in their implementation and effect, and too often applied in a way that makes them ineffective. Some are little more than fig-leaves. Others (like anonymisation) are increasingly defeated by technological advances. They also often do not tackle the issues at the right moment, in particular the design stage, or are user-unfriendly. In the new technical environment, renewed - and more critical - attention will have to be given to these measures. Some relatively low-tech solutions, such as requiring the default settings for various applications to be strongly privacy-protective, or the issuing of privacy seals, can help to ensure adequate protection.

This is further discussed in Section V, sub-section V.8.

18. Any serious review of the European data protection regime will have to address all the above-mentioned problems - which are all greatly aggravated by the social and technical changes that await us (or are already upon us). The challenges are growing. However, as noted, they are mainly challenges to matters of application, interpretation and effectiveness of enforcement/assertion of rights: the basic data protection principles are not challenged, but rather, need reasserting and fuller, practical application.

- o – O – o -

IV. Fundamental imperatives

19. Certain matters are so fundamental that they must be taken into account in any review of the data protection regime in the EU: they cannot be ignored (or trivialised as "too legalistic") without endangering core European constitutional values. They are therefore briefly set out here, and inform all our specific conclusions and recommendations.

Socio-political imperatives:

20. New developments in information- and communication technology offer great benefits, but they also pose new threats to the individual and his/her relationship with powerful bodies (public and private). These include not just new threats to privacy in the traditional sense (freedom from intrusion and surveillance), but also new threats to personal autonomy and personal freedoms, including political freedoms - and indeed to society at large.

21. In traditional terms, it may suffice to quote the words of the German Constitutional Court in its famous 1983 *Census*-judgment:[6]

> A social and legal order in which the citizen can no longer know who knows what when about him and in which situation, is incompatible with the right to informational self-determination. A person who wonders whether unusual behaviour is noted each time and thereafter always kept on record, used or disseminated, will try not to come to attention in this way. A person who assumes, for instance, that participation in a meeting or citizen initiative is officially recorded, and may create risks for him, may well decide not to use the relevant fundamental rights ([as guaranteed in] Articles 8 and 9 of the Constitution). This would not only limit the possibilities for personal development of the individual, but also the common good, because self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizens.

The society that the social-technological developments noted in Working Paper No. 1 almost unthinkingly threaten to bring about, is no longer the "free and democratic society" envisaged in this quote.

22. But the new technologies bring further, newer threats: Increased, and increasingly automated analyses of ever-increasing, and ever-more-easily-accessible data carry the risk of individuals becoming mere objects, treated (and even discriminated against) on the basis of computer-generated "profiles", probabilities and predictions, with little or no possibility to counter the underlying algorithms. Unless strong data protection is maintained, decisions with "significant effect" (such as a decision to deny you a job, or to not even invite you for an interview; to be stopped at a border, and possibly denied entry into a country; to be subjected to intrusive surveillance, and possibly arrested, etc.) will increasingly be taken "because the computer said so" - without even the officials or staff carrying out the decision able to fully explain why. The new technologies inherently tend to shift the balance of power away from the individual towards those who hold data on them: the terms "data subject" and "controller" are gaining deeper, more sinister meaning. Some technologies can sometimes be used to counter some of this - but they are much weaker and often *inherently* less effective than

6 *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1 ff.

claimed or believed. Unless we tame the new technologies, their unimpeded use will undermine democratic society itself. And the tool to tame the machine in this respect is data protection.

Reference: For further detail, see Working Paper No. 1 (summarised at I, above and Section V, sub-section V.8, below.).

European constitutional-legal imperatives:

23. Data protection is increasingly recognised by the European Court of Human Rights in its case-law under Article 8 of the European Convention on Human Rights, and in EU law (in the latter case in particular through "general principles of Community Law", the Charter of Fundamental Rights, and the case-law of the European Court of Justice). The basic data protection principles and -rules therefore now have, effectively, constitutional status. In any revision of the EC Directive(s) on data protection, this should be kept fully in mind. If a revised Directive were to fall short of these fundamental requirements, it would invite judicial challenges and negative rulings in both Luxembourg and (as far as its implementation in and by the Member States is concerned) in Strasbourg. It should be a major aim of any revision of the main Directive, not to just avoid such violations, but indeed to make most certain that any new EU data protection regime - across what are now still three EU "pillars" - fully meets basic European human rights requirements.

Reference: For further detail, see Douwe Korff, *Paper No. 4: The Legal Framework*, in: Ian Brown & Douwe Korff, Privacy & Law Enforcement, study for the UK Information Commissioner, 2004 (included in the material submitted with this report).

24. Data protection has a strong constitutional basis in several EU Member States, including Denmark, Germany and Greece. Any failure of any EU data protection regime to meet the constitutional-legal requirements of those Member States is likely to cause serious tension between such national laws and EC/EU-law, as exemplified by the *solange* approach of the German Constitutional Court, recently reaffirmed in relation to Lisbon Treaty. The quotes below may illustrate this tension:

Quotes:

ECJ Stauder judgment:
(Case 29/69, *Stauder v. Ulm*, [1969], ECR 419, paras. 3-4)

Recourse to the legal rules or concepts of national law in order to judge the validity of measures adopted by the institutions of the Community would have an adverse effect on the uniformity and efficacy of Community law. The validity of such measures can only be judged in the light of Community law. In fact, the law stemming from the Treaty, an independent source of law, cannot because of its very nature be overridden by rules of national law, however framed, without being deprived of its character as Community law and without the legal basis of the Community itself being called in question. Therefore **the validity of a Community measure or its effect within a Member State cannot be affected by allegations that it runs counter to either fundamental rights as formulated by the constitution of that State or the principles of a national constitutional structure.**

continues overleaf

> *Cf., by contrast:*
>
> German Constitutional Court judgment on the constitutionality of the Lisbon Treaty:
> (German Constitutional Court Decision [BVerGE], 2BvE 2/08, of 30 June 2009, para. 240)
>
> **When legal protection is not ensured at the [European] Union level, the Constitutional Court judges [i.e., re-asserts for itself the power to judge - DK] whether legal acts of the European Organs and Institutions stay within the limits of the sovereign powers granted to them ...**

An important judgment from Romania, issued while this Final Report was in preparation, shows that the above tension is not limited to the "old" Member States: On 8 October 2009, the Romanian Constitutional Court ruled that a law which would have required mobile operators and internet service providers to store communication data for six months was unconstitutional.[7] The law was aimed at implementing the EC Data Retention Directive (Directive 2006/24/EC) and the ruling suggests that the requirements of that directive itself, too, violate the national-constitutional legal requirements of the country.

The above shows that, within the EU, data protection is eminently suited to resurrect the *solange* issues. It is therefore imperative that any revised EU data protection regime (especially if it were to apply in all the areas currently covered by all three "pillars") meets the requirements of the ECHR and of the constitutions of the Member States (including in particular, but not only, the requirements of the German Constitution in this respect, as developed by the Constitutional Court in that country).

References: For further detail, see in particular the *Country Report on Germany*, and the comparative analysis in Working Paper No. 2. See also para. 43, below.

25. In some of the non-EU/EEA countries considered, too, the constitutional basis of data protection can be potentially significant. This applies in particular to Japan and Hong Kong. However, in these countries data protection has not yet been fully developed within a more general constitutional protection of privacy. In Australia there is little if any constitutional basis for data protection. In other countries in Asia and the Pacific the position is similarly mixed. Across Asia and the Pacific there is therefore, for now, no comparable harmonising element to European human rights standards. In the USA, Federal Constitutional protection is largely limited to restraints on Government access to, and use of, personal information (and even then, largely only insofar as it relates to US citizens), and also often used to be trumped by the First Amendment (but see para. 34, below, for more recent developments). Although some States (such as New Jersey) have extended State Constitutional protection further, this is still far removed from the situation in European countries such as Germany.

References: For further detail, see the *Country Reports* on the above-mentioned non-EU countries.

---

[7] See: http://sofiaecho.com/2009/10/09/797385_romanian-constitutional-court-data-retention-law-unconstitutional.

V. Conclusions & Recommendations

1. BASIC APPROACH [expanding on the previous sections]

26. Any review of the EU data protection regime should start with explicit recognition of the need to meet the requirements of the ECHR and the Charter of Fundamental Rights, and of the constitutions of the Member States.[8] Meeting the socio-political and constitutional-legal imperatives in this respect (in all areas covered by the previous three pillars) will be all the more important in the new global socio-political and technical environment.

27. Data protection law in the EU (in all areas covered by the previous three pillars) can and should continue to rest on the basic data protection principles and –criteria set out in Directive 95/46/EC. The application of these broad standards needs to be clarified (as further discussed below, in particular in sub-section V.4), but they themselves do not require major revision in order to meet the new challenges. On the contrary, they reflect European and national constitutional/human rights standards of the kind just mentioned, that need to be strongly re-affirmed.

28. The focus of any review aimed at meeting the new challenges should be on the following (interrelated) matters, discussed in the sub-sections indicated:

- the problematic exclusions of certain matters from the scope of the Directive (V.2);
- the vexed question of "applicable law" (V.3);
- the need for much greater harmonisation (at a high level) within the EU/EEA, through various means including stronger enforcement action by the Commission (V.4);
- the need for more cooperation with non-EU countries, and greater recognition of "adequate" non-EU efforts (V.5);
- the need to ensure much greater compliance with and much stronger enforcement of existing law, at the domestic level, by the DPAs (V.6);
- the need to strengthen the rights and remedies for individuals (possibly acting with or through relevant NGOs) (V.7); and
- the need to further develop supplementary and alternative measures (while understanding the built-in limitations and practical restrictions of such measures) (V.8).

29. The second and third of these matters in particular are closely interrelated, in that the crucial question of "applicable law" (i.e., of ensuring that to any processing operation in the EU/EEA only one, readily-identifiable national law applies, and never no law) can only be resolved if much greater harmonisation is achieved in the application of the Directive. And overall, of course, there is no point in having strong data protection rules if they either do not apply to important activities, or are not properly or fully complied with and enforced.

Our conclusions and recommendations in these respects are set out below.

[8] With the entry into force of the Lisbon Treaty on 1 December 2009, the Charter became legally binding. Art. 8 recognises an autonomous right to the protection of personal data, and Article 16 TFEU provides for the adoption of a homogeneous legal framework implementing this fundamental right across all Union's activities, by the Union and its Member States. Moreover, the treaty abolished the previously separate three "pillars".

2. SCOPE OF THE EU DATA PROTECTION RULES

(i) Former First- and Third Pillar matters:

30. **Finding/Conclusion:** Activities in what before the coming into force of the Lisbon Treaty used to be the first and third "pillars" of the EU[9] are increasingly intertwined and becoming inseparable (cf., e.g., the SWIFT- and PNR controversies); to that extent the abolition of the different pillars is welcome. Moreover, the old third-pillar principle of "continued ownership" of data is unworkable in that it assumes the possibility for an originating country to really retain control over data passed on to authorities in another country. It is also incompatible with the also-used requirement of "availability" (enshrined in the Prüm Treaty) - which runs fundamentally counter to data protection principles.

31. We believe that the price for increased police and security cooperation must be guaranteed data protection, both within the Member States and in any EU institutions in this area, at the highest level required by any of the Member States' constitutions, and by European human rights law. Intra-EU cooperation on what used to be third-pillar matters is seriously threatened unless data protection is ensured (as in the old first pillar) at at least that level. Harmonisation of data protection in police matters should be based on COE Recommendation R(87)15, which is routinely invoked in EU (and COE) instruments on police cooperation such as the Schengen and Europol treaties (but without the implications being fully taken on board, or its principles adhered to in practice).

    Note: Some might argue that, beyond the question of whether national law properly implements European law, the level of national data protection is not a matter for EC or EU law. However, as explained in sub-sections V.3 and V.4, this argument could already not be sustained in the old first pillar, because of the close interplay between harmonisation and the question of "applicable law". If the Directive were to be extended to what used to be the third pillar, or if similar rules to the current "applicable law" rules in the Directive were otherwise to be applied to that area, the level of protection of police data in all EU/EEA countries would become a matter for urgent and pressing concern to countries with a high level of constitutional protection in this regard. They could not accept, in such a sensitive context, the application to their citizens of foreign laws that did not meet their own national constitutional requirements: see para. 24, above. In fact, the "availability" principle already raises these same concerns even if they have not yet been put before the courts.

32. The above requires strict legal rules, meeting the European "quality requirements" for "law" as spelled out by the European Court of Human Rights; limitations on "availability" and retention of data (including communications- and DNA data); and strict limitations on the use of "profiles"; as well as strong procedural protection, with full access for individuals affected by the relevant measures to the national and European courts, and full jurisdiction on the part of those courts to assess all the issues in each case on their merit.

    Reference: Working Paper No. 2, section 2, sub-section 2.1.

[9] See the previous footnote.

33. **Recommendation**: The basic data protection principles, rules and criteria enshrined in the Directive must be applied "seamlessly" to activities in all the areas previously covered by the different pillars. This includes the application of the (limited) exceptions for the old third-pillar activities listed in Article 13 of the Directive. If the challenges are to be met, there will have to be greater harmonisation, or at least approximation, of data protection rules covering those activities in the EU, based on COE Recommendation R(87)15. Also crucial is full judicial protection in the national courts, and through the ECJ, with data subjects having full standing (with the back-stop being the European Court of Human Rights).

(ii) Exceptions for purely personal processing and freedom of expression, in particular in relation to social networking sites and "blogging" on "Web 2.0":

34. **Finding/Conclusion:** User-generated content (UCG) will massively expand in the new online environment, in particular through SNS, "blogging", "twittering" and similar phenomena: there is a tsunami of currently not yet digitalised information waiting to hit the new "Web 2.0". This may well be dominated by UGC, or at the least UGC will be of equal importance to institutionally-generated content. The special exemptions in the Directive relating to "purely personal processing" and "freedom of expression" will be very difficult to apply to this phenomenon. In both respects, there is the danger, on the one hand, of exempting from the law, activities that directly impact on privacy and data protection; and on the other hand, of applying "heavy" rules, designed to regulate (presumably) well-organised institutions, to simple actions carried out by ordinary individuals as part of their everyday activities. This was in fact one of the criticisms of the ECJ's Linqvist judgment, which applied the full force of the main Directive to a small website of a local Swedish Church parish.

We should note that in non-EU/EEA countries with constitutional protection of competing rights such as privacy and free speech, the issues are much the same: the question of how to balance such rights is inevitable but has yet to be fully considered in most countries. In the USA, it used to be felt that the First Amendment to the Constitution (protecting free speech) usually trumped privacy, and various torts (civil wrongs) such as defamation and (wrongful) "public disclosure of private facts" have indeed been severely curtailed under the First Amendment. However, data-protection-like statutes such as credit reporting and financial services laws have more recently survived First Amendment scrutiny: see the Country Report on the USA, sections 1.5 and 1.6. While it is too early to speak of a convergence between the US- and EU approaches, these developments do mean that the differences have decreased.

References: Working Paper No. 1, section on *Social networking and user-generated content* (pp. 11-12); Working Paper No. 2, section 2, sub-section 2.2. Country Report on the USA, sections 1.5 and 1.6.

35. **Recommendation**: It should be possible to apply data protection rules more lightly to relatively trivial activities on the Internet. It is particularly problematic to try and subject ordinary, individual users of the Internet to the full force of the rules applicable to "controllers". We believe that the best way to address this problem is to regulate services that such ordinary users rely on: the social networking sites, the sites hosting "blogs", etc. In particular, such hosts should be made to provide default settings for their sites and services and tools that are privacy-friendly. Ordinary users that use such

sites without changing the default settings should have a reasonable expectation that they will not be violating data protection law; if the default settings fail to protect privacy and personal data, the site that chose those settings should carry the primary responsibility for this. This would leave open the possibility of adopting (or where they already exist, retaining) a tort [civil wrong or *faut*] regime under which individuals can be held liable for wrongful or unjustified public disclosure of private information or "intrusion" over the Internet or through other ubiquitous communication systems such as SMS or MMS. Such systems operate reasonably well in the USA (subject to First Amendment questions, as noted earlier) and have recently arisen through case-law in New Zealand; they are recommended by law reform commissions in Australia and Hong Kong. Such systems could be reinforced by possibilities to obtain temporary injunctions from the courts, or orders from the DPAs, requiring take-down of UGC which the data subject or the DPA feels breaches the law, which could be challenged by the poster on the grounds that the posting did not violate the law. We believe that in many EU Member States, solutions on these lines are already possible (partly on the basis of civil law, partly - in particular in respect of the default settings of SNSs - on the basis of data protection law).

References: Country Reports on Australia and Hong Kong, sections 1.7 in each, and on the USA, sections 1.5 and 1.6.

3. APPLICABLE LAW

36. **Finding/Conclusion:** All data processing, including the processing of personal data, is becoming increasingly internationalised. This is inherent in activities on the Internet, and will be all the more so in an era of "cloud computing". The actors involved in such processing are also becoming increasingly diversified and split between countries, with often not-easy-to-distinguish tasks and responsibilities. This will cause increasing conflicts of law, also within the EU/EEA, because of the ambiguity and different implementation of the "applicable law" rules in the Directive.

37. Specifically, under the main Directive, within the EU/EEA, Member States must apply their national data protection law to a processing operation if "*the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State*"; but "*when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable*." (Article 4(1)(a) of the main Directive). This means that the question of what law applies to a particular operation depends first of all on: (i) who the "controller" is (which is often not easy to determine, and will become more difficult to determine in the new global-technical environment described in Working Paper No. 1); (ii) where the controller is "established" (and the question of "establishment" is far from easy to answer under Community law generally); (iii) what the "context" is within which the processing takes place; and (iv) which is the "establishment" of the controller concerned (which is often difficult to determine precisely) - and all that does not yet even take into account the second sub-clause, about controllers "*established on the territory of several Member States*". The rules in Article 4(1)(a) are quite simply utterly confused and impossible to apply in the new global-technical environment. Not surprisingly, the rules are applied differently in the Member States, leading to conflicts of law (which are only not too serious in practice because the competing and conflicting laws on paper are often not enforced in practice).

Reference: D Korff, EC Study on Implementation of Data Protection Directive 95/46/EC, 2002, section 4, "applicable law", which concluded (on the basis of more detailed analysis in the report on that study) that:

> There are ... serious problems with the implementation of the first main rule in the Directive, that "*each Member State shall apply [their national law] to the processing of personal data where ... the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State.*" This rule is not fully or properly - and especially not consistently - applied in all the Member States, which results in the very kinds of conflicts [of law] that Art. 4 of the Directive seeks to avoid. Partly, this is the result of deficient transposition of Art. 4 of the Directive; but partly, it is caused by the excessive complexity of that provision itself."

38. Further study is also required of the application of these rules to public bodies and, especially, semi-public bodies that are increasingly involved in the processing of personal data in the Member States, including in such sensitive areas as health and criminal justice.

39. The rules in the Directive on applicable law are also effectively impossible to apply to non-EU/EEA companies and organisations that are active in Europe - especially if they are active on the Internet (as they almost all are, and certainly will be). On their face, they often require all such companies and organisations to conform to all the data protection laws, of all the 27 Member States, simultaneously - which is impossible, given the still remaining major differences between the laws and the difficulty of even knowing what they each require in relation to processing by non-EU/EEA-established companies on the Internet.

40. The rules on "applicable law" in relation to non-EU/EEA countries with "adequate" data protection are also unclear.[10] Specifically, the Directive does not clarify whether, for "applicable law" purposes, they should be treated in the same way as EU/EEA countries, or as non-EU/EEA countries.

41. In the countries studied outside the EU, (which are all "*in*adequate" in EU terms) the question of "applicable law" is seen as part the question of the extra-territorial scope of the national data protection laws. This question remains unsettled in some jurisdictions, but is the subject of a specific provision in the Australian legislation, although the scope of that provision is also open to interpretation.

Reference: Country Report on Australia, section 2.5

42. All these problems are serious and hamper internationally operating companies and organisations, making it more difficult for them to comply with data protection rules and principles. These problems are greatly enhanced in the new, generally internationalised socio-technical environment, and in relation to the Internet in particular (but not only).

Reference: Working Paper No. 2, section 3.

43. A further crucial issue is the nexus between the rules on "applicable law" and harmonisation, in the light of the national-constitutional requirements of several

[10] The question of the use of "adequacy" findings as such is discussed in sub-section V.8, below.

Member States (as noted in para. 24, above). Clearly, under the "applicable law" rules, processing in one Member State, and on individuals in that Member State, will at times already - and in the new socio-technical global environment will often - be subject to the data protection law of another Member State. However, if the applicable "foreign" law were to fail to meet the constitutional requirements of the State where those individuals are, this would raise further *solange*-type problems: the chances are that the constitutional court of the State in question would refuse to apply the foreign law to the extent that it failed to meet the requirements of the State in question, even if that meant, in effect, refusing to apply the European "applicable law" rules. In other words, in such a constitutionally-sensitive matter as processing of personal data, "applicable law" rules that by-pass the laws of a State whose citizens are the subject of the processing can only be accepted if they are twinned with rules that ensure that all the national rules, in all Member States, meet the highest domestic-constitutional requirements of any Member State.

44. **Recommendation:** Better, clearer and unambiguous rules are desperately needed on applicable law. We would tentatively suggest rules on the following lines:

– Within the EU/EEA, the rules should, in our opinion, simply be based on the "country of origin" principle, as originally intended. This may not resolve all issues: we realise that questions such as "establishment" are difficult in a wider EC context, too. But it would at least reduce the problems, and synchronise them in different Community law contexts. However, as explained in para. 43, above, it is an essential prerequisite for this that there is greater harmonisation, or at least approximation at a high level, between the laws of the Member States. This harmonisation is currently still absent in many crucial respects: see sub-section V.4, below, at A. The basic tools exist to achieve (or at least encourage) greater harmonisation (especially in the form of the Article 29 Working Party), but they are not effectively used at present and need strengthening (see sub-section V.4, below, at B).

– Non-EU/EEA companies etc. with a presence (i.e., that are "established") in the EU/EEA should be able to comply only with the law of their EU/EEA country of main establishment (their European HQ), and should otherwise be treated as EU/EEA companies (provided they also comply with the EU/EEA rules on transfers of data to third countries without adequate protection, and will thus treat personal data sent to their third-country [global] HQ still in accordance with EU/EEA data protection law).

Note: This is in line with general Community law, under which non-EU companies established in the EU are treated as EU companies.

– The rules on "applicable law" in relation to non-EU/EEA companies etc. without a presence in the EU/EEA but that use "means" in the EU/EEA (typically, non-EU/EEA companies that offer products or services to EU/EEA citizens and -companies over the Internet, without having an establishment in the EU/EEA) should be simplified, so that they too can adhere to the law in one (relevant) EU/EEA country only. Consideration could be given to making this choice of law possible within such a company's Binding Corporate Rules; the appropriateness of the choice of law would be one of the issues to be assessed in judging the adequacy and appropriateness of the BCRs.

– Subject to the first note, below, non-EU/EEA companies etc. that are subject to an "adequate" law in their country (as determined by the Commission) should be treated on

a par with EU/EEA companies, i.e., they should only have to comply with their own ("adequate") law - provided the States concerned also comply with the measures taken in the EU/EEA to ensure ongoing harmonised/approximated application of the law (as again also further discussed in sub-section V.4, below).

Notes:

(1) The latter suggestion may require granting a say to the non-EU/EEA countries concerned, e.g., in the form of full or partial membership of, or observer status on, the WP29, and regular reviews of continued "adequacy".

(2) The possibility of non-EU/EEA countries becoming parties to Council of Europe Convention No. 108 and its Optional Protocol must also be borne in mind. This would be particularly interesting if a finding could be issued to the effect that States that are party to that Convention and Protocol *ipso facto* will be deemed to provide "adequate" protection. However, there are still issues to be resolved in that respect.

(3) In the last tentative suggestion, it is also assumed that the "adequate" laws apply extra-territorially to the relevant non-EU/EEA companies, in particular in respect of its operations in the EU/EEA. This may not necessarily be the case, if the example of Australia (extra-territorial effect limited to data on Australian citizens) is common. On the other hand, the example of Japan (extra-territorial effect applies to any company with a presence in Japan) will fit this criterion. This of course merely serves to highlight to intricate problems in this area. It is certainly an issue that the Commission (and the WP29) should take into account in future considerations of laws in non-EU/EEA countries.

References: Country Reports on Australia and Japan, section 2.5 in each case.

We realise that these are very complex issues, and the above are merely suggestions for debate. However, we do feel that this is one of the most important issues: the current rules on "applicable law" are impossible to fully understand or comply with. In an increasingly globalised environment, with "cloud computing", clarification - and simplification - in this respect is urgently needed.

4. HARMONISATION OF SUBSTANTIVE LAW

45. In this sub-section, we will first, briefly, set out, at A (paras. 47 – 78), our findings and conclusions on some major issues on which harmonisation is still lacking even within the EU/EEA. We then briefly note, at B (paras. 79 – 88) that the issues are not much clearer in non-EU/EEA countries. We will only then, at C (paras. 89 – 96), make recommendations on the ways in which such harmonisation could be achieved in all these regards (and others). We should stress that the aim of the brief summaries is not to be comprehensive, but rather, to show that there are still major divergences, both within the EU/EEA and between the EU/EEA and other countries, that need to be addressed if data protection is to be properly ensured in the new global-technical environment.

Note: This sub-section must of necessity be brief, and cannot do justice to the complexities of the matter. For that, we refer to the more extensive entries in section 4 of Working paper No. 2. For yet further detail, see the Comparative Summary of National Laws, written for the Commission by Douwe Korff in 2002 and published by the Commission in 2003.[11] See also the Comparative Chart, attached to this report.

[11] Douwe Korff, Study on Implementation of Data Protection Directive 95/46/EC - Comparative Summary of National Laws, 2003, available from http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm. In

46. Before discussing the specific issues, we may note that one could argue that, up to a point, a straight-forward regime on "applicable law" could also address the many major divergences: it would allow countries to go their own way, up to a point. However, as noted in Section IV, at para. 24, and above, at para. 43, at least within the EU/EEA, this would very quickly lead to conflicts between national-constitutional and EU law, and re-open the *solange* problems. Significantly divergent non-EU laws could also not be accepted as "adequate" by the EU or the Member States. We therefore believe that "approximation" of national laws is required, at a level that would at least clearly meet the requirements of the most demanding constitutions (including, but not at limited to Germany) and of the ECHR. We are convinced that failure to do this will lead to major problems in terms of national and European human rights law, and indeed in terms of the validity and supremacy (or primacy) of EC/EU law. Harmonisation, at least within the EU/EEA, is a central requirement to meet the new challenges. Our conclusions in respect of inadequate harmonisation are therefore serious: this is one of the major challenges that should be addressed in any review of the EU/EEA data protection regime.

A. (NON-) HARMONISATION WITHIN THE EU/EEA

(i) Core concepts and definitions (Article 2 of the Directive)

47. **Finding/Conclusion:** The definitions of many core concepts in the Directive still leave many crucial questions unanswered.[12] Thus, for example, in respect of the concepts of "personal data" and "data subject", important questions remain about anonymisation and pseudonymisation, re-identifiability, data on "things" that are linked to people (like IP addresses and traffic and location data), and "profiling". National laws and practices still give widely differing answers to these questions. Although some useful guidance has been given, in relation to these issues, by the WP29 in its Opinion on the concept of personal data,[13] we fear that these questions are still inadequately dealt with at both EU- and national level, and do not take into account the serious problems with re-identification which have been well known (to computer experts at least) for some years.[14] The serious problems stemming from the near-impossibility of full anonymisation of personal data in the new socio-technical global environment pose some of the most crucial challenges to data protection, and should be at the heart of any debate on a review of the European data protection regime.

48. In addition, in some respects, the very definitions of "controller" and "processor" (and thus of "third party" and "recipient") in the main directive are confusing, and in

---

some respects the 2003 summary is now somewhat out of date. Where relevant, we have updated matters in the Working Paper No. 2 in the light of information from the experts involved in the current study. In that Working Paper, we have also addressed one special issue that cuts across many aspects of data protection, and that is central to the new environment, but that is not further discussed here: "profiling".

[12] Apart from the concepts mentioned in the text, it may be noted that it is also unclear what kinds of "unstructured" manual files fall within the concept of "personal data filing system", and what kinds do not. However, except for very special cases, this is less important in the digital era. The question of what constitutes (valid) consent is discussed in paragraph iii, below.

[13] Opinion 4/2007 on the concept of personal data of 20 June 2007 (WP136), discussed at some length in Working Paper No. 2, section 4.1.

[14] See in particular the (for non-computer experts) seminal paper by Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, Colorado Law, Legal Studies Research Paper Series, Working Paper Number 09-12, August 13, 2009, available online from: http://ssrn.com/abstract=1450006. Comments based on this paper have been added to Working Paper No. 2.

practice, it is often difficult to discern exactly who is a controller and who a processor (or a third party, or a non-third-party recipient),in particular in complex international organisations such as multinational companies or groups of companies. The laws in the Member States moreover diverge in these respects too. This issue too will become much more important in the new, complex global-technical environment; it has important implications in terms of "applicable law" in particular - yet in this respect, there is much less clear guidance, and confusion remains.[15]

Reference: Working Paper No. 2, section 4.1.

(ii) The data protection principles (Article 6 of the Directive)

49. **Finding/Conclusion:** The data protection principles are contained in the laws of all the Member States, with a few exceptions in terms identical to or close to those used in the Directive. However, a few laws use somewhat varying terms; one sets out the data protection criteria (discussed below, at iii) in the middle of the principles; and one adds further principles. In addition, some countries add clarification or gloss to the principles, in ways which sometimes strengthen them but sometimes do the opposite.

50. The purpose-specification and –limitation principle is set out in terms identical or very similar to the ones used in the Directive in the laws of most of the Member States. However, in spite of the similar wording, the very vagueness of the principle leaves it open to divergent application, and different Member States apply different tests in this regard, ranging from the"reasonable expectations" of the data subject, to "fairness" or the application of various "balance" tests. In a few countries, the principle is subject to quite sweeping exemptions, in particular for public-sector controllers. In others, purposes are sometimes defined in excessively broad terms, thus undermining the principle itself. For instance, UK law refers to "policing purposes" in one breath (and thus allows data obtained for one police purpose to be used for any such purpose), where German law strictly distinguishes between "countering immediate threats", "general and specific prevention", and "investigation and prosecution of [suspected] criminal offences".[16] More blatantly in violation of the Directive, the UK Data Protection Act adds "medical research" to the list of medical purposes set out in Article 8(3) of the Directive, thus circumventing purpose-limitation in that regard (contrary to the clear guidance on this from the WP29).[17]

51. The rules concerning secondary processing of non-sensitive personal data for research purposes without the consent of the data subjects also otherwise vary very considerably. Some Member States fail to provide any safeguards (in manifest breach of the Directive); some lay down minimal (i.e., insufficient) safeguards (e.g. that the data may

---

[15] The difficulty of identifying, in certain complex cases, who is the controller and who a processor, was noted at the recent conference of data protection authorities in Barcelona, in January 2009, where it was suggested that sometimes it could be accepted that the relative roles and responsibilities are mixed, or shared. However, this did not take into account the implications and complications of such an approach for the question of "applicable law".

[16] See Douwe Korff, The feasibility of a seamless system of data protection rules for the European Union, Study for the European Commission (1996 – 97, published 1999).

[17] See the WP29 "Working Document on the processing of personal data relating to health in electronic health records (EHR)", WP131 of 15 February 2007. Note: The implications of ill-defined purposes in legal rules, and of seeking "consent" for processing for insufficiently-defined purposes, are discussed at iv. The multiple ramifications of the need to narrowly define purposes in itself underlines the importance of further guidance and harmonisation in this regard.

not be used to take decisions on the data subjects, or may only be used for the research in question); and some lay down rather abstract "balance" tests or only say that the research must be based on an "appropriate research plan". On the other hand, the laws in some countries provide for detailed rules which limit the data and the processing and stipulate that the research must be approved by an academic "ethics committee", or require researchers to apply for a special authorisation from the Data Protection Authority, which is to stipulate various conditions (or these additional conditions may be spelled out in the law already).

Reference: Working Paper No. 2, section 4.2.

(iii) The data protection criteria (Article 7 of the Directive)

processing on the basis of statutory authorisation[18]

52. **Finding/Conclusion:** Many national laws repeat the criteria relating to legal obligations, tasks and powers in terms identical to, or very similar to the ones used in the Directive. Two general, fundamental points need to be made. First of all, these criteria generally relate to processing on the basis of some form of statutory authorisation:[19]in terms of the ECHR, they relate to processing of personal data (which, in terms of the Convention, *ipso facto* constitutes an "interference" with private life) that is provided for by "law". Secondly, the criteria contain the other key term used in Article 8 ECHR, "necessary". This means that the legal rules on which the processing is based must meet the detailed requirements of "law" and "necessity" (including specificity and proportionality) that the European Court of Human Rights has elaborated in extensive case-law.[20] In the last few years, the European Court of Human Rights has, on several occasions, ruled that national laws allowing for the processing of personal

[18] This phrase is used here to cover the two criteria contained in paras. (c) and (e) of Article 7 of the Directive, i.e.: "processing [that] is necessary for compliance with a legal obligation to which the controller is subject" and "processing [that] is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed". Specifically, we may note that the "legal obligations" referred to in Article 7(c) are not those derived from a contract or pre-contractual situation, since these are covered by Article 7(b); and that the "tasks" and "authority" referred to in Article 7(e) will be tasks and powers granted by law.

[19] See the previous footnote.

[20] For further detail, see Douwe Korff, *Paper No. 4: The Legal Framework*, in: Ian Brown & Douwe Korff, Privacy & Law Enforcement, study for the Information Commissioner, 2004, from the UK ICO website: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/legal_framework.pdf. For an overview of the ECHR requirements in relation to "law", "legitimate aim" (purpose), "necessity", etc., see pp. 9 – 15. The paper goes on to summarise in some detail the ECtHR cases of Amann v. Switzerland (Judgment of 16 February 2000) and Rotaru v. Romania (Judgment of 4 May 2000), with shorter references to the earlier cases of Leander v. Sweden (26 March 1987), Gaskin v. the UK (Judgment of 7 July 1989), Peck v. the UK (28 January 2003), and others (pp. 16 – 33); as well as the ECJ cases of Österreichischer Rundfunk v. Austria (Joined Cases C-465/00 (Rechnungshof v. ÖRF et al.), C-138/01 and C-139/01 (respectively, Christa Neukomm and Lauermann v. ÖRF) (references for preliminary rulings from the Austrian Verfassungsgerichtshof and Oberster Gerichtshof respectively), Opinion of Advocate-General Tizzano of 14 November 2002; Judgment of 20 May 2003) and Lindqvist v. Sweden (Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping (Reference for a preliminary ruling from the Göta Hovrätt), Opinion of Advocate-General Tizzano of 19 September 2002; Judgment of 6 November 2003) (pp. 33 – 44). For a briefer overview, see Douwe Korff, The need to apply UK data protection law in accordance with European law, Data Protection Law & Practice, May 2008. Some more recent ECtHR cases are noted in the next footnote. They confirm the approach of the Strasbourg Court in the cases mentioned above, and if anything strengthen the case-law further. A further seminal judgment, issued after the 2004 ICO study, is I. v. Finland (Judgment of 17 July 2008): this case has major repercussions for the processing of health data in Electronic Patient Records in Europe.

data did not meet these quality requirements. These cases also raised doubt about whether the purpose(s) for which the personal data were being processed was (were) defined in sufficiently precise terms.[21]

53. It is clear that in several Member States, legal rules that are relied on to allow processing (and sharing, and "data mining") of personal data, especially in the public and quasi-public sectors, do not meet these standards. This will cause problems in purely domestic terms, but also (and of more importance to this study) in relation to other States, and the EC/EU, if such deficient laws were to apply extraterritorially as a result of the "applicable law" rules. This is certain to become much more common in the new internationalised environment, in which data processing will increasingly become subject to national laws of other countries than the place where the data subject is resident (or where he or she happens to be when the data were obtained).

Reference: Working Paper No. 2, section 4.3 (under this heading).

processing on the basis of consent

54. **Finding/Conclusion:** In terms of "informational self-determination", processing on the basis of consent is clearly crucially important, but with the *caveat* that (as it is put in Article 7(a) of the Directive) such consent must be "free, specific and informed". Yet again, in spite of this being such a core issue, the matter is not dealt with uniformly in the Member States. Thus, Several laws emphasise the need for any consent to be *manifestly* free, specific and informed etc., by including the term "unambiguous " in the very definition of consent (Portugal, Spain, Sweden); the Luxembourg law even includes both the term "unambiguous" and the term "explicit" in the definition. The laws in Germany and Italy stipulate that consent should (in principle) be in writing (while allowing for the giving of consent on the Internet by means of a "mouse-click"). By contrast, guidance on the law, issued by the UK data protection authority, suggests that consent for the processing of non-sensitive data can often be implied.

55. In Germany, a request for consent for a separate purpose than the primary purpose must be specially emphasised in printed forms etc. – but in that country (and elsewhere), there is some lack of clarity as to whether the granting of one's consent to such secondary processing, unnecessary for the primary purpose of an agreement, may be made a condition for the entering into of the primary agreement: under the previous law in the UK this was lawful, unless there was some abuse, but the Irish data protection authority is stricter in this regard.

56. All these divergences will yet again become more problematic in the new, generally-internationalised environment, including the Internet. "Consent" obtained under the law of one country - the "applicable law" at the time of data collection - and valid under that law, may well be regarded as insufficient and invalid if relied on for subsequent processing in another country (even another EU/EEA Member State), e.g., because (in the view of the second country) the original consent was insufficiently specific, or obtained under what the second country regards as duress, etc.

57. All this is without even considering the more general, fundamental questions of the validity of consent obtained on the basis of small print in online Privacy Statements that

[21] See, e.g., Copland v. the UK, ECtHR judgment of 3 April 2007; S. & Marper v. the UK, ECtHR GC judgment of 4 December 2008 (both confirming earlier case-law).

are read by no-one (except privacy activists or lawyers). Suffice it to note, first of all, that yet again Member States may differ in how they deal with such "consent", and there is as yet no clear guidance on this from the WP29; and secondly, that the issue will often touch on wider legal issues such as consumer protection, unenforceability of certain standard Terms & Conditions, unfair competition, etc.

Reference: Working Paper No. 2, section 4.3 (under this heading). See there also for references to the obtaining of consent by minors, and on WP29 guidance on consent in the contexts of transborder data flows, employment, schools, and medical care.

processing on the basis of the "balance" criterion

58. **Finding/Conclusion:** The "balance" criterion (Article 7(f) of the Directive) is, by its nature, the vaguest and most open-ended of the criteria, and thus the one perhaps most in need of clarification as to how it can and should be applied in specific contexts. This is recognised in the laws of several countries (Belgium, Ireland, UK), which envisage the issuing of further rules on the application of the "balance" criterion in specific contexts. However, remarkably, none of these have actually issued such more precise rules.

59. Overall, there are also notable differences in approach to this criterion in the Member States. In the UK, it is largely left to controllers to determine for themselves whether they can process non-sensitive data on this basis. In Germany, a "balance" test expressed in the kind of general terms used in the Directive applies only to the private sector. Somewhat similar, but more precisely-worded tests apply in the public sector, but these in fact get closer to the application of a "necessity" test. Other countries generally apply more-strictly-phrased test, or impose strict procedural requirements on processing on the basis of this criterion. Thus, in Greece, the law tilts the "balance" strongly towards the data subject by allowing processing only if "the processing is *absolutely* necessary for the purposes of a legitimate interest pursued by the controller or a third party or third parties to whom the data are communicated and on condition that such a legitimate interest *evidently* prevails over the rights and interests of [the data subjects] and that their fundamental freedoms are not affected."

60. In Italy, the "balance" test only applies in cases specified by the Data Protection Authority, while under the Finnish law, controllers need to obtain a permit from the Authority if they wish to rely on that test (but the law also contains four special provisions allowing for processing in certain circumstances, such as a customer relationship, which can be said to be specific examples of the application of that test).

61. These divergences can again cause problems in the new, generally-internationalised environment, if data are obtained on the basis of this criterion in one Member State, and then transferred to another, in which the criterion is more restrictively applied - or indeed, if a controller in one country, which is relatively lax in its application of the criterion, tries to obtain data directly from data subjects (e.g., over the Internet, or by 'phone) on this basis, under the controller's national law (which would normally be the "applicable law"), when the data subjects are in fact in another Member State with a stricter law in this respect.

Reference: Working Paper No. 2 (extended version), section 4.3 (under this heading).

(iv) Processing of sensitive data

62. **A preliminary remark:** Processing of sensitive data will become much more widespread, and even more difficult to control, in the new global-technical environment: pictures and video clips uploaded to social networking sites, comments on "blogs" and in "twitters", all routinely "reveal" sensitive matters such as ethnicity, sexual orientation or religious beliefs (or even criminal matters). And they are all-too-easily disseminated to many people, also across national borders. As already noted, even determining the "applicable law" to such processing is difficult. Conflicts of law are therefore particularly problematic in this respect.

63. **Finding/Conclusion:** Some Member States extend the special conditions (technically, in the Directive and in the laws of the Member States, exceptions to an in-principle prohibition on the processing of such data) to certain data not included in the list in the Directive. This concerns data on debts, financial standing and the payment of welfare (social security) benefits in particular. Some States also include data on criminal convictions etc. in the general list of sensitive data - which means that such data can be processed on the basis of the same exceptions (special criteria) as the other sensitive data (and in particular also on the basis of consent, which is not mentioned in Article 8(5) of the Directive).

64. Apart from this, it may suffice to note the rules on the processing of sensitive data in some special contexts:

Employment: Although the laws in several of the Member States contain general provisions concerning the processing of sensitive data to meet the requirements of employment law, on the lines of the Directive, these laws provide little specific detail in this regard. Some envisage the adoption of special rules (or a special law), but in most this has not yet been done. Overall, the situation in this regard is still very much determined by separate – and widely divergent - provisions in other laws than in the data protection laws implementing the Directive, without the data protection laws, or more specific rules issued under the data protection laws (as yet) providing much guidance in this respect.[22]

65. The WP29 has issued one general opinion on the processing of personal data in the employment context; a recommendation on employment evaluation data; and a working document on surveillance of electronic communications in the workplace; also relevant is its opinion on email screening services.[23] However, to date, these have not led to any major convergence (let alone harmonisation) in this respect.

66. Substantial public interest: Several of the data protection laws of the Member States envisage the issuing of decrees or other subsidiary rules concerning the processing of sensitive data for important public interests - but this has only been done in a very few

[22] This is also confirmed by a recent study commissioned by the EU Fundamental Rights Agency: see the Executive Summary of the final draft of the Comparative Legal Study on assessment of data protection measures and relevant institutions, report commissioned by the Fundamental Rights Agency (FRA) of the European Union (2009), para. 8.

[23] These are, respectively: Opinion 8/2001 on the processing of personal data in the employment context (WP48 of 13 September 2001); Recommendation 1/2001 on Employee Evaluation Data (WP42 of 22 March 2001); Working document on the surveillance of electronic communications in the workplace (WP55 of 29 May 2002); and Opinion 2/2006 on privacy issues related to the provision of email screening services (WP118 of 21 February 2006).

Member States (in particular, the UK and France), and in the rules in question, at least in the UK, the standards are somewhat ambiguous.

67. Several laws similarly allow for the issuing by the national Data Protection Authority of specific *ad hoc* authorisations- but as far as we know the Commission has not been notified of any (as it should have been under Article 8(6) of the Directive). One Member State (Belgium) provides for the issuing of permits to human rights organisations, allowing them to process sensitive data without consent (See Art. 6 § 2(k) of the Belgian Data Protection Law), but this is in itself controversial and may contravene the European Convention on Human Rights; to the best of our knowledge, no such permits have been applied for, at least not by the major international human rights organisations.

68. It should be noted in this context, however, that several of the data protection laws in the Member States quite generally defer to any other domestic laws or –rules -and many of these do authorise the processing of sensitive data. It is a moot question whether these other laws contain the "suitable safeguards" that should be provided in this respect, according to Article 8(4) of the Directive. Such other laws or provisions should have been notified to the Commission, but this does not appear to have been done to any great degree. This area therefore remains rather obscure, but it is clear that in many countries, in many respects, there must be serious doubts as to whether the rules comply with the Directive in this regard. What is more, it is also clear that given that these matters are regulated in so many disparate laws (mostly not drafted to deal with data protection at all), major differences remain between the Member States.

69. Once again, this would have serious implications if such laws were to be relied on in circumstances in which the relevant national law was the "applicable law" in a transnational context. Until recently, this was perhaps not so urgent, since many matters of "substantial public interest" were dealt with entirely within the domestic legal framework, and related only to the State's own citizens and residents. However, the ever-increasing cooperation within the EU, also on matters such as health, welfare, migration, etc., means that there will also be increasing transnational (European-level) arrangements, and corresponding data flows, that will come under data protection law.

70. Guidance, in particular on what would be "suitable safeguards" in this regard, is therefore urgently needed to facilitate (upward) approximation of the data protection guarantees in these respects.

71. Criminal convictions: The laws in the Member States differ substantially with regard to their approach to the processing of data on criminal convictions etc. Some include such data in the general category of "sensitive data" (which can have repercussions, in particular as concerns the permissibility of such processing with the consent of the data subject), while others extend more special rules on criminal convictions to data on other legal disputes or to data on "serious social problems" or "purely private matters". The laws also apply quite different standards to the processing of such data. Some permit any processing of such data if it is "authorised by or under any legal provision", or for any "purpose specified by law"; or allow it on the basis of vague and subjective "balance" tests; while others lay down strict "necessity" tests and\or require that controllers (especially in the private sector) obtain special permits or authorisations. There are therefore still clearly substantial differences between the laws of the Member States in this respect.

72. National Identity Number; There are different basic approaches to the use of national identity numbers and similar general identifiers, with some Member States allowing for the widespread exchange of such a number between public administrations if this facilitates their work, and others taking a restrictive approach, under which the use of such numbers is (to be) regulated more precisely. Some countries allow the use of such a number in the private sector with the consent of the data subjects, while others are again more restrictive, fearing in particular that the use of such a number can too easily lead to interconnections of databases and unchecked disclosures of data.[24]

Reference: Working Paper No. 2 (extended version), section 4.4

(v) The rules on transborder data flows

73. **Finding/Conclusion:** The Directive deals with two types of transborder data flows: data flows within the EU/EEA, and transfers of data to non-EU/EEA (so-called "third") countries, and in the latter case further distinguishes between third countries with, and without "adequate" data protection. The basic rules are (or were) straight-forward: within the EU/EEA, and within what used to be the first pillar, data flows should be unrestricted. However, that pillar has now been abolished, and the matter is consequently no longer simple, as noted below.. Data may also be freely transferred to third countries with adequate protection (if they are adequate in some respects, but not in others, provided the data fall within the adequately protected area) (Article 25(1)). And data may in principle not be transferred to third countries without adequate data protection (or to countries that are adequate in some respects, but not in others, if the data fall within the not-adequately protected area), unless a special condition is met (Article 26(1)).

74. Once again, however, these rules are not uniformly applied. First of all, only a few States expressly provide for the free transfers of data within the EU/EEA; most imply this (by only imposing explicit restrictions on transfers to third countries) but do not spell it out. Of the few States that do stipulate this freedom, moreover, only one (Austria) makes clear that that freedom only applies with regard to processing within the scope of the Directive. This is of course essential, since there is no guarantee that processing that is outside the scope of the Directive - in particular, in the former Third Pillar - is subject to adequate data protection (cf. Article 3(2), first indent, of the Directive). The uncritical application of the "free data zone"-rule in Article 1(2) of the Directive, so that it also places no obstacles in the way of trasnfers of data within what used to be the Third-Pillar within the EU, is thus highly problematic and certain to lead to violations of data protection standards. Of course, formally, now that the Lisbon Treaty has come into effect, the three-pillar structure of the EU has been abolished. However, it is crucial that, in this new situation even more than before, full and appropriate data protection is going to be ensured throughout all matters previously in the different pillars (as discussed above, at 5.02(i)) - only then can a rule be adopted on the lines of Article 1(2), applicable to all data transfers within the EU/EEA, unlimited to matters within the scope of Community law. If the challenges of the new global-technical environment are to be met, that should happen sooner rather than later.

---

24 In the UK, there is (as yet) no official national identity number, although this would be created if the National Identity Register is established in relation to the creation of National Identity Cards. However, other widespread identifiers, such as the National Insurance Number, National Health Service Number and Driver License details are widely used, by both the public and private sector, with few restrictions.

75. As concerns transfers of data to countries with "adequate" data protection, the main difference - but an important one - concerns the situation pending a formal finding of "adequacy" by the Commission. In Austria, Greece, Luxembourg, Portugal and Spain the law makes clear that in the absence of a Commission finding of "adequacy", only the national authorities can determine that a particular third country provides "adequate" protection. In other words, until and unless such a domestic (or European) finding has been made with regard to a particular "third country", transfers of personal data to that country are subject to the in-principle prohibition. In some countries, like the UK, the assessment pending a Commission "finding" is left to controllers. This reflects a generally relaxed, limited-interference approach by the authorities there.[25] This would appear to be out of line with the views of the WP29. The WP acknowledges that "[t]he directive does not specify ... whether an authority should be charged with assessing the adequacy of data protection in third countries", but concludes from this that it is therefore at least "possible that national legislation in Member States endows this task on national data protection authorities, whose authorisation may be required for the transfer of personal data to a third country to take place." Indeed, from the next paragraph, the WP would appear to feel that these are the only two real options:[26]

> Beside this possibility for national authorities to assess adequacy as allowed by national legislation, the Directive provides for Europe-wide decisions on adequacy to be adopted by the Commission, thus providing an added value of legal certainty and uniformity throughout the Community ...

76. The problem is that if one combines the basic "free transfers within the EU/EEA"-rule with the lax position in the UK (and some other countries), the strict rules in the first category of countries can be easily circumvented: the data protection authorities in these countries cannot (in terms of the Directive) stop transfers of personal data to the Member States with less strict rules, and the data can then be transferred from those other Member States to third countries in respect of which there is no formal "adequacy" finding, either at the EU level or by the authorities in the original country, on the basis that the controller feels that protection is nevertheless sufficiently ensured. We cannot assess how widespread this loophole is used (the basic impression is that compliance with the legal rules on data transfers is generally very low) - but a loophole clearly it is. What is more, in the new environment, in which data are constantly and routinely transferred to different jurisdictions, this problem - the use of this loophole, knowingly or unknowingly - will grow very fast.

77. Finally, there are divergences in the application of the special conditions under which data may be sent to third countries without "adequate" data protection. It may suffice to merely note here that yet again, the conditions are not uniformly applied: Some Member States add additional, stricter tests or requirements, e.g. that the derogation concerning transfer to protect the vital interests of a data subject only apply if that person is incapable of giving consent to the transfer. One Member State excessively relaxes the rules concerning transfer of data to tax officials in third countries without protection, while several others do not provide for the required derogation concerning

---

[25] See the quote from the UK Information Commissioner on p. 180 of the Comparative Summary (footnote 11, above).

[26] WP29 "Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (footnote 12, above), p. 4.

transfers of data obtained from public registers. In this respect, the WP29 issued a working document specifically:[27]

> to address its concern that differing interpretations are made of the provisions of Article 26(1) in practice, which prevent these provisions from being uniformly applied in the different Member States.

It added that:

> The Working Party considers this document as an essential element of its policy on data transfers to third countries. This document should accordingly be read in conjunction with other work done by the Working Party in this domain, namely on "binding corporate rules", standard contractual clauses, and adequacy in third countries, including Safe Harbor.

78. The document gives guidance on the application of the various special conditions for data transfers to third countries without adequate protection, set out in Article 26(1) of the Directive. However, this has not led to real changes in the practice in the Member States. In particular, the "strict" countries noted above continue to subscribe, on paper, to the view that data should not be transferred from their jurisdiction to countries in respect of which they (or the Commission) have not issued a finding of adequate protection; and the "laxer" countries continue to feel that the assessment can be left to controllers. Indeed, to the best of our knowledge, the "strict" countries do not ever issue any adequacy findings in respect of countries not already deemed adequate by the Commission.

79. Overall, in many Member States, whether strict or lax on paper, Article 26 therefore appears to be honoured more in the breach than through compliance. More harmonised interpretation of this important provision is clearly urgently needed; and this should be coupled with a uniform policy of ensuring effective compliance in all Member States. As discussed at C., below, we believe that the WP29, in particular, can help in achieving this.

B. THE NON-EU/EEA COUNTRIES

80. Even if the Directive and the OECD Guidelines inspired many of the laws in the non-EU/EEA countries, the laws are not formally linked to either of these. It is therefore not surprising that in these countries, the issues noted above are dealt with in even more divergent ways - and where there is ambiguity, as there often is, there is even less guidance to alleviate that. Some brief comparative summaries may suffice to illustrate this:

81. Definitions: In non-EU/EEA countries the approach to defining "personal information" (or "personal data") is basically much the same as in the EU, although there are variations in wording and approach to the related definitions. A lack of judicial interpretation means it is difficult to conclude whether these indicate significant differences, but they do not seem to except perhaps in Hong Kong where "personal data" has been interpreted in by the Court of Appeal, which held that there was no "personal data" where information was collected with no intention to identify the individual. Some laws are restricted to systematically organized collections of data. Indian laws do not use the term "personal data/information" at all.

---

[27] *Idem*, Executive Summary, p. 2.

82. Laws in non-EU/EEA countries do not consistently use the expressions "controller" and "processor". Some use the terms "processing" and "data user" (Hong Kong), while others use the term "processing" but do not define it (Japan).

References: Hong Kong report, 2.2; Japan report 2.2; India report 3.2.

83. Data protection principles: Laws in most of the non-EU/EEA countries included in this study are even more various in their approach on this issue, since they do not attempt to conform to any template other than the rather general OECD Guidelines. However, Australia, Hong Kong and Japan all make an attempt to implement the finality principle (though Australia and Japan allow rather broad secondary use exceptions). India does not yet have general data protection laws, but its credit reporting law applies the concept of finality very strictly (as does the equivalent Australian law, but the Hong Kong law less so).

References: Australia report, 2.2; Hong Kong report, 2.2; Japan report 2.2; India report 3.2.

84. Data protection criteria: In Asian and Pacific jurisdictions in this study, the concept of 'lawful processing' is not explicitly at the centre of the data protection legislation, and it is arguable not there by implication either. In these jurisdictions there is no assumption that processing must be justified, otherwise it is unlawful. Instead, processing (though the term may not be used) is assumed to be lawful unless it breaches one of the information privacy principles (collection, use, disclosure, security etc). As a matter of substance, this may not often lead to differences in practice, but it is a significantly different approach and attitude. Direct comparisons between these laws and the EU laws discussed in the rest of this section is therefore difficult"

85. In these jurisdictions, it is therefore necessary to assess specifically, in a particular context, whether consent or some form of notice is necessary for collection of personal data, so as not to result in a breach, and when consent, statutory authorisation or a public interest 'balance' consideration means that a secondary use or a disclosure will not be a breach of the use or the disclosure principle. In other words, the question to be asked is usually whether some particular instance of collection, use or disclosure is "legitimate", rather than the more general question of whether the processing is 'legitimate processing' in terms of a particular "criterion". Often, however, this will lead to the same answer.

86. The USA generally does not recognize a principle of proportionality in data collection. Its sectoral approach moreover creates various opt-in consent, opt-out, and no-opt situations. Opt-in consent may be required in some contexts, but not in others where the data at issue are arguably just as sensitive. See USA report at section 7.6. The USA approach focuses more on the formalism of obtaining the specified level of consent, and does not substantively probe how well individuals are informed of the implication of giving consent. Further, many businesses equate the purchase of a product or service with consent to secondary uses; this is reflected in a number of statutes that exempt consumers with "established business relationships" with a company from certain consent requirements.

Reference: USA report, sections 4.3 and 7.6.

87. Processing of sensitive data: The USA framework does not create general protections for data based upon its sensitivity alone. However, pre-employment background screening is subject to significant regulation (treated as credit reporting), based upon data protection principles. On the other hand, human resources data and other information collected in the workplace context are not covered by a sectoral privacy law. The USA treats criminal arrests and convictions as public records; generally the information can be used for almost any purpose.

Reference: USA report, sections 5.1, 5.5 and 5.7

88. Transborder data flows: In non-EU/EEA countries, restrictions on transborder data flows are very various. In the Asian –Pacific countries reported on, the position is as follows (leaving aside complications caused by the position of agents/trustees and questions of [limited] extraterritorial effect of the relevant laws):

(a) Australia has an in-force data export restriction in its private sector law (NPP 9), based loosely on Articles 25 and 26 of the Directive but weaker; it has never been the subject of a reported complaint, let alone a Court decision;
(b) Hong Kong SAR has a data export restriction in its Ordinance (s. 33) but it has never been brought into force; if in force it would be at least as strong as the Directive's provisions;
(c) India has no restrictions on data exports;
(d) Japan has no restrictions on data exports beyond the usual 'finality' requirements concerning use and disclosure, and they are also easily avoided.

89. Elsewhere in Asia and the Pacific, the only other data export restrictions are found in the Macau SAR (a strong provision based on the Directive), South Korea (based on consent) and Taiwan (a weak and unused provision). New Zealand is in the process of legislating a minimalist provision.

References: Australian Report, 6; Hong Kong report, 6; India report, 7; Japan report, 5.

C. HOW TO ACHIEVE GREATER HARMONISATION

90. **Recommendation:** As noted earlier, achieving far greater harmonisation of data protection rules within the EU is an essential prerequisite for an effective data protection regime in the EU/EEA, capable of meeting the challenges posed by the new global-technical environment. One means of achieving this would be to replace the main Directive (and therefore probably the subsidiary directives) with a (directly applicable) Regulation (something that had been originally considered in the drafting of the main Directive), or with a much more tightly-drawn entirely new directive. However, this would both open up complex questions of subsidiarity and legal competence, and would make the resulting rules less flexible. We have therefore focused on the alternative: looking for ways to achieve greater harmonisation within the framework of the main Directive, as it stands. There are various means to do this, not all incompatible with each other:

91. First of all, in respect of EU/EEA Member States, we feel that the Commission could be more robust in taking action against Member States that manifestly do not properly apply the provisions of the Directive (on paper or in practice); and indeed that the

Commission should use its enforcement powers to achieve greater harmonisation (in the manner suggested in para. 94, below).

92. However, we feel that the most crucial function in this regard could lie with the WP29: Although its opinions etc. are not binding, it has the expertise, and the direct link with national practices, to be able to formulate harmonised interpretations and manners of application of the provisions of the Directive. However, it is a point of criticism of the WP29 that at times it adopts, collectively, at the EU level, views and interpretations, and suggestions for application of the Directives, which its members are not able (or unwilling) to apply domestically. Sometimes, the texts of the domestic laws stand in the way; at other times, the DPAs simply do not have the legal power to impose interpretations or solutions agreed at the European level, domestically.

93. We feel that in this regard there is extensive scope for a strengthening of the EU data protection regime. The WP29 already adopts many important views, working documents and opinions on the interpretation and application of the Directive. Leaving aside the criticism mentioned above about these matters not always being reflected in domestic practice, these views and opinions are highly respected, in Europe and beyond, as authoritative statements of the proper interpretation and application of the EU (and world-wide) standards. The core issue is how to ensure that these views and opinions have a real impact at the domestic level - without granting the WP29 powers that should properly pertain to the Commission or the courts.

94. We recommend that the WP29 be asked, in consultation with the Commission (which in any case serves as its Secretariat) to carry out more, and more in-depth, surveys of national law and practice, with a view to formulating "best practice" and suggested interpretations (which is basically what they do already), but with an added requirement that the Member States should report on the extent to which they comply (or feel they should not have to comply) with such suggestions. It would then be up to the Commission, if needs be, to test out whether the WP29 guidance is the one that, in law, should be followed by the Member States - with enforcement action being considered as a normal means of testing this if required (cf. our earlier recommendation on stronger enforcement action, in para. 91, above). The basic idea is that the WP29 provides guidance on the proper interpretation and domestic application of the Directives (as it already does); and that if the Commission agrees that the proposed interpretation and application are the right ones, but if they are not followed by some Member States, the Commission would take enforcement action against those States. The States in question could comply - in which case harmonisation would be achieved. Or they could challenge the Commission-endorsed WP29 interpretation in the ECJ - in which case a final, authoritative ruling would be obtained, which would also support greater harmonisation.

95. We believe that this would not require any amendment to the Directive. However, it would signal a major difference in the Commission approach to ensuring more harmonised transposition and implementation of the directives, with WP29 opinions effectively, in appropriate cases, enforced by the Commission (subject, of course, to the supervision of the ECJ).

96. As a very modest step in that direction, aimed at enabling such actions by both the WP29 and the Commission, we recommend that, at least, the views of the WP29, and the extent and manner in which they are reflected in national law and practice in the

Member States, be made available in a more structured, comprehensive form, and that the attention of relevant administrative and judicial bodies at national and EU level be drawn to them.

Reference: A recommendation to this effect was already included in the recommendations of another EU Commission study that reported this year, which carried out an Evaluation of the contribution of Working Party 29 to the work of the Commission in the field of Data Protection: see Recommendation 7 of that study, which reads as follows :

> We recommend that the WP29 examine the possibility of establishing a database or similar online resource, in which relevant sections from all WP29 opinions and working documents are stored in a structured way, so that comments in any of them on a wider topic (say, on the concept of personal data, or applicable law) can be found easily and correlated; and that the members of the WP29 are asked to contribute similar details from their own national law and practice to this same resource. We believe this would create a very significant contribution to both the "added European value" already generally provided by the WP29, and to the harmonisation of (the application of) national laws and practices.
>
> We believe this resource would contribute to all three sub-topics mentioned by the WP29 in its latest Work Programme under the heading "Making the Article 29 Working Party more effective": it would contribute to the development of guiding principles and standards, improve the effectiveness of the WP29 in relation to national practice, and help in enforcement. It would also undoubtedly assist the WP29 in its advisory functions to the Commission.
>
> Note: The beginnings of such a resource have already been established in the context of an EC "e-TEN" programme, on the establishment of a European Privacy Seal, "EuroPriSe", which has just ended. For the benefit of the experts trained in that project, a set of Criteria were created, derived from the data protection directives, and a Commentary was drafted which provides exactly the kind of guidances just mentioned, with reference to WP29 documents and national practice. The Commentary was highly praised by the Commission and by the DPAs involved in the project, and eagerly sought after by companies.[28]

97. In principle, COE Convention No. 108 (with its Optional Protocol) and its associated Consultative Committee and the Project Group on Data Protection (CJ-PD) can fulfil a useful role also, and especially, in relation to non-EU/EEA and non-COE States. The Consultative Committee and the CJ-PD certainly issue important guidelines on the application of the basic data protection principles (which are shared by the Convention and the EC Directive), in particular areas, such as policing, the exchange of judicial information in criminal matters, etc..[29] However, this has not led to any greater harmonisation between the States that are party to this Convention than between the

[28] The EuroPriSe Criteria Catalogue and Commentary were prepared by the Team Leader in the current project, who was also a leading legal adviser to that project, together with lawyers from the Schleswig-Holstein data protection authority, with further input from the Madrid and French data protection authorities. The Commission has been presented with copies of these documents (NB the Commentary is not made public, for commercial reasons). [original footnote to the WP29 Evaluation report]. This recommendation was complemented by a further note from the Team Leader for that Evaluation (who is also the Team Leader for the current study), at the request of the Commission. That Note was attached to the WP29 Evaluation report as Attachment 2 to that report.

[29] These bodies have also covered some areas also (and generally similarly) covered by the EU/EEA, such as CCTV and transborder data transfer contracts. See: http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Committee%20Studies%20and%20reports.asp#TopOfPage.

EU/EEA Member States, on the contrary: harmonisation, however poor, is still better in the EU/EEA than compared with the COE Convention area.

98. Finally, we may note that outside the EU/EEA/COE there is no institution that has any prospect of encouraging much in the way of harmonisation. The APEC Privacy Framework has not had any effect in that regard. ASEAN's agreements concerning harmonisation of e-commerce laws could have some harmonising effect by 2015 within its member countries, but this remains to be seen. The Asia Pacific Privacy Agencies (APPA) meeting has no institutional basis equivalent to the WP29, nor any track record or ambitions relating to harmonisation. This makes the work of the EU WP29 even more important, on a global scale.

5. COOPERATION WITH NON-EU/EEA COUNTRIES (INCLUDING "ADEQUACY" FINDINGS)

99. **Finding/Conclusion:** In the context of the new socio-technical environment, and globalisation in particular, it is crucially important, from a European perspective, to encourage other (non-European) States to adopt data protection- or privacy laws that are "adequate" from that perspective. The main Directive of course envisages special procedures to do exactly that, and "rewards" States that do adopt "adequate" laws, after an assessment by the Commission (also involving the views of the WP29). However, this procedure has so far only been used in half a dozen cases, including three British territories in Europe (plus the rather special case of the USA "Safe Harbor" and the even more contentious US-PNR data case).[30] The Commission has not yet made a single decision concerning the adequacy of the legal regimes of any jurisdiction in Asia or the Pacific in the nearly 15 years since the Directive came into force.

100. While we accept that "adequacy" findings can only formally be issued after a rigorous process, in respect of States that really do provide such protection, this limited use of the procedure may not have sent the right signal to other, especially non-European, countries. In the Asian and Pacific countries in particular, the proposition that a country's law should meet the European adequacy standard was originally an important one in that it was felt that this could have beneficial effects on trade. This can be illustrated by the following (purely hypothetical) examples:

(i) a finding that South Korea's private sector regime is adequate, whereas Japan's is not because of its lack of enforcement;
(ii) a finding that, within China, Macau's regime is adequate, whereas that of Hong Kong is not because of deficiencies in enforcement and the failure to bring into force the data export restrictions;
(iii) alternatively, a finding that Hong Kong's law is adequate whereas that of Taiwan is not;
(iv) A finding that New Zealand's law is adequate whereas Australia's law is not.

[30] The countries currently benefiting from an "adequacy" ruling are Switzerland, Canada, Argentina, Jersey, Guernsey and the Isle of Man. Some countries (such as Hungary) had been judged to have "adequate" protection in the past, but have since joined the EU, and the procedure therefore no longer applies to them: they must fully comply with, and implement, the directives. While there was no formal finding on Australia, the WP29 gave a basically negative opinion (Opinion 3/2001 of 26 January 2001, WP40). However, it has been suggested that some of the WP29's criticisms were misconceived, and some have now been addressed by legislation, as detailed in the experts' report to the Commission on the adequacy of Australia's protections by Bygrave and Greenleaf in 2005. This does not mean that the conclusion in WP40 was wrong, only that the position is more complex than is suggested there.

Within each of these pairs of jurisdictions, such adequacy decisions would be likely to create significant pressures for strengthening of the data protection laws of the "inadequate" jurisdiction (along with some predictable political displeasure with the EU), because of their perceived position in relation to their "peer". All countries in Asia and the Pacific would also be likely to ask "would we want our laws to be found inadequate?".

101. However, this argument has steadily lost its force and has become hollow. The Asian and Pacific countries are less likely to think that this is a serious question in 2009 than they would have in 1999. The bestowing of an adequacy finding on the USA's "Safe Harbor" scheme also did not assist the credibility of the European position from this perspective, particularly when contrasted with the lack of any findings concerning some jurisdictions in Asia and the Pacific which any impartial observer would consider to have far more significance in terms of data protection than does the Safe Harbor. However, the prospect of adequacy findings has not yet lost all its force, and is still explicitly cited by the New Zealand Privacy Commissioner as a reason why New Zealand's current Bill to strengthen its data export provisions should be enacted.

Note: This is a different question than whether the standards set out in the Directive are seen as a good model for new data protection laws in Asia and the Pacific. The answer to that question still seems to be "yes", with the most recent law enacted in the region, that of the Macau SAR, being closely modeled on the Directive (via the Portuguese legislation), and the Bill under consideration in China in 2006-7 also being strongly EU-influenced.

102. We accept that the there are a number of other factors which have to be taken into account to moderate this rather blunt conclusion, and that complicate the simple examples given in para. 100: (i) the Commission normally waits for a request for an adequacy assessment from a country (although it does not need to, we can understand that it may be politically difficult to commence a procedure without such a request); (ii) "adequacy" findings - and even more so, possible "*in*adequacy" findings - have potential political implications going beyond the area of data protection, which have to be taken into account; and (iii) there are other methods available to the Commission, other than public adequacy findings, by which the Commission can encourage higher data protection standards in non-EU/EEA countries.

103. **Recommendation:** Here, we can only simply make the point that the "adequacy" process has not (yet?) had the impact that it potentially could have. In our opinion the process, and the time it takes to apply it, should be a matter for review. Perhaps provisional rulings could be an answer. In any case, the other, less formal measures, such as technical assistance, close cooperation (including "twinning" of EU- and non-EU DPAs), and other processes should continue and be strongly supported. In the meantime, it is important, at a political level, to reverse the process of Article 25 of the Directive loosing its potential international impact.

6. SUPERVISION AND ENFORCEMENT: The roles of the Data Protection Authorities (DPAs) and the courts:

104. **Finding/Conclusion:** DPAs have great insight and knowledge, and provide helpful guidance on the law - but they are not effective in terms of enforcement: "Policing" of

data protection compliance by DPAs is generally weak and ineffective. To quote the conclusions from a major report for the EU Fundamental Rights Agency, drawn up in parallel with the present report:

> This comparative report highlights the main deficiencies of the current system of personal data protection in the 27 EU Member States. Shortcomings are identifiable in the lack of independence, adequate resources and sufficient powers of some Data Protection Authorities. Compliance with data protection legislation in the praxis of several Member States also raises concerns. Legislative reforms are needed also in the field of sanctions and compensation to ensure a higher degree of enforcement of the relevant legislation and protection of the victims of personal data violations.
>
> Executive Summary of the final draft of the Comparative Legal Study on assessment of data protection measures and relevant institutions, report commissioned by the Fundamental Rights Agency (FRA) of the European Union (2009), para. 8.

We refer (and defer) to the FRA study in these general respects, except to note that weak enforcement in many countries was already noted in a much earlier study,[31] and does not appear to have improved much.

105. Here, we may limit ourselves to some more specific observations. First of all, we feel that too often, DPAs are brought in too late: they are asked to give a view on systems that are already largely "cast in stone", especially in the public sector. This can even apply to *soi-disant* "prior checks", if those are only carried out once the system has already been finally designed (with major cost implications). A second problem is that a number of DPAs are still lacking in core technical competence: there are still too many lawyers, and not enough system- and computer specialists in the authorities.

106. There is also a more fundamental question about the - in our view, to some extent incompatible - functions of the DPAs. They are advisers and guides. They are also interpreters of the law - and sometimes even quasi-legislators. They are supposed to be advocates on behalf of data subjects. And they are supposed to be law-enforcers. We feel that this is too much to ask of any single body. One danger is that as regulators, they become "captives" of those they regulate, industry and government agencies in particular. That phenomenon is far from limited to data protection authorities: it has been observed in many modern regulatory bodies. But it too serves to underline the tensions between the different functions of these authorities.

107. We feel that this issue - these tensions - should be further discussed in any review of the Directive. Perhaps consideration should be given to separating the "soft" advisory and guidance functions of the authorities from the "hard" role of law enforcement, with the latter placed basically in the hands of the courts (also acting in cases brought by individuals: see section V.7, below) and (in respect of more serious or general breaches) the prosecuting authorities. Of course, DPAs, as experts on the issues, could still always be asked to advise the court; they could even be given a right to submit their opinions *ex officio* and to have rights of appearance *ex officio* in any case raising data protection issues. In any case, to the extent that data protection issues are placed in the hands of the courts (or special tribunals, as in the UK), there should be equal access to them for data subjects and controllers.

---

[31] Douwe Korff, EC study on Case-law on compliance, 1998.

108. **Recommendations:** We recommend that there should be "prior checking" of all population-scale systems in the Member State, especially in the public sector - but (i) before they are cast in concrete (i.e., starting in the early planning stage) and (ii) by better (technically) qualified staff. It is notable that the Australian Government has recently proposed that the Privacy Commissioner in that country should be given the power to require government agencies to prepare Privacy Impact Assessments (Australia report, 8.2). In the private sector, a similar role could be fulfilled by Privacy Audits or (real and effective) Privacy Seals, strongly encouraged by public procurement rules giving competitive advantage to data protection-compliant products and services (as is already the case in Schleswig-Holstein in Germany). We will return to this latter suggestion in sub-section V.8, on *Supplementary and Alternative Measures*. More generally, we feel (without wishing to prejudge this) that consideration could be given to moving enforcement largely away from the DPAs, to the courts and the prosecuting authorities.

7. INDIVIDUAL RIGHTS AND REMEDIES

109. **Finding/Conclusion:** One of the most important requirements in any new data protection regime in the EU/EEA (and beyond) is the empowerment of individuals, in particular by removal of obstacles to litigation such as cost rules in some countries (notably England) that make it effectively impossible for individuals to sue.[32]

110. **Recommendations:** Individuals should be able to obtain effective redress, as well as interim and permanent injunctions, in speedy, simple and cheap processes before competent, independent and impartial fora. While under the principle of subsidiarity, the details of such remedies should be left to the Member States, the basic right to such remedies should be spelled out in more detail than is the case at present. In particular, the basic requirements that should be met in order to make the "judicial remedy" referred to in Article 22 truly effective, should be discussed in the WP29, and guidance issued in this respect - and in line with our recommendations in sub-section V.4.C (para. 94 in particular), the Commission should not hesitate to take enforcement action if these requirements are not met.

111. We feel that further consideration should also be given to means of supporting individuals in this respect, by allowing non-governmental/civil society groups to support, or be formally involved in, such proceedings, or to act on behalf of groups of data subjects, again without being at risk of exorbitant cost rulings (subject to court tests or court permission to prevent vexatious litigation if necessary). Although full "class actions" of the kind available in the USA are rarely envisaged in European legal systems, not dissimilar processes are sometimes available, and we feel these offer potentially more support to individuals than the current extremely weak support given to data subjects by the DPAs. A separate study into the procedures and remedies that could and should be made available to individuals and NGOs would be useful in the context of any review of the Directive. Such a study could also look at more unusual, but possibly useful arrangements, such as the US system of "*qui tam*" (described in the

[32] On this issue, see the Foundation for Information Policy Research (FIPR) consultation response on the Civil Litigation Costs Review, carried out by Lord Jackson, July 2009, which claimed that: "*From what we have been able to digest, it appears that England may be the worst place in the world for citizens to enforce our digital rights*." The submission argued for less onerous rules for individual litigants (or NGOs supporting them), as exist in other countries, such as Germany, at least in human rights cases (which would extend to data protection issues). The paper is available from: http://www.fipr.org/090730jackson.pdf.

Country Report on that country). Of course, such a study should recognise that it is primarily up to the Member States to decide how to give effect to directives. However, it may still be useful to have a clearer view of the advantages and disadvantages, and the effectiveness or otherwise, of such various procedures.

112. Consideration should also be given to setting a default, liquidated damages award for violations of certain subjects' rights. These damages awards have to be higher than the cost of non-compliance.

113. In addition, free and easy systems to support data subject rights in special contexts such as direct marketing, are popular and effective. There are Mail-, Fax- and Telephone Preference Schemes in most EU/EEA States, as well as in New Zealand, South Korea, Australia and India. The USA has a website for free access to consumer reports that is very popular. On telemarketing, the system now has 160 million numbers on its "do not call" list. These systems are popular worldwide because they are well-advertised, easy to use, and provide an effective remedy against the receiving of unwanted marketing letters, faxes, calls or SMSs (although in order to benefit from them, the data subjects' details must of necessity be kept on the relevant suppression lists, so they are not a remedy against being "on record").

8. SUPPLEMENTARY AND ALTERNATIVE MEASURES

114. In this final section, we will critically discuss a number of measures that, some believe, can supplement, or provide alternatives to, the existing means to try and ensure compliance with data protection law and –principles. Some of these measures have been well-known for a decade or more; some are encouraged by the Directive itself. However, it seems that there have so far been insufficient incentives for their use by data controllers - despite the Directive's requirement for "appropriate technical and organizational measures to protect personal data" (Article 17(1)). They also often fail to deliver. We will discuss in turn both the potential benefits and the limitations - and the often deceptive, or broken, promises - of:

- ✓ **Privacy Enhancing Technologies (PETs)**, including encryption (as a means of ensuring compliance with at least data security requirements) and a related issue: security breach notification; de-identification; and others, such as P3P and online subject access systems;
- ✓ **Privacy-Friendly Identity Management**, including (now largely outdated) centralised systems, more recent "user-centric" ones, "vendor relationship management systems", and the use of identity cards for miscellaneous purposes;
- ✓ **Privacy by Design**, including the use of Privacy Impact Assessments;
- ✓ **User Privacy Controls and Default Settings**;
- ✓ **Sectoral Self- and Co-Regulation**; and
- ✓ **Privacy Seals.**

(i) Privacy Enhancing Technologies (PETs):

Encryption

115. A recent technological development that can assist with compliance with at least some data protection requirements is the availability of encryption and related information security mechanisms. In 1990, encryption was rarely used to protect data outside government and the financial services industry. Now it is present in every Web browser to enable the secure transmission of payment card information to e-commerce servers; and most e-mail software allows messages to be encrypted before transmission. However, payment card details are still stolen from users' own machines by malicious software, and as a result of poor protection at the server; and email encryption is very rarely used by individuals or most companies – partly due to the "chicken and egg" problem that it only works when supported by both sender and recipient of a message.

116. Mainstream operating systems including Microsoft Windows, Linux and Apple's MacOS allow stored data to be encrypted, reducing the risk that thieves can gain access to data on stolen machines and removable media such as CDs and USB sticks. This is particularly important for mobile devices and laptops that are easily lost or stolen, and whose data would otherwise be easily accessible. It would be possible for "cloud" Web services (such as Google Docs) to store and even process data only in encrypted form, ensuring that access is limited to the owners of that data. However, more research is needed into "secure third-party computation" and other techniques that can improve the protection of personal data stored in cloud services.

117. Of course, encryption must be enabled and configured correctly to protect data against unauthorised access and modification. Some of the biggest personal data breaches of recent years have resulted from the absence or incorrect configuration of data security measures - including the UK government's 2007 loss of 25 million individuals' child benefit records and the exposure of the financial records of millions of TJX Companies' customers in 2003 and 2006. These breaches also reflected extremely poor organisational practice in overall system design and management.

118. Nor does encryption protect data against use of the encrypted data for purposes such as marketing and "profiling" by private- or public-sector organisations, or against abuse by "insiders" that have authorised access to the unencrypted information. The UK Information Commissioner has documented a significant criminal market in personal data stolen through the corruption or deception of staff with legitimate access to large databases at work. Encryption is far from a privacy-panacea.

A related special issue: Security Breach Notification

119. We feel that Data Breach Notification is not so much a question of remedies, but instead an addition to the security principle, because it adds to the obligations of data controllers when a security breach occurs, requiring them to provide notice(s) to DPAs and data subjects under certain circumstances. Breach of the data breach notification requirement should be regarded as a breach of a data protection principle, with all the consequences that flow from that. This means that it should not be seen as a remedy, as is sometimes proposed. However, effective data breach notification would help to make existing remedies more effective.

De- and re-identification

120. In principle, one would think that de-identification or anonymisation of personal data by controllers can reduce the risk of abuse. However, even in the "old" environment, in practice this was only true within the context of ongoing protection appropriate to the ease with which the subjects of data can be re-identified. These included strict limits on access to the full data sets; controls on queries that can collectively re-identify individual records; and a recognition that organisational failures, security vulnerabilities and changes in public policy could all result in the reversal of de-identification procedures. Even now, de-identification is hard to achieve.

121. In the new socio-technical global environment depicted in Working paper No. 1, the widespread availability of population datasets such as electoral registers, credit records and social networks will often - usually - make it trivial to identify the subjects of data even when obvious personal information such as names, dates of birth or postcodes have been removed. Advances in computer science show that we are far past the point when "anonymised" data sets such as records of search queries, movie ratings or episodes of medical treatment could be made widely available with no potential privacy harm. As Paul Ohm puts it: anonymisation is a broken promise, and in the new environment fails to protect privacy.[33] As already noted in Section IV.A (para. 47), we believe that the serious problems stemming from the near-impossibility of full anonymisation of personal data in the new socio-technical global environment pose some of the most crucial challenges to data protection, and should be at the heart of any debate on a review of the European data protection regime. In the meantime, the basic approach should be to reduce the collecting and even initial storing of personal data to the absolute minimum (cf. the German - but also European - principle of "data minimisation" and the Australian "anonymity principle"): once data have been collected and are stored, they are almost impossible to eradicate or (to take Ohm's point) truly, permanently anonymise.

Other PETs (P3P, online subject access, miscellaneous)

122. Going beyond the secure storage and communication of data, Privacy Enhancing Technologies (PETs) have been developed that provide further technological enforcement of data protection law. They can both increase the transparency of processing and minimize or eliminate the personal data required to carry out specific functions –reducing the risk of theft by organisational insiders and re-use of data for unanticipated purposes. However, they all have their limitations. We shall discuss a few.

P3P:

123. Basics PETs can provide automated disclosure of the details of processing operations by data controllers, with software helping data subjects understand this information more easily than by reading through complex legalistic privacy policies. One such system, developed in the late 1990s, was the Platform for Privacy Preferences Project (P3P). The Article 29 Working Party noted that, within an enforceable legal framework, "*P3P can help standardise privacy notices. While this in itself does not offer privacy protection, it could, if implemented, greatly advance transparency and be used to*

[33] Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (footnote 14, above).

support efforts to improve privacy protection."[34] However, P3P was criticised by campaigning groups as a "*complex and confusing protocol that will make it more difficult for Internet users to protect their privacy*".[35] Its value remains in doubt.

Online subject access:

124. The Directive's right of access must usually be exercised by data subjects in an expensive and time-consuming exchange of letters with controllers. Online subject access tools can enable suitably authenticated individuals to see all of the data held about them by data controllers. However, organisations commonly store some personal data offline for good security reasons. A major concern is also that individuals can be coerced (or simply persuaded) into providing access to third parties such as employers or parents. Without safeguards against such abuse, online subject access is more dangerous than helpful.

Miscellaneous:

125. More technically sophisticated PETs provide counter-intuitive capabilities such as anonymous communication across the public Internet; electronic cash that mirrors the anonymous nature of money in the physical world; and anonymous credentials that prove an individual has permission to access specific resources without revealing their identity. A 2007 Communication from the European Commission (COM/2007/0228) calls on industry, regulators and public authorities to better educate consumers and to make greater user of PETs to "*improve the protection of privacy as well as help fulfil data protection rules… complementary to the existing legal framework and enforcement mechanisms.*" However, it remains a challenge to deploy these technologies in usable form in mass-market software.

(ii) Privacy-Friendly Identity Management

126. Identity management is a burgeoning field of technology that aims to help Internet users manage their relationships with service providers, particularly by proving an individual is authorised to access specific resources (such as a customer account). These technologies have a key impact on privacy and can be designed in ways that facilitate the tracking and centralized surveillance of all of an individual's online and offline activities; or alternatively strictly minimize the personal data that are revealed to second and third parties, allowing individuals to enjoy the same level of privacy on the Internet as they more commonly do in the offline world.

127. A range of solutions has been proposed. Initial, centralised systems (such as Microsoft's Passport) presented significant potential privacy problems including a point of aggregation for surveillance of users and a persistent identifier that could be used to link user information across different service providers. Passport was withdrawn partly in response to consumer privacy concerns. More recent "single sign-on" and "federated" identity management systems such as Open ID also suffer from some of these problems, yet are being widely deployed by companies such as Yahoo! and Google.

---

[34] WP 37, adopted 21 November 2000

[35] Electronic Privacy Information Center and Junkbusters (2000), Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. Available at http://epic.org/reports/prettypoorprivacy.html.

128. More privacy-protective are "user-centric" identity management systems such as Microsoft's CardSpace, IBM's Idemix and the 6th Framework Programme Privacy and Identity Management for Europe (PRIME) project prototypes. These systems give users control of their own identifying information and minimise the personal information required by service providers. They prevent multiple organisations from linking together information about specific individuals, and allow users to provide anonymous "credentials" that prove various attributes (such as permission to drive or buy age-related products) without revealing any identifying information. CardSpace is now included in new versions of Microsoft's operating system and Web browser, although it has so far had limited support from service providers. There is therefore currently very little use of these technologies. We believe that their future take-up may depend upon significant government coordination, standardisation and possibly procurement action to provide the requisite incentives to consumers, businesses and system developers.

129. Vendor Relationship Management (VRM) is an associated concept that supports individuals in managing their relationships and personal data exchanges with businesses rather than the other way around, as is common with Customer Relationship Management systems. VRM systems that allow users to store data on their own systems are more privacy- protective than those which keep data on central servers. Yet again, these systems are only in the early stages of development.

130. Many countries with national identity schemes are adding identity management functionality to cards to support users' online interactions with government and in some cases the private sector. The simplest systems allow users to physically and remotely "prove" their possession of a card and its corresponding national identity number, with all of the privacy implications of using a long-term general identifier. Some cards include privacy-protective features such as access control (only authorised parties may use card information), the use of domain-specific identifiers (preventing casual linking of personal records across different government departments), and selective disclosure of information tailored to the specific application. Austria and Germany have gone the furthest in including such privacy-protective features in their national cards. However, they too all still suffer from inherent weaknesses. It might be added that, without European-level standardisation, it is unlikely that national systems will have any impact on the global market.

(iii) Privacy Impact Assessments and Privacy By Design

131. Privacy Enhancing Technologies and Privacy-Friendly Identity Management both have significant potential to protect individual privacy. However, most important of all is persuading policy-makers and business leaders to pay appropriate attention to the privacy implications of new information systems before they are commissioned. The quantity of personal data collected and processed can be very significantly affected by details decided long before system architects and programmers start building new database applications. It is much easier to produce privacy-friendly systems if data protection issues are considered early in their design stage, with data minimization and security as key concerns. Significant privacy harms can result from systems that contain sensitive personal data on millions or tens of millions of individuals, with authorized access for hundreds of thousands of staff and long retention periods - as we see with many e-government applications - and are extremely difficult to address retrospectively.

132. Two specific attempts should be mentioned that have been made to encourage early privacy planning by organisations. Privacy Impact Assessments are now mandatory in many jurisdictions including the US, requiring government agencies to assess privacy risks of new policies before systems are commissioned. As already noted, the Australian Government is also proposing to empower the Privacy Commissioner there to require PIAs from government agencies. The UK Information Commissioner encourages government and businesses to undertake assessments in order to address privacy concerns from the outset of projects, focusing on a systematic process that manages risk and incorporates the views of all those affected by new systems. Privacy By Design is an approach originally developed by the Ontario Privacy Commissioner that supports the production and operation of systems that minimise the collection, storage, processing and retention of personal data. This encompasses business policies and practices as well as the details of technologies used. It employs privacy impact assessments through the whole life-cycle of a system, from initial design, through operation, upgrades, and eventual decommissioning. The methodology needs senior management support to be effective, ensuring that privacy needs are included in the business cases for new systems and that they are met through the system life-cycle.

(iv) User Privacy Controls and Default Settings

133. Many Internet sites give users detailed information on, and options to control, the amount of personal data collected and how that data is processed. The P3P protocol was designed to specify site privacy practices to Web browsers, but controversy over default policies and other definitional issues were one reason why there has not been widespread use of these features. Browsers commonly feature "cookie cutter" functionality to manage the information exchanged with sites - although some sites limit access where all cookies are blocked. End-users make limited use of cookie management functionality, and hence the (often permissive) default settings on browsers have a significant impact on overall privacy levels.

134. Most online advertising networks follow the Internet Advertising Bureau's code of conduct for "behavioural targeting" of adverts, which specifies that users should be able to opt-out of being shown adverts based on their previous browsing behaviour. Google allows users to update their profile of interests generated by browsing sites in the AdSense network. Social networking sites such as Facebook provide detailed options for controlling who gets access to individual profiles and shared content - although researchers have found that these controls are often difficult to use and not prominent. The initial settings are rarely altered by users, and therefore have a strong impact - leading the Article 29 Working Party to suggest in a recent opinion (5/2009) that they should be privacy-protective by default.

135. In general, while "user empowerment" has been a key theme of efforts to improve online privacy since the early days of the World Wide Web, these tools are often too complex for non-technical users. Recent behavioural economics research has also found that few people have the time or inclination to undertake frequent fine-grained risk analyses of the abstract potential harms of future privacy breaches, limiting the effectiveness of these solutions in isolation.

(iii) Sectoral Self- or Co-Regulation

137. The Directive already, in Article 27, encourages the use of sectoral codes of conduct, at both the national and European level. The WP29 has given detailed, helpful guidance on the matters that should be covered by such codes, and on the "added value" that codes should provide.[36] The exact status of codes that are "ascertained" to be in accordance with the relevant national law is left somewhat open: The Directive does not require that the assessment amounts to a formal "approval" of such codes or that they be given any formal status within the legal systems of the Member States, and national practice varies. Thus, in the Netherlands, the "approval" of a code by the data protection authority does not bind the courts, while in Ireland codes can be more formally integrated into the legal regime and become legally binding. However, whatever the exact formal status of a code, once held to be in accordance with the law it will have a significant, at least quasi-legislative function. In this sense, the explicit reference to such codes in the Directive confirms a more general trend towards an increasing intermingling of statutory and *soi-disant* self-regulatory but in effect quasi-legislative norms.[37] In that sense, codes of conduct therefore shade seamlessly into more formal systems of subsidiary legislation, such as the issuing of "simplified norms" by the French data protection authority. In the public sector, the emphasis tends to be on subsidiary regulation, in the private sector on codes of conduct (although in the UK, non-binding codes of conduct and "protocols" are also - contentiously - widely used in the public sector, and in relation to data sharing between public-, and between public and private bodies). In either case, the rules are often the outcome of close cooperation between the regulators (ministries, data protection authorities, etc.) and the sector(s) concerned, usually (but regrettably not always) with input from groups representing other interested parties (indeed, often the main interested parties) such as consumers, patients, etc.

138. The WP29 approach to codes was carried over to the latest system of similar measures at corporate level, "Binding Corporate Rules" (BCRs).[38]

139. This is not the place to analyse the overall usefulness or otherwise of such self- (or quasi-self-) regulatory measures, or codes of conduct and BCRs generally. Suffice it to note that at the European level, there has only been a limited uptake of the process, with the FEDMA European Code of Practice for the Use of Personal Data in Direct Marketing the main positive example (although even in that regard, the additional rules on marketing to minors have still not been adopted or endorsed, after many years of discussion). Indeed, the slowness and meticulous attention to detail by the WP29 and the Commission have been criticised by industry and cited as the main reason for the

---

[36] See in particular WP29 Working Document Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country (WP07 of 14 January 1998). Although this document deals with the question of when a code can be said to provide "adequate" protection to allow data transfers to third countries without adequate data protection laws, the criteria applied to such codes are equally relevant for the assessment of codes in the Member States and of EU-wide codes. Codes of conduct are discussed in some detail in Douwe Korff, Data Protection Law In Practice In The EU, FEDMA/DMA, Brussels/New York, 2005, pp. 159 – 166; the text above draws on this chapter in that book.

[37] See the section (drafted by the Team Leader of the present study) on "*Regulatory Trends and New Media*" in the Commission Study on The Future of Media and Advertising (usually referred to as the Admedia Study), DG XIII/E, November 1995, Part D.1.

[38] See WP29 Working Document Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (WP77 of 3 June 2003).

presentation of so few draft codes for approval. Binding Corporate Rules have been offered for approval by national DPAs mainly in respect of multinational companies' personnel data - they have so far not given much protection to other data subjects, such as clients.

140. Outside the EU/EEA, codes have played a very limited role in Australia and Hong Kong. On the other hand, a number of sectoral "Guidelines" (e.g., METI Guidelines) have played and continue to play a key role in Japan - but they are only developed by those in the sector to a limited extend, they are more imposed by the Ministry.

141. We feel that, on the one hand, sectoral or intra-corporate rules are to be encouraged: they help to clarify how the often vague and complex rules in the directives should be applied to concrete situations. On the other hand, they should not be used to allow controllers, or groups of controllers, to effectively by-pass the basic requirements of the directives, by "creatively" interpreting or stretching the rules in the European instruments. We feel that this makes it unavoidable that the drafting of such rules will require considerable effort and consultation - and therefore time. However, in any review of the main Directive, it would be worth discussing how the process can be made more efficient, and less demanding for the WP29 in particular. Perhaps the system used in the European Privacy Seal, discussed in the next sub-section, can be helpful: in that system, approved independent experts do the preparatory work (paid for by the private parties concerned, which for codes would be the industry), subject to a close review and (if positive) certification by an official body, involving national data protection authorities. As mentioned in the next sub-section, it may be worth considering establishing a special office of the EU/EEA DPAs to deal with such matters, on a quasi-commercial (or at least fully self-financing) basis. If the idea put forward in that sub-section is deemed worthwhile, it could be useful in relation to the drafting of codes of conduct and BCRs, too.

(iv) Privacy Seals

142. Privacy seals have had a bad press: see the stinging, but justified criticisms of Trust Guard, TRUST-e, BBB, etc., in the Country Report on the USA (where most global seals originate).[39] As noted there, the main problem with voluntary seals is the question of incentives:[40]

> Privacy seal programs suffer from a fundamental incentive problem: some companies that have a strong user base have few incentives to have their privacy practices certified. For instance, Google and MySpace do not have TRUSTe privacy seals. At the other end of the spectrum, more marginal websites that seek a larger user base have strong incentives to be certified. TRUSTe and other seal programs gain revenue from issuing seals, and thus they must balance the goal of ensuring responsible practices while resisting the appeal of additional revenue from companies with marginal practices.

143. An attempt has been made to address this, to some extent, in the data protection law of the German *Land* of Schleswig-Holstein. There, the law expressly instructs public bodies of that State to give preference in their procurement to IT-based products and services that have been certified as being compliant with the local data protection law,

[39] Chris Hoofnagle, Country Report on the USA, pp. 46 – 48, with detailed references. See the Country Report on Japan for similar criticism of the Privacy Mark there.
[40] *Idem*, p. 48.

by means of a privacy seal, issued by the Schleswig-Holstein data protection authority, the ULD.[41] This has been held to not constitute an improper restriction on fair competition - on the contrary, it means that privacy-compliant products and services are given a fair chance to compete against less user-friendly competitors.

144. The Schleswig-Holstein system has been the model for the recent establishment of a European Privacy Seal, *EuroPriSe*, administered by the ULD but in cooperation with other DPAs, in France and Spain in particular. EuroPriSe was established on the basis of a pilot project funded by the European Commission in its then "e-TEN" programme. The project was given the highest possible mark by the EU evaluators, who judged it to be "high" on the criterion "supportive on EU policies on data protection, compliance and application and directly relevant to EU policies in trust and security." The EuroPriSe scheme was also warmly welcomed by (then) Commissioner Viviane Reding and strongly supported by the European Data Protection Supervisor, Peter Hustinx. A report on privacy in the digital age (*La vie privée à l'heure des mémoires numériques*), released by the French Senate's Commission on Laws in June this year, considered to be one of the most important legislative initiative in France in the field of privacy and data protection since the implementation of the EU Data Protection Directive in 2004, also praised EuroPriSe and stated that the initiative is exemplary for national schemes and should be intensified.

145. We suggest that the EuroPriSe scheme be further discussed in the context of any review of the Directive. In particular, we believe that it would be most useful to include in the Directive a rule on the lines of the Schleswig-Holstein one, that instructs public authorities in the Member States, and EU bodies, to procure privacy-compliant products and services whenever possible. If this cannot be formally stipulated in the Directive, we feel that nothing stands in the way of encouraging such procurement rules in other ways, e.g., by the adoption of such an approach as a matter of policy by the Commission and the Member States. We feel that in principle (but subject to the note, below, and to the more general *caveat* in para. 146) procurement rules and –policies of this kind can offer the best incentives yet for strong, effective data protection and serious compliance with data protection rules on the part of commercial bodies offering privacy-sensitive products or services.

Note: Any such measure must of course take into account both EU competition law and the law on free movements of goods and services (and indeed WTO rules). Such schemes must be designed in a manner that excludes the risk that they have anti-competitive effects or unfairly influence the trade between Member States. However, the Schleswig-Holstein scheme suggests this is possible.

146. A further aspect of the EuroPriSe scheme (already mentioned) is the establishment of a Certification Authority for the issuing of the seals, and the accreditation of specially-trained and tested independent experts, who carry out the primary evaluation of the products. The Authority is essentially made up of the participating DPAs, and the experts are rigorously trained and strictly assessed. The system is self-financing, through the payment of fees by companies applying for the seal (who also pay the experts, but separately, on the basis of individual arrangements). As noted above, in Schleswig-Holstein, the State DPA is formally authorised to act in this way. At the European level, this has proven to be more complicated, in that not all national DPAs

[41] See: https://www.datenschutzzentrum.de/guetesiegel/index.htm, or for more summary information in English: https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm.

can formally participate in the scheme, under their current laws. In the review of the Directive, consideration could be given to mentioning participation in such a scheme in the list of tasks of DPAs (cf. the current Article 28).

147. Indeed, it may be useful to consider the establishment of a special body or office of the EU/EEA DPAs, closely linked to the WP29 and the Commission, to deal with such matters, on a quasi-commercial (or at least fully self-financing) basis, in a way similar to the ULD system. As already mentioned, such a body or office could be asked to deal, not only with the European Privacy Seal, but perhaps also with the preparation of European codes of conduct, and Binding Corporate Rules - in each case leaving the initial work to independent (but tested and properly accredited) experts, with the final assessment and certification carried out on a semi-commercial (self-financing) basis by the bureau.

Note: The question of the status of such a body, and its formal relationships with national DPAs and the EU bodies is a complex one, as was noted in the "e-TEN" *EuroPriSe* pilot project. However, the establishment of national certification- and accreditation bodies is quite a usual phenomenon in Europe. Indeed, there is a recent regulation, Regulation (765/08) on Accreditation and Market Surveillance, that will, from 1 January 2010, for the first time provide a legal framework for the provision of accreditation services across Europe, setting out the provisions for operation of accreditation in support of voluntary conformity assessment as well as conformity assessment required by legislation. An assessment of the basic idea of a European Privacy Seal certification and accreditation system could look at this wider context for inspiration.

148. However, any of the above must be undertaken with great care. Everything depends on the strength of the seal conditions and their enforcement. The EuroPriSe scheme scores well on both points precisely because the criteria that are applied are very strict and set by data protection authorities in countries with strong data protection, and because the scheme is also basically administered by DPAs, who are not driven by the need to optimise return or make any profit (many DPAs are indeed prevented by law from participating in any profit-making activities). Schemes without such guarantees are unlikely to ensure real compliance with the EU/EEA standards.

149. Clearly, these are only tentative suggestions. However, we feel that it will be important, in the new socio-technical environment, to have new systems in place that can deal in an effective, not overly bureaucratic way with measures aimed at ensuring appropriate data protection in specific sectors, (multinational) companies or contexts. But unlike the previous, largely discredited seals (etc.), such systems should (like the EuroPriSe system) be closely linked to the official regulators, and not be driven by commercial interests.

(v) Conclusion

150. We fear that there is no "magic bullet" to ensure adequate data protection. The law is by its nature often difficult to interpret and apply, and either too vague or too inflexible, while supplementary and alternative (non-legal or quasi-legal) measures have suffered from serious, often inherent weaknesses. Some measures and technologies have been shown to be little more than fig-leafs. Any review must be based on realistic, and technically correct evaluations of such measures. That is not to say that they should be dismissed out of hand. However, they will have to be closely scrutinised, by technical as well as legal experts: as Ohm's article makes clear in one (but crucial) respect, de-

and re-identification, legislators and policy-makers the world over have often failed to understand the new technologies and their implications.

151. Overall, as noted in the last sub-sections, the question of incentives and economics of privacy and data security are central. If the law makes the protection of privacy economically attractive (e.g., through procurement incentives, coupled with the issuing of serious privacy seals, as discussed), or punishes breaches of data protection and data security rules (by placing the onus for protection on those who are in the best position to ensure them, rather than by allowing them to shift the costs to others, such as consumers), then data protection can have a future. We believe that that requires the right combination of law and self- or co-regulatory rules and mechanisms. We hope the above gives some food for thought on these.

- o – O – o -

Core experts:
Douwe Korff, Team Leader
Ian Brown, Co-Leader

Special experts:
Peter Blume
Graham Greenleaf
Chris Hoofnagle
Lilian Mitrou
Filip Pospíšil
Helena Svatošová
Marek Tichy

Advisers:
Ross Anderson
Caspar Bowden
Katrin Nyman-Metcalf
Paul Whitehouse

Cambridge/London/Oxford, 15 January 2010

ATTACHMENTS:

- Working Paper No. 1 **The challenges to European data protection laws and principles**
  (An overview of the global social and technical developments and of the challenges they pose to data protection)

- Working paper No. 2: **Data protection laws in the EU**
  (A comparative-analytical overview of the difficulties the law has in meeting the challenges posed by the global social and technical developments)

- Country Reports: **European countries:**

  – Czech Republic
  – Denmark
  – France
  – Germany
  – Greece
  – United Kingdom

  Non-European countries and jurisdictions:

  – USA:
    ✓ Federal level
    ✓ California
    ✓ New Jersey
  – Australia
  – Hong Kong
  – India
  – Japan

- Comparative Chart of National Laws

- o – O – o -

NB: In addition to the above attachments, which are formally part of the study, the authors have also provided the Commission with several other reports, mentioned in the text or in footnotes, with most of which one or more members of the expert team were involved and on which they could therefore draw (unless the Commission already had those reports).