D.2.2 European Cultural Preservation in a Changing Legislative Landscape

DOI: 10.5281/zenodo.1170112

Grant Agreement Number:	620998
Project Title:	European Archival Records and Knowledge Preservation
Release Date:	9th February 2018
Contributors	
Name	Affiliation
David Anderson	University of Brighton
Andrew Wilson	University of Brighton
Kuldar Aas	National Archives of Estonia
Zoltán Szatucsek	National Archives of Hungary

TABLE OF CONTENTS

1. Executive Summary

The adoption by the EU of the Data Protection Directive (95/46/EC) marked a pivotal moment in the history of European personal data protection. Two decades later, the fundamental principles around which the Directive was structured continue to be relevant, but the ever-increasing pace of technological change, and globalisation have undoubtedly presented challenges for data protection that the original Directive is ill-equipped to address. The world of the early 21st Century is the world of social networking, apps, cloud computing, location-based services and smart cards. It is almost impossible for individual citizens to go about their daily business, or to buy goods and services without leaving digital footprints. Without effective control over how this information is stored and used, the potential for adverse consequences is obvious.

So it is that the European Commission is currently engaged in a process of modernising the EU legal system for the protection of personal data. One of the key policy objectives behind the revisions is to make more consistent the implementation and application of the protection of personal data in all areas of the Union's activities. Anticipated benefits include the strengthening of the rights of individuals, reduced administrative overhead, and an improved flow of personal data within the EU and beyond.

The main part of this report covers the requirements of Directive 95/46/EC, which have been implemented by Member States in a variety of legislative instruments since the adoption of the Directive in 1995. These are set alongside the General Data Protection Regulation (GDPR) proposals currently under discussion between the Commission, the Council of Ministers and the European Parliament. As a final form of the text has not been agreed at the time of writing some of the conclusions reached in this report are necessarily tentative in nature.

Individual citizens (or data subjects) are not the only stakeholders on the digital playing field. Within the context of this report, we will also pay attention to institutional stakeholders, particularly in the cultural heritage sphere. Memory institutions such as galleries, libraries, archives and museums are both custodians of our common digital heritage, and aggregators and generators of large quantities of born digital and newly digital information. Many of the leading organisations such as national archives and libraries have a legal deposit responsibility which obliges them to collect and retain vast quantities of digital information, and to make this, as far as possible, available to the public today and in the future.

The law, even within a single national jurisdiction, is often complex in character, and legislation is generally drafted in a form that lay readers struggle to comprehend. The situation is made even more difficult when many pieces of legislation may potentially apply to an activity, and where the law makes competing demands. Thus, a national archive may have a general obligation under the Directive(s) on the Re-use of Public Sector Information to ensure that information held by them is made available to the public, while the Data Protection Directive, may oblige them to protect the privacy of individual data subjects by keeping some information undisclosed. Preserving files intact is a natural activity for memory organisations, yet there is increasing pressure for data subjects to be given the right to have data concerning them purged altogether. In some cases this may not even be technically feasible. Even the act of preservation, which constitutes much of the raison d'etre of galleries, libraries, archives and museums, may in the digital

context, involve techniques and processes which conflict with EU Directives, while simultaneously being required under national legislation. The legal landscape is thus far from clear, even to experts in the field, and while discerning the overall legal requirements in every case may not be an intractable problem, it does provide an on-going, and ever more complex challenge to those charged with preserving our digital records.

The Commission's proposals amount to a fundamental modernisation of Europe's data protection rules, establishing a number of new rights for citizens of which the right to be forgotten is only one.

General Jurisdictional scope

The new regulatory arrangements both simplify the existing arrangements, and extend significantly the reach of EU legislation, taking it beyond Europe's borders. Under the new regime, processors of personal data will fall under the regulations. The existing old "means" and "equipment" tests are abandoned in favour of concentrating on whether non-EU controllers are providing goods/services to data subjects in the EU, or are monitoring their behaviour. However, some potential remains for legal uncertainty arising from a lack of clarity about the meaning and scope of key terms in the new proposals.

Scope of personal data

Under Directive 95/46/EC there is some divergence of opinion between Member States as to what constitutes 'personal data' The new proposals are expected to establish a single broad definition of personal data for the whole of the EU. Henceforward, 'identification' will depend on the likelihood of 'singling out' an individual directly or indirectly, rather than being limited to the possibility of knowing details such as their name and address.

It will be prudent to take a very conservative approach to the collection, processing, and retention of personal data. Only the minimum data should be handled; data should be assumed to be personal unless there are clear grounds for believing otherwise; personal data should be held only for the minimum time required mindful of the purpose for which it is being held and processed; organisations should be able to demonstrate an audit trail showing that data no longer held has been securely deleted; where possible data should be anonymised.

The Obligations and Liabilities of Data Controllers

It is something of a truism to assert that the notion of 'data controller' is key in data protection regulation. The new proposals introduce a modify somewhat the definition of 'controller' used in Directive 95/46/EC, and having done so, then pay considerable attention to delineating obligations and liabilities which controllers must respect.

Echoing the provisions of Directive 95/46/EC, the general principles which govern personal data processing are stated and may be understood as stipulating "the less the better". Thus, data should be retained no longer than absolutely necessary, and processing should be kept to a minimum.

Controllers will be held responsible for ensuring the existence of transparent and easily accessible policies with regard to the processing of personal data, and for the exercise of data subjects' rights, as well as ensuring that any information or communication concerning the processing of personal data uses clear and plain language. They will also be required to provide the means for data subjects to exercise their rights.

The new regulations assert the right of data subject's right to data 'portability', that is to say, they will have the right to both obtain those data from the controller, and to have them provided in a structured and commonly used electronic format.

Controllers will have to respect the 'principle of accountability' and be able to demonstrate their compliance. Typically this would mean being able to show internal policies and mechanisms for ensuring such compliance. There is also a requirement for controllers (and processors) to carry out a data protection impact assessment prior to risky processing operations.

The new proposals introduce 'joint controllers', who are understood to be processors working beyond the controller's instructions, and clarify the obligations of the controller and the processor for co-operation with the supervisory authority.

Building on the personal data breach notification in Article 4(3) of the e-privacy Directive 2002/58/EC, the new proposals place an obligation on controllers to notify supervisory authorities of personal data breaches, and to notify personal data breaches to data subjects.

Finally, the new rules build on Article 23 of Directive 95/46/EC to extend the rights of data subjects to damages resulting from the action of processors and clarify the liability of joint controllers and joint processors.

Lawfulness of processing

The new regulations follow closely the existing requirements under Directive 95/46/EC. However, one area where a significant tightening of the rules will take place is the regime for obtaining valid consent.

Controllers will be required to bear the burden of proof for the data subject's unambiguous consent to the processing of their personal data for specified purposes. Data subjects will have the right to withdraw their consent at any time.

In cases where there is a significant imbalance between the position of the data subject and the controller, consent will not be regarded as providing a legal basis for processing.

The impact these amendments will have in individual Member States, will naturally depend on the extent to which their current national legislation takes a stricter or more lenient position on consent.

The Right to be Forgotten

It is clear that while, under the new regulations, data subjects are set to enjoy the right to be forgotten, this right will be by no means unrestrained. Data controllers will be required to attenuate the right to be forgotten against, particularly, the right to freedom of expression when determining whether to accede to removal requests. Controllers will also have the option to 'restrict processing' of contested data rather than to remove it completely, but, in practice, the burden imposed on data controllers by expecting them to balance the right to be forgotten against the right to freedom of expression, and deciding whether it is more appropriate to restrict processing or to complete erase data, is likely to be severe. This is, if anything, exacerbated by cascading this responsibility down to secondary controllers.

Either way, many data controllers are likely to find themselves acting as both judge and jury when considering requests. The right to be forgotten has been the subject of much discussion at Council level, particularly in the light of the decision of the Court of Justice of the European Union in Google Spain.

Data Portability

There remains considerable debate over the provisions for data portability, whether they would not sit more appropriately under competition law, and what limitations may apply. Undoubtedly, compliance with the regulations in their current form would impose on businesses a significance cost burden. The extent to which this is justifiable, particularly in the absence of any real evidence of 'customer lock-in', is questionable. While we may be reasonably confident that data portability, in some form, will feature in the final version of the new regulation, it is far from clear what that form will be.

Automated Individual Decisions / Profiling

It is not yet possible to have any clear idea what the final shape of the new regulations will be with respect to profiling. However, a balance needs to be struck between providing, on the one hand, rights for data subjects to object to automated profiling, and on the other the interests of businesses who depend for the viability on being able to 'target' audiences, or discriminate between potential customers. What that balance will look like is by no means clear.

Data protection officials/officers

The appointment of a Data Protection Officer represents a significant administrative and cost overhead on businesses, in consequence of which there has been a robust debate as to whether the new regulations should require them to be employed, or to permit organisations to continue with the current voluntary arrangements. Counter-proposals include limiting the mandatory appointment of a Data Protection Officer to cases where a certain threshold of data processing activity has been crossed in addition to limiting the requirement to public bodies and larger enterprises. It is simply not clear at this point how this particular aspect of the proposed new regulations will be resolved in the final text.

Data protection by design and by default

Privacy by Design (PdD) is an approach to systems engineering which promotes privacy and data protection compliance from the outset and involves the whole engineering process. The gold standard for PbD is encapsulated in the seven 'foundational principles of privacy by design' produced by The Canadian Privacy by Design Centre of Excellence. The proposals put forward by the Commission fall some way short of incorporating all seven of foundational principles, and reflect to some extent the debate which has been going on between the European Commission, Parliament and Council as to the scope and detail of the PbD requirements.

Nevertheless, it is clear that the new regulatory framework will require organisations to take full account of developments in technology and solutions for privacy by design and data protection by default and will no longer be satisfied to see privacy and security as something of a post hoc addition to products and processes.

Jurisdictional scope: Controllers not established in the Union

Proposals are still under discussion about bringing non-EU processors conducting business within the EU, and processing EU data subjects' personal data under the scope of the new law.

However desirable this may be, it will not be clear for some time after the introduction of the new rules whether it is possible, in practice, to enforce the rules. Some commentators have questioned whether sufficient resources will be available to enforcement agencies to bring to a successful conclusion prosecutions outside the geographical boundaries of the European Union.

Security of Processing

Measures to ensure the security of data processing are implemented differently in the various Member States. Directive 95/46/EC gives relatively little guidance on how to handle security. The new proposals while broadly repeating the approach of Directive 95/46/EC do make some movement in the direction of providing indicative compliance benchmarks

Personal Data Breach Notification

While there may be some amendment of the precise time periods within which notification to the competent authority, and the data subject must take place, there is little doubt that the new regulations will require controllers and processors to make notification of breaches within a relatively short time. Mindful of the sanctions proposed for non-compliance these deadlines will need to be respected.

It will take some time after the new regulation comes into effect before it is clear whether this aspect of the new rules will be workable in practice. On the one hand, notification within 24-72 hours may prove to be too challenging, while on the other, concern over the possible consequences of being found in breach of an obligation to notify may lead controllers/processors to err on the side of caution and notify so frequently that the system fails in practice.

Transfer of personal data to a third country

At present there are marked differences in how Member States treat the transfers of personal data to third countries in those cases where neither the Commission nor their national authorities have determined the adequacy of the arrangements in place.

Overall, the intention under the new proposals appears to be to build on the current framework. Organisations who are acting solely in the capacity of data processors will need to be mindful of the rules which govern international data transfers, as significant penalties may be incurred for breaches of the regulations.

It should be noted that under the new proposals the Commission will have sole authority to determine which countries are deemed to provide adequate safeguards for personal data, and that decisions once taken will continue to be subject to being overturned or revised. There is general approval for the idea of a European Data Protection Seal, and this will be only one of a number of new mechanisms for certifying data processing as adequately safeguarded. An important distinction has been drawn in the new proposals between safeguards (such as one-off contractual clauses) which will continue to require authorization from a data protection authority, and those (such as legally binding and enforceable instruments between public

authorities) which will not. It is also worth highlighting that data transfer may, if the Council has its way, henceforward require explicit consent to count as valid.

Legal enforcement & Penalties

Final decisions have not yet been reached about the sanctions and penalties that will be available under the new regulatory scheme. However, it is already clear that sanctions will in the future be much onerous than those in place today. Originally, the commission proposed fines amounting to 2% of annual global turnover be imposed in the most serious cases, but that figure seems to have been abandoned in favour of even more severe penalties. We can expect that sanctions will be set at a level that compels data holders to take very seriously the potential legal consequences of paying insufficient attention to (particularly) their corporate data protection responsibilities. Whereas the relatively modest sanctions scheme provided under Directive 95/46/EC meant that organisations could, if they chose, afford to risk infringing data protection requirements, this course will no longer be open under the new scheme.

Reproduction Rights

With respect to reproduction rights, Community law does not provide an appropriately accommodating legal framework. Articles 5.2 (c) and 5.3 (n) of the Information Society Directive of 22 May 2001, appear to provide libraries with public access, educational establishments, museums and archival services, limited exceptions to the general restrictions placed on unauthorised reproduction and communication. However these do not cover computer programs or databases and therefore transfers of this kind of material remain problematic.

More and more, digital objects are multimedia in nature. Problematically, no definition of multimedia exists in Community law. Therefore it is necessary to look to national interpretations to determine their legal nature. The legislative frameworks examined for this report (France, Germany, The Netherlands) regard multimedia works as 'complex works' and take a distributive, fragmented approach in which each component part of a multimedia work: audio, graphics, software, database, etc., is considered separately. Since multimedia works are not, in general, made available on computer platforms in such a way that individual elements can be removed from the whole, this means that, in practice, a multimedia work will enjoy, as a whole, the strongest protection under law that is available for any of its constituent parts.

Technological Measures of Protection (TMP)

Many works are made available in a form to which technical measures have been applied to prevent or restrict the use that may be made of them. This might take the form of a simple password protection scheme or may involve considerable technical sophistication.

The Information Society Directive (2001/29/EC) recognises the "need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect". Article 6 [2], stipulates that "Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective." However it also permits Member States to be given the option of "providing for certain exceptions or limitations for cases such as educational and scientific purposes, for the benefit of public institutions such as libraries and archives".

The potential for exemptions is quite limited, and does not extend to permitting the creation or use of tools by individuals to bypass TMP generally.

2. Specific recommendations to the archival community arising from the GDPR[1].

The GDPR introduces new concepts, and revises the understanding of those drawn from earlier data protection regulation. Not everything has changed, but a great deal has, and nothing should be taken for granted. In this E-ARK deliverable, readers will find a section by section comparison of the existing regulation with the text of the GDPR. The purpose of the current section, together with section 3, and appendix 1, is to supplement that analysis with a very abbreviated set of discrete recommendations targeted, primarily, at the archives community.

In what follows suggestions are made under five key areas:

- The Obligations and Liabilities of Data Controllers
- Consent
- Personal Data Breach Notification
- Transfers of personal data
- Legal enforcement & Penalties

Where advice is offered, it is couched in terms of:

- what one should Ensure happens
- what one should Monitor
- what one should Consider

[2] **Disclaimer:** The advice given in this deliverable, is simply advice, and as such should NOT be treated as legally definitive.

[1] The recommendations here draw on a number of third party sources. The most important of these is Bird & Bird's extremely valuable guide to the General Data Protection Regulation. See https://www.twobirds.com/en/hot-topics/general-data-protection-regulation. See also Allen & Overy's "The EU General Data Protection Regulation", available from http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf and the various factsheets and other advice available from the European Commission at http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[2] Graphic taken from: https://commons.wikimedia.org/wiki/File:Warning_icon.svg

The Obligations and Liabilities of Data Controllers

Ensure: that any data processing carried out using "legitimate interests" as a justification remains lawful under the changes introduced by GDPR.

Ensure: that all decision-making which involves striking a balance between the interests of the controller and the rights of data subjects is fully documented.

Ensure: that careful and documented consideration is given to the balance of children's interests against the interests of your organisation when processing children's data.

Ensure: compliance with the new GDPR rules covering the processing of sensitive data, especially with respect to "genetic" and "biometric" data where this is used to uniquely identify a person.

Ensure: processes, procedures, training, and data formats are adequate to deal with the new access and portability rules.

Ensure: that every element of supporting information is made available.

Ensure: data (and metadata) can easily be exported in structured, machine-readable formats.

Ensure: that individuals are told about their right to object in an intelligible manner, clearly, and separately from other information, they receive.

Ensure: staff training is adequate to equip staff to recognise, and respond appropriately to, data erasure requests.

Ensure: explicit consent exists for all automated decision-taking based on consent.

Ensure: explicit consent exists for all automated decision-taking based on sensitive data.

Ensure: explicit consent exists for all automated decision-taking involving children.

Ensure: that the purposes for which personal data are collected are specified at the time of data collection

Ensure: that all existing information notices are reviewed and updated where necessary.

Ensure: that appropriate and timely notice is given in cases where data is collected indirectly.

Monitor: which records are covered by the GDPR portability rules

Monitor: data protection notices and policies, and practices, including those delivered by third party organisations.

Monitor: the extent to which automated decision-taking is used.

Consider: using a legal basis other than “legitimate interests” for data processing

Consider: discontinuing some areas of data processing activity altogether.

Consider: using interoperable systems where possible, to facilitate data portability.

Consent

Ensure: compliance with the new GDPR rules covering obtaining consent.

Ensure: that consent is provably "active" (documentation).

Ensure: that consent to processing (other than that which is absolutely necessary) is not a condition of the supply of services.

Ensure: that data subjects are made aware of their right to withdraw consent at any time, without undue difficulty.

Ensure: that each distinct processing operation, has a corresponding distinct consent.

Ensure: consent is active, and does not rely on silence, inactivity or pre-ticked boxes;

Ensure: consent is not relied on as a justification for data processing where there is a clear imbalance between the data subject and the controller (especially if the controller is a public authority).

Ensure: that services offered directly to children contain notices written in plain language, adapted to a child's understanding.

Monitor: all relevant codes of conduct.

Consider: the extent to which the GDPR rules on children affect you.

Consider: which national rules need to be followed when obtaining the consent of children.

Personal Data Breach Notification

Ensure: that your organisation has clear lines of responsibility, and a sufficient budget, for data protection compliance.

Ensure: a proper record is kept of data processing activities.

Ensure: that your organisation has a complete compliance program, covering processes, procedures, and training.

Ensure: internal breach notification procedures comply with GDPR.

Ensure: appropriate technical and organisational measures exist to render data unintelligible in case of unauthorised access.

Ensure: insurance policies provide adequate cover in light of the new GDPR enforcement regime.

Transfers of personal data

Ensure: that all proposed transfer of personal data is GDPR compliant.

Monitor: Review and map key international data transfers for both data controllers and data processors.

Consider: whether existing data transfer mechanisms are adequate under GDPR

Legal enforcement & Penalties

Ensure: each controller and processor and, if any, the controller's representative, maintains documentation of all processing operations under their responsibility.

Ensure: All personal data breaches are reported to the data controller, and that the content and format of such reports is GDPR compliant.

Ensure: everyone involved with data processing operations understands their data protection obligations.

Ensure: risk registers are kept up to date.

Ensure: insurance policies provide adequate cover in light of the new GDPR enforcement regime.

3. General recommendations to the archival community.

Clearly, the introduction of the GDPR presents a challenge to archives. Not only is the GDPR wide ranging and fairly complex in and of itself, but it is only one of a number of legal and regulatory instruments the requirements of which archives must address. Within the Archives community, discussion around the GDPR has brought into focus the need to develop robust and accessible support mechanisms to assist archivists navigate the legal and regulatory landscape. This was discussed at length at the DLM Forum meeting held in Oslo during November 2016, and a number of recommendations were made under the general headings of Analysis, Inventory, Professional Contacts, Expert Groups(s), and Visibility.

Recommendation 1: Analysis

The community, working through organisations such as the DLM Forum and the International Council on Archives, should develop, circulate, and maintain information sources on the detailed legal and regulatory instruments in force at any given time. An example of this sort of resource is this report, but similar analyses need to be developed for the full range of laws and regulations which apply to archives and archiving, particularly those which apply at the European Community level (as National law is subordinate to European Community Law).

Where possible, these analyses should draw out, and make clear to the community, any tensions (or contradictory requirements), within individual laws or regulations, as well between different statutory or regulatory instruments applying to the same, or related, area of activity. These are precisely the issues which give rise to the greatest difficulty in applying legislation or regulation effectively, and understanding where difficulties are likely to arise is very beneficial to practitioners. Additionally, understanding where laws or regulations have not been drafted consistently is key both to formulating an appropriate action plan, and to informing community feedback to legislators and regulators.

A clear understanding of the requirements of current legislation and regulation is of undoubted value, but it is also important for the community to carry out 'horizon scanning', so that we may alert in advance practitioners to changes in the regulatory and legal framework which have not yet come into force, but are likely to do so in the foreseeable future. Being in possession of information about the intended direction of travel with respect to legislation and regulation, enables the community to engage better with the process of developing new controls, and to participate more effectively in a dialogue with legislators and regulators.

We are a community of practitioners, therefore where possible, it is helpful to provide 'real-life' examples, rather than theoretical analysis alone.

Recommendation 2: Inventory

The archival community should develop a knowledge base of past and present problems encountered in applying legislation and regulation, together with a record of both the formal and informal approaches taken.

Judicial decisions often involve interpretation, and in cases where there is no applicable legislation, the decisions of courts serve to establish legal norms, which may come to affect future legislation and/or regulation. It is therefore important that we also maintain a database of case law as it applies to the legal

control of archiving. Since so much of our activity is involved with the use of computers, it is important to include ICT-related cases as part of our overall knowledge base.

Recommendation 3: Professional Contacts

It is vital that archives should not simply become spectators as legislation and regulation is conceived and implemented. In order both to shape legislation and regulation, as well as to comprehend fully how it applies to the archiving sector, we need to be fully engaged. This may be accomplished through personal contacts at a senior institutional level, as well as by engaging with a variety of bodies such as Digital Preservation Expert Groups, and the national data protection authorities[3].

Under the current arrangements, representatives of the national data protection authorities (DPA), the EDPS and the European Commission, comprise the so-called "Article 29 Working Party", the remit of which is to:

> "To provide expert opinion from member state level to the Commission on questions of data protection.
>
> To promote the uniform application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities.
>
> To advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy.
>
> To make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community."[4]

With the introduction of the General Data Protection Regulation (EU) 2016/679 (GDPR), the organisation of national data protection authorities will be changing. In 2018, this will become the European Data Protection Board (EDPB), and on 2nd February 2016 the Article 9 Working Party released a work programme[5] which laid out the activities they have planned to ensure that the EDPB works effectively from day one. During this interim phase, it is particularly important to monitor closely the work of the Article 9 Working Party.

[3] A full list of the contact details for the national data protection authorities, and their Article 29 Working Party representatives, is appended to this report as Appendix 1. Last updated; 13th February 2017.

[4] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/tasks-art-29_en.pdf

[5] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp235_en.pdf

Recommendation 4: Expert Group(s)

The archival community, represents a considerable body of expertise in its own right, and this would be deployed more effectively through the establishment (or extension) of both formal and informal digital preservation professional groups and bodies.

In addition to engaging with groups such as the EDPB, we should not hesitate to give our expert opinion on problems, indeed we should actively seek out opportunities to make the voice of the archival community heard. We should therefore develop a formal process through which to issue recommendations both to the archival community, as well to legislators and regulatory authorities.

Recommendation 5: Visibility

One of the noticeable differences between the archival community and the library counterpart, is a relative lack of visibility.

It is important, in the context of the application of legislation and regulation of our activities, that we make every effort to raise the profile of archives and bring to the attention of regulators and law-makers the issues that affect us most significantly, as well as any areas where the impact of legislation and regulation is not immediately obvious. It is also important that we speak to, and involve, the wider archival community.

This may, in part, be accomplished through panel sessions and presentations at digital preservation conferences, and archival fora. Additionally, conventional publications, interviews, blogs and tweets help to raise our profile and to engage the wider community.

In all of this, organisations such as the DLM Forum Foundation, and the International Council on Archives have a significant role to play.

4. General Introduction

Archives provide an indispensable component of the digital ecosystem by safeguarding information and enabling access to it. Harmonisation of currently fragmented archival approaches is required to provide the economies of scale necessary for general adoption of end-to-end solutions. There is a critical need for an overarching methodology addressing business and operational issues, and technical solutions for ingest, preservation and re-use.

In co-operation with commercial systems providers, the E-ARK consortium aims to create and pilot a pan-European methodology for electronic document archiving, synthesising existing national and international best practices, that will keep records and databases authentic and usable over time. Our objective is to provide a single, scalable, robust approach capable of meeting the needs of diverse organisations, public and private, large and small, and able to support complex data types.

The practices developed within the project will reduce the risk of information loss due to unsuitable approaches to keeping and archiving of records. The project will be public facing, providing a fully operational archival service, and access to information for its users. The project results will be generic and scalable in order to build an archival infrastructure across the EU and in environments where different legal systems and records management traditions apply. E-ARK will provide new types of access for business users.

At present, no comprehensive survey of the legal and organisational framework under which European recordkeeping, preservation and access take place is available to practitioners in the field.

Facilitated by the DLM Forum with its broad EC-wide membership comprising public bodies, service providers, technology providers and national archives, we aim to provide an overview report in relatively plain language dealing with the legal and regulatory requirements for data protection, the reuse of public sector information, and copyright legislation. In particular, this report provides coverage and an analysis of the following EC Directives and Regulatory Instruments:

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
- Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property
- Directive 95/46/EC of the European parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Directive 96/9/EC of 11 March 1996 on the legal protection of databases (the “Database Directive”)
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001, on the harmonisation of certain aspects of copyright and related rights in the information society
- Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Directive 2003/98/EC of the European parliament and of the Council of 17 November 2003 on the re-use of public sector information
- Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)

- Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs (Codified version replacing the abrogated Directive 91/250/ EEC of 14 May 1991, known as the "Computer Programs Directive")
- "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012
- Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information

The findings presented in this report are intended to provide a greater understanding of the legal framework as it impacts on cross-border co-operation. This report will be used to inform the other Work Packages within E-ARK as it is essential to ensure the project aligns with EU Directives as implemented by Member States.

Three broad areas are examined:

- Data Protection
  At the time of writing, it is not possible to say exactly what regulatory provisions for Data Protection will be put in place by the EC, as discussions are still taking place within (and between) the European Parliament, the Council of Ministers, and the Commission about exactly what changes should be made to the provisions of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. However, the broad brush stokes of the new regulations are reasonably clear, and some 17 key areas, where change seems more or less certain, are examined reasonably closely.

  The approach has been to present and analyse the current requirements as set out in Directive 95/46/EC, followed by presenting and examining the regulations which are expected to replace them, finally, some concluding remarks are offered.

- Re-use of Public Sector Information.
  The general approach here is broadly similar to that taken with Data Protection. The background to the regulatory framework is discussed, and placed in context. The obligations placed on Member States by Directive 2003/98/EC on the re-use of public sector information, are explained, and then compared against Directive 2013/37/EU, which was introduced to amend it.

- Copyright Legislation
  Copyright protection is an area of European regulation that is both more diffuse than the other areas considered, in that there is not a single over-arching Directive to consider, and the Directives are more stable in the sense that they have not been subject to major revision over recent years.

In addition to providing analysis and commentary on matters of law, this report also provides some introductory material, which examines the broad legal context within which modern legislators are operating. To this end, there is discussion of a number of conventions such as:

- The Paris Convention for the Protection of Industrial Property (1883)
- Berne Convention for the Protection of Literary and Artistic Works (1886)
- Universal Declaration of Human Rights (1948)
- European Convention on Human Rights (1950)
- Council of Europe Convention 108 (1981)

as well as influential state and national legislation such as:

- Hessisches Datenschutzgesetz (1970)
- Datalag (1973)

Extensive free-standing appendices will be produced to accompany this report, and will include full copies of the principal legislation under discussion, together with related material such as the Malmö Ministerial Declaration on eGovernment that sets out eGovernment practices up to 2015.

The intention is to provide in a single location many of the resources which practitioners may need to have available to navigate these three key areas. Somewhat against normal academic practice, extensive use is made of in-line quotation of the text of Directives and other regulatory instruments. These are generally placed directly alongside explanation and analysis. The purpose behind this approach is to simplify the process of using this report in practice, and to avoid the need to engage in "footnote hunting", a task often made particularly difficult for readers for whom English is not their first language.

5. Legal Context of European Data Protection Legislation & Regulation

Universal Declaration of Human Rights (1948)

EU legislation on Data Protection falls within Privacy and Human Rights law, and may be traced back directly to the United Nations' Universal Declaration of Human Rights.

Privacy is widely recognized as a fundamental human right, and has been protected under multinational privacy guidelines, directives and frameworks in different countries or conventions at international level. This process may be said to have begun in the immediate aftermath of the Second World. Motivated by a widespread desire to ensure that steps should be taken to avoid any future occurrence of the atrocities witnessed during that conflict, the 55th plenary meeting of the United Nations (11th December 1946) adopted a resolution on the report of the Joint First and Third Committee. The Assembly transmitted this to the Economic and Social Council "for reference to the Commission on Human Rights for consideration . . . in its preparation of an international bill of rights." The detailed work of drafting what would become the Universal Declaration of Human Rights undertaken by a formal drafting committee, consisting of 18 members from various political, cultural and religious backgrounds, under the chairmanship of Eleanor Roosevelt, widow of American President Franklin D. Roosevelt who was recognized as the driving force for the Declaration's adoption.

The first draft of the Declaration was proposed in September 1948 with over 50 Member States participating in the final drafting. By its resolution 217 A (III) of 10 December 1948, the General Assembly, meeting in Paris, finally adopted the Universal Declaration of Human Rights.

European Convention on Human Rights (1950)

The first instrument to give effect and binding force to certain of the rights stated in the Universal Declaration of Human Rights was the Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights. This was signed in Rome on 4th November 1950 by 12 Member States of the Council of Europe and entered into force on 3 September 1953.

This was also the first treaty to establish a supranational organ to ensure that the signatory states[6] fulfilled their undertakings. The Convention has therefore come to be seen as a milestone in the development of international law. By accepting the principle that an international court could challenge legitimately decisions taken by national courts, nation states had conceded that human rights had precedence over national legislation and practice.

For the purposes of the current report Article 8 of the European Convention on Human Rights is of particular importance. It asserts:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the

[6] See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CM=8&DF=14/07/2015&CL=ENG for a full list of signatories.

country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[7]

In subsequent interpretation, The European Court of Human Rights has understood this article very broadly and has thereby given impetus to further Data Protection legislation.

Hessisches Datenschutzgesetz (1970)

The first special-purpose data protection law (Hessisches Datenschutzgesetz) was enacted in the German State of Hessen in 1970. Its purpose was to protect all digitized material of public agencies within their responsibilities against disclosure, misuse, alteration or deletion by civil servants. The aim was not to set special terms for the obtaining and storage of personal data. However, if personal data became part of an official document they had to be accurate; if not, the data-subject was granted the right to rectification. A key innovation was to create an independent data protection office tasked with upholding the confidential handling of citizens' data. This continues to be a feature of European data protection legislation today.

Datalag (1973)

The first national law regulating automated data processing was the Swedish Datalag (Data Act) of 11th May 1973. This came about as the result of public concern arising out of the public census of 1969.

Mistrust centered not so much on the census itself as on the fact that, for the first time, much of the data gathering would be done in a form specifically designed to facilitate automated data processing.

In response, the Swedish government asked an official commission to report on the problems of computerized record keeping. This resulted in a report containing draft legislation for a comprehensive statute for the regulation of computer-based personal data systems in Sweden[8].

The key provisions were:

- The establishment of an independent "Data Inspectorate," charged with the responsibility for executing and enforcing the provisions of the Data Law.
- The requirement for automated data systems containing personal data to have a license from the Data Inspectorate.
- Data subjects were given the right to be informed about all uses made of the data about them
- No new use of the data was to be permitted without the consent of the data subject.
- Data subjects were given the right of access without charge to all data about them, and if the data were found to be incorrect, incomplete, or otherwise faulty, they must either be corrected to the subject's satisfaction, or a statement of rebuttal from the subject must be filed along with the data.
- The Data Inspectorate was empowered to act as ombudsman in all matters regarding automated personal data systems.

U.S. Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens (July 1973)

The international development of fair information practices, and data protection regulation, is widely regarded as being influenced by the Revelations about the surveillance activities of J. Edgar Hoover, and the activities of Richard Nixon during the Watergate period created a political context appetite for government

[7] http://www.hri.org/docs/ECHR50.html#C.Preamble

[8] Sweden, Justice Department, Data och integritet (Data and Privacy), Document SOU 1972:47 (Stockholm: Almänna Förlaget), 1972.

reform in the United States. Against this background, US Secretary of Health, Education, and Welfare, Elliot Richardson established, early in 1972, a Special Advisory Committee charged with analyzing the harmful consequences that might result from automated personal data systems, making recommendations about safeguards, and suggesting means of providing redress for any harm caused.

The committee submitted its final report "Records, Computers and the Rights of Citizens"on 31st July 1973.

The Report proposed a federal Code of Fair Information Practices for all computer systems. This Code of Fair Information Practices, now commonly referred to as Fair Information Practice Principles (FIPPs), established the framework on which much privacy policy would be built.

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual, to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[9]

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

In 1980, as a response to the increased transfers of personal data across national borders made possible by the growth of automatic data processing, the Organization for Economic Co-operation and Development (OECD) adopted a set of privacy guidelines. The guidelines were a revised version of the U.S. Department of Health, Education & Welfare Fair Information Practices (1973).

The guidelines are intended to provide an operational and policy framework to promote a consistent approach to dealing with transnational and international information security. Eight basic principles are set out in Part 2 of the OECD Guidelines[10]:

> **Principle 1 - Collection Limitation**
> "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[11]
> **Principle 2 - Data Quality**
> "Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."[12]

[9] Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July, 1973. Available online at https://www.epic.org/privacy/hew1973report/
[10] See http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[11] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Part 2, Sec. 7. Available online at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[12] Ibid. Part 2, Sec. 8

Principle 3 - Purpose Specification
"The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."[13]

Principle 4 - Use Limitation
"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law."[14]

Principle 5 - Security Safeguards
"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."[15]

Principle 6 - Openness
"There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."[16]

Principle 7 - Individual Participation
"An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."[17]

Principle 8 - Accountability
"A data controller should be accountable for complying with measures which give effect to the principles stated above." [18]

Laudable though the intention was, the OECD Guidelines were still nonbinding, and data privacy laws continued to vary widely across Europe. The United States endorsed the OECD recommendations but did

[13] Ibid. Part 2, Sec. 9
[14] Ibid. Part 2, Sec. 10
[15] Ibid. Part 2, Sec. 11
[16] Ibid. Part 2, Sec. 12
[17] Ibid. Part 2, Sec. 13
[18] Ibid. Part 2, Sec. 14

not implement them. However, the guidelines remain influential and can be said to form the basis of most information privacy legislation around the world.

They address credibly the basic issue of trying to balance the "fundamental but competing values" of "privacy and the free flow of information," and, in so doing, they set out reasonable baseline standards for protecting personal data. Their central tenet is that the collection and use of personal data must be limited, open, lawful and accountable, and they require personal data to be both secured, and reasonably accessible.

Council of Europe Convention 108 (1981)

During the 1960s and 70s the Council of Europe adopted a number of resolutions aimed at protecting personal data, culminating in 1981 with Convention 108, for the Protection of Individuals with regard to Automatic Processing of Personal Data[19]. The convention was the first legally binding international instrument in the data protection field. It deals with "automated personal data files and automatic processing of personal data in the public and private sectors."[20], and its purpose is:

> " … to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")[21].

The Council of Europe's explanatory report on Convention 108, opines that:

> "The preamble reaffirms the commitment of the signatory States to human rights and fundamental freedoms. Moreover, it acknowledges that the unfettered exercise of the freedom to process information may, under certain conditions, adversely affect the enjoyment of other fundamental rights (for example: privacy, non-discrimination, fair trial) or other legitimate personal interests (for example employment, consumer credit). It is in order to maintain a just balance between the different rights and interests of individuals that the convention sets out certain conditions or restrictions with regard to the processing of information. No other motives could justify the rules which the Contracting States undertake to apply in this field." [22]

The convention itself stipulates five conditions for personal data undergoing automatic processing. Data should be:

> "a. obtained and processed fairly and lawfully;
> b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
> c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
> d. accurate and, where necessary, kept up to date;
> e. preserved in a form which permits identification of the data subjects for no

[19] See http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[20] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Article 3(1)
[21] Ibid. Article 1
[22] Council of Europe, "Explanatory report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 1981, Page 13

longer than is required for the purpose for which those data are stored."[23]

Convention 108 also establishes four safeguards for individual data subjects, who shall be entitled:

> "a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
>
> b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
>
> c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;
>
> d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with."[24]

It also seeks to regulate the transborder flow of personal data.

> "1 The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
>
> 2 A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.
>
> 3 Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
>
> a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
>
> b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph."[25]

Convention 108 was a major inspiration for Directive 95/46/EC which aimed at spelling out and expanding on the principles it enshrines.

[23] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Article 5
[24] Ibid. Article 8
[25] Ibid. Article 12

Data protection reform

On the 25th January 2012, the European Commission announced formally its intention to carry out a comprehensive reform of the 1995 EU data protection rules to strengthen online privacy rights and boost Europe's digital economy. Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. It has been suggested that the introduction of a single law covering the whole of the European Union, would have the effect of doing away with the current fragmentation and resultant costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative is intended to help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe.

Trilogues

Before new regulations can be introduced, the agreement of the European Parliament, The Commission, and the Council of Ministers must be secured. At the time of writing, the text of the proposed new regulations on data protection is still being discussed in a series of informal tripartite meetings, which are known as trilogues.

Trilogues do not have a fixed format of representation but, depending on their content and purpose, may range from highly technical discussions, to very political discussions. Generally speaking, trilogues involve a rapporteur, a chairperson of COREPER I (see below), or the relevant Council working party assisted by the General Secretariat of the Council and representatives of the Commission. The purpose of this somewhat intricate arrangement is to try to secure widespread agreement on a package of amendments that will be acceptable to the Council and the European Parliament. Any agreement which is arrived at in trilogues remains entirely informal until it is approved formally within each of the three institutions.

COREPER

The 'Committee of the Permanent Representatives of the Governments of the Member States to the European Union' (COREPER) was established by Article 16 (7) of the Treaty on European Union and the Treaty on the Functioning of the European Union (2012/C 326/01), which lays down that :

> "a committee consisting of the Permanent Representatives of the Member States shall be responsible for preparing the work of the Council"[26].

The working of COREPER is spelled out in Article 240 of the Treaty on European Union and the Treaty on the Functioning of the European Union:

> " 1. A committee consisting of the Permanent Representatives of the Governments of the Member States shall be responsible for preparing the work of the Council and for carrying out the tasks assigned to it by the latter. The Committee may adopt procedural decisions in cases provided for in the Council's Rules of Procedure.
> 2. The Council shall be assisted by a General Secretariat, under the responsibility of a Secretary-General appointed by the Council.
> The Council shall decide on the organisation of the General Secretariat by a simple majority.

[26] Article 16 (7) of the Treaty on European Union and the Treaty on the Functioning of the European Union (2012/C 326/01)

> 3. The Council shall act by a simple majority regarding procedural matters and for the adoption of its Rules of Procedure."[27]

COREPER meets each week and is divided into two parts responsible for different EU legislation areas.

COREPER I, consisting of deputy permanent representatives from the EU Member States, prepares the ground for the following Council configurations:

- Employment, Social Policy, Health and Consumer Affairs;
- Competitiveness (internal market, industry, research and tourism);
- Transport, Telecommunications and Energy;
- Agriculture and Fisheries;
- Environment;
- Education, Youth and Culture (including audiovisual);

COREPER II, which consist of permanent representatives from the EU Member States, prepares for the other Council configurations:

- General Affairs Council;
- External Relations Council (including European security and defence policy and development cooperation);
- Economic and Financial Affairs (including the budget);
- Justice and Home Affairs (including civil protection).

Overall, COREPER monitors and coordinates the work of some 250 committees and working parties consisting of officials from the Member States who prepare the dossiers at technical level.

[27] Article 240 of the Treaty on European Union and the Treaty on the Functioning of the European Union:

6. Data Protection Law

Introduction

The new Data Protection proposals currently under consideration promise to introduce a number of fundamental reforms across the European Union, and, in some cases, extending to third countries. In the section which follows, we will consider each of the key areas where reform is planned. In each case, we will present, and analyse the current requirements as set out in Directive 95/46/EC28, followed by presenting and examining the regulations that are expected to replace them. Finally, some concluding remarks are offered.

In total, sixteen areas are examined, and these are considered in the order in which they appear in the text of the new proposals:

- General Jurisdictional scope
- Scope of personal data
- The Obligations and Liabilities of Data Controllers
- Lawfulness of processing
- The Right to be Forgotten
- Data Portability
- Automated Individual Decisions / Profiling
- Data protection officials/officers
- Data protection by design and by default
- Jurisdictional scope: Controllers not established in the Union
- The Obligations of Data Controllers and Data Processors
- Security of Processing
- Personal Data Breach Notification
- Transfer of personal data to a third country
- Legal enforcement & Penalties
- Administrative sanctions

[28] In some cases, Directive 95/46/EC makes no provision whatsoever. Where this is the case, it will be noted in the text.

General Jurisdictional scope (Article 3)

The proposed new regulatory arrangements will extend significantly the reach of the EU legislation, for the first time taking it clearly beyond Europe's borders.

Under the present scheme, the territorial scope of Directive 95/46/EC is set out in Article 4 Sections 1a, 1b & 1c:

> "1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; 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;
>
> (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
>
> (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."[29]

Taken together, this represents a somewhat complex set of tests for determining jurisdictional scope, and, in practice, it is not always simple to determine with certainty whether, and to what extent, a particular personal data processing activity falls within the territorial coverage of Directive 95/46/EC. Some of the issues have recently been explored in the Court of Justice of the European Union (CJEU)30, which in 2014 was asked to rule on matters arising out of a case originally brought in 2010, by Mr Costeja González against La Vanguardia Ediciones SL (a large circulation daily newspaper), Google Spain SL, and Google Inc. The complaint was based on the fact that users making a Google search on Mr Costeja González's name, had returned to them links to two pages of La Vanguardia on which Mr Costeja González's name appeared connected with the sale of a property for the recovery of social security debts. Mr Costeja González requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results. The case raised the question of what obligations are owed by operators of search engines to protect personal data, but also the matter of the territorial application of Directive 95/46/EC. The corporate structure of Google whose headquarters are located outside the EU, with only a subsidiary company based in Spain, might be argued to have left it outside EU regulation. Similarly, the possibility that Google's data processing activity was in fact taking place outside the EU, might also have implications on the extent to which it may be thought of being subject to the requirements of Directive 95/46/EC.

The CJEU was asked to rule (among other things) on whether Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an

[29] Article 4(1a,1b &1c) "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"
[30] See http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065

establishment of the controller on the territory of a Member State, within the meaning of that provision, when one or more of the following three conditions are met:

> "the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State, or
>
> the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking, or
>
> the branch or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to protection of personal data, even where such collaboration is engaged in voluntarily." [31]

Clarification was also sought as to whether Article 4(1)(c) must interpret as a 'use of equipment situated on the territory of the said Member State',

> "when a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in that Member State, or when it uses a domain name pertaining to a Member State and arranges for searches and the results thereof to be based on the language of that Member State?"[32]

The court's decision, as far as it related to the territorial scope of Directive 95/46/EC, was that:

> "Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State."[33]

The new proposals (Article 3) simplify the existing arrangements:

> "1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.
>
> 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
> (a) the offering of goods or services to such data subjects in the Union; or
> (b) the monitoring of their behaviour.

[31] para 44, Judgment of the Court (Grand Chamber), Case C 131/12, 13 May 2014
[32] para 20, section b, op.cit.
[33] Ruling 2, op.cit.

> 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law."[34]

Thus, under the new regime, processors of personal data will fall under the regulations. The old "means" and "equipment" tests are abandoned, concentrating instead on whether non-EU controllers are providing goods/services to data subjects in the EU, or are monitoring their behaviour. Recital 20[35] of the Council's agreed text spells this out further:

> "In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services, irrespective of whether connected to a payment or not, to such data subjects, or to the monitoring of such data subjects. In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging the offering of services to data subjects in one or more Member States in the Union."[36]

The new proposals have, however, left some potential for legal uncertainty arising from a lack of clarity about the meaning and scope of terms such as "offering", "only occasionally", "monitoring" and "main establishment".

[34] Article 3, Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012

[35] In Law generally, a recital (from the Latin word recitare, meaning: to read out) consists of an account or repetition of the details of some act, proceeding or fact. In EU law, a recital is a text that sets out reasons for the provisions of an act, while avoiding normative language and political argumentation.

[36] Recital 20, op.cit.

Scope of personal data (Article 4)

For the purposes of Directive 95/46/EC 'personal data' is defined as:

> "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"[37]

This somewhat generic definition needs to be read alongside Recital 26 of the Directive, which states that "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person".

Under Article 29 of Directive 95/46/EC, an independent and advisory working party on the "Protection of Individuals with regard to the processing of Personal Data and on the free movement of such data " was established. It is generally known as the "Article 29 Working Party"[38]. It comprises, a representative of the supervisory authorities designated by each EU country; a representative of the authorities established for the EU institutions and bodies; and a representative of the European Commission.

The remit of the Article 29 Working Party is to

> "To provide expert opinion from member state level to the Commission on questions of data protection.
>
> To promote the uniform application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities.
>
> To advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy.
>
> To make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community."[39]

The Article 29 Working Party is generally considered to provide the best guidance on personal data, and its "Opinion 4/2007 on the concept of personal data"[40], sets out a very broad interpretation of personal data. Working from the definition given in Directive 95/46/EC, the Article 29 Working Party opines that four questions must be answered before a determination may be made whether something counts as 'personal data':

1. Is it information?

[37] Article 2(a) "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"
[38] See http://ec.europa.eu/justice/data-protection/article-29/index_en.htm
[39] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/tasks-art-29_en.pdf
[40] http://bit.ly/1HgYcFs

2. Does it relate to a person?
3. Is that person identified or identifiable?
4. Is the person a living natural person?[41]

The working party's broad view of what constitutes personal data is widely supported by the Member States. However, there is some divergence of opinion. For example, UK's implementation relatively idiosyncratic implementation of Articles 2, 3, 8, 10, 11, 12, 13, 22, 23, 25 and 28 has led the Commission to investigate the UK's interpretation. Courts in Italy and France have taken decisions on the status of IP addresses as personal data, which are at odds with their Austrian, Swedish, and Spanish counterparts. As with many other aspects of the current regulatory system, there is an uneven approach to the national implementation of Directive 95/46/EC.

The new proposals are expected to establish a single broad definition of personal data for the whole of the EU. The current text defines 'personal data' to mean "any information relating to a data subject"[42]

In turn, a data subject is understood as meaning an:

> "identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person"[43]

It is important to note that 'identification' will henceforward depend on the likelihood of "singling out" an individual directly or indirectly[44], rather than being limited to the possibility of knowing details such as the name and address of a particular individual. Recital 23 explicitly states that "The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.", but it may be expected that some divergence of opinion will emerge as to the precise circumstances under which data subjects are 'no longer identifiable'. However, the clear intention is that the new regulations should not apply to activities such as the processing of anonymous data, including for statistical and research purposes.

Another point worth noting is the reference to 'online identifiers'. This would certainly include the use of cookies, web beacons, IP addresses and other technologies used to track specific users. It will be interesting to see how the Court will treat data processing that is entirely client side, and does not feed information back to the server but filters how the information sent from the server is handled by the client.

The general approach which is emerging from the discussions around the draft text of the new regulations shows an appetite to understand 'personal data' in the same broad way as the Article 29 Working Party treats the same nation under Directive 95/46/EC. In Member States, such as the UK, which are currently working under a more restrictive interpretation of 'personal data', the new rules are likely to require a much greater change in business practice to ensure compliance than in countries whose interpretation has

[41] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Adopted on 20th June 2014, pp.6-23
[42] Article 4(2), "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012
[43] Article 4(1), op.cit
[44] Recital 23 op.cit.

been closer to the Article 29 Working Party approach. In all cases, it will be prudent to take a very conservative approach to the collection, processing, and retention of personal data. Only the minimum data should be handled; data should be assumed to be personal unless there are clear grounds for believing otherwise; personal data should be held only for the minimum time required mindful of the purpose for which it is being held and processed; organisations should be able to demonstrate an audit trail showing that data no longer held has been securely deleted; where possible data should be anonymised.

The Obligations and Liabilities of Data Controllers (Articles 5,11,12,14,18,22,23,24,26,28,30,31,33,77)

The new data protection regulations pay considerable attention to obligations and liabilities of Data Controllers. Under Directive 95/46/EC a controller is understood to:

> "mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;"[45]

This understanding of what it means to be a data controller was substantially drawn from the Council of Europe's Convention 108, but there were a number of modifications made from the earlier concept of the 'controller of the file"[46] involved in "processing of personal data"[47]. Within the understanding of Directive 95/46/EC, processing is held to be:

> "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[48]

This notion is clearly much more far-reaching than is captured by 'file' and covers activities reflecting the full life cycle of information from its collection to its destruction. Consequently, it was necessary to expand the notion of 'controller of the file' to reflect the wider and more dynamic role required from them.

Other important changes introduced in Directive 95/46/EC were:

- the notion of pluralistic control ("either alone or jointly with others")
- the requirement that the controller should "determine the purposes and means of the processing of personal data"
- the notion that this determination could be made by national or Community law or in another way.
- The introduction of the concept of 'processor', which is not mentioned in Convention 108.

Article 4 (5) of the new proposals provides a slightly modified notion of 'controller', which is now understood as:

> "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the

[45] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Art 2(d).
[46] This was defined in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Article 2(d) as a "…natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them."
[47] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Article 1
[48] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Art 2(b).

> processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law"[49]

Article 5 sets out the principles that relate to personal data processing. Personal data must be:

> "(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
> (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;
> (d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;"[50]

These correspond almost exactly to the provisions set out in Article 6 (1) of Directive 95/46/EC. Echoing Article 2 of the same Directive, all of this falls under:

> "the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation."[51]

Article 11 of the proposed new regulations lays out a number of rights of the data subject, and following the proposals to be found in the 2009 Madrid Resolution[52], introduces the obligation on controllers to provide transparent and easily accessible and understandable information:

> "1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.
>
> 2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information

[49] "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012. Article 4 (5). ,
[50] Ibid. Article 5 (a – e).
[51] Ibid. Article 5(f)
[52] International Conference of Data Protection and Privacy Commissioners, "International standards on the protection of personal data and privacy." 5th November 2009, Section 16 "Right of Access".

addressed specifically to a child."[53]

Article 12 places an obligation on controllers to provide procedures and mechanisms to ensure data subjects can exercise their rights:

> "1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.
>
> 2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.
>
> 3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.
>
> 4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request."[54]

Building on Articles 10 and 11 of Directive 95/46/EC, Article 14 of the new proposals specifies more fully the obligations of data controllers to provide information to data subjects. These include providing additional information on the storage period, the right to lodge a complaint, in relation to international transfers and to the source from which the data are originating. In section 5, the derogations provided by Directive 95/46/EC are carried over into the new proposals:

> "1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:
>
> (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;

[53] "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012. Article11

[54] Ibid. Article 12

(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
(c) the period for which the personal data will be stored;
(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;
(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
(f) the recipients or categories of recipients of the personal data;
(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;
(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.

3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.

4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:
(a) at the time when the personal data are obtained from the data subject; or
(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.

5. Paragraphs 1 to 4 shall not apply, where:
(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or
(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or
(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or
(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.

6. In the case referred to in point (b) of paragraph 5, the controller shall provide

appropriate measures to protect the data subject's legitimate interests."[55]

Article 18 introduces the data subject's right to data portability. Within this context, it provides the rights both to obtain those data from the controller, and to have them provided in a structured and commonly used electronic format.

"1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.
2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn."[56]

Article 22 describes in detail the obligation of responsibility of the controller to comply with the "principle of accountability" and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance.

"1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. The measures provided for in paragraph 1 shall in particular include:
(a) keeping the documentation pursuant to Article 28;
(b) implementing the data security requirements laid down in Article 30;
(c) performing a data protection impact assessment pursuant to Article 33;
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);
(e) designating a data protection officer pursuant to Article 35(1).

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises."[57]

Article 23 sets out the obligations of the controller arising from the principles of data protection by design and by default:

[55] Ibid. Article 14
[56] Ibid. Article 18
[57] Ibid. Article 22

> "1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
>
> 2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals."[58]

Article 24 clarifies the responsibilities of joint controllers both as regards their internal relationship, and towards the data subject:

> "Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them."[59]

Article 26, which is based partly on Article 17(2) of Directive 95/46/EC, clarifies the position and obligation of processors. It furthermore adds new elements, including that a processor who processes data beyond the controller's instructions is to be considered as a joint controller.

> "1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.
>
> 2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:
>
> (a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;
> (b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
> (c) take all required measures pursuant to Article 30;
> (d) enlist another processor only with the prior permission of the controller;
> (e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational

[58] Ibid. Article 23
[59] Ibid. Article 24

> requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
> (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;
> (g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;
> (h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.
>
> 3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.
>
> 4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24."[60]

Article 28 obliges controllers (and processors) to maintain documentation of the processing operations under their responsibility, and sets out the documentation format required. This replaces the general requirements set out in Articles 18(1) and 19 of Directive 95/46/EC to "notify the supervisory authority…. before carrying out any wholly or partly automatic processing operation"[61]:

> "1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.
> 2. The documentation shall contain at least the following information:
> (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
> (b) the name and contact details of the data protection officer, if any;
> (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
> (d) a description of categories of data subjects and of the categories of personal data relating to them;"[62]

Article 29 clarifies the obligations of the controller and the processor for the co-operation with the supervisory authority.

> "1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.
>
> 2. In response to the supervisory authority's exercise of its powers under Article 53(2),

[60] Ibid. Article 26

[61] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article 18(1)

[62] "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012. Art 28

> the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority."[63]

Article 30 places both the controller and the processor under an obligation to implement appropriate measures for the security of processing. This is based on Article 17(1) of Directive 95/46/EC, the principal change being to extend that obligation to processors, irrespective of the contract with the controller.

> "1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
>
> 2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.
>
> 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.
>
> 4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:
>
> (a) prevent any unauthorised access to personal data;
>
> (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;
>
> (c) ensure the verification of the lawfulness of processing operations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)."[64]

Article 31 introduces an obligation on controllers to notify supervisory authorities of personal data breaches, building on the personal data breach notification in Article 4(3) of the e-privacy Directive 2002/58/EC.

> "1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.

[63] Ibid. Article 29
[64] Ibid. Article 30

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.

3. The notification referred to in paragraph 1 must at least:
(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;
(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;
(c) recommend measures to mitigate the possible adverse effects of the personal data breach;
(d) describe the consequences of the personal data breach;
(e) describe the measures proposed or taken by the controller to address the personal data breach.

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)."[65]

Closely related to Article 31, Article 32 places controllers under an obligation to notify personal data breaches to data subjects.

"1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).
3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any

[65] Ibid. Article31

person who is not authorised to access it.
4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.
6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)."[66]

The Article 32 requirements build on the similar obligations set out in Article 4(2) of the e-privacy Directive 2002/58/EC:

> "In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved."[67]

Article 33 introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations.

> "1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
>
> 2. The following processing operations in particular present specific risks referred to in paragraph 1:
>
> (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;
> (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;
> (c) monitoring publicly accessible areas, especially when using optic-electronic

[66] Ibid. Article32
[67] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Article 4(2)

devices (video surveillance) on a large scale;
(d) personal data in large scale filing systems on children, genetic data or biometric data;
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities."[68]

Article 77 sets out the right to compensation and liability. It builds on Article 23 of Directive 95/46/EC, extends this right to damages caused by processors and clarifies the liability of joint controllers and joint processors.

"1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.
2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.
3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage."[69]

Lawfulness of processing (Article 6)

Within the scope of Directive 95/46/EC, Member States are required to ensure that:

"personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

[68] "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012. Article 33
[69] Ibid. Article 77

> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
>
> (d) processing is necessary in order to protect the vital interests of the data subject; or
>
> (e) processing 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; or
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).;"[70]

Additionally:

> "it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. "[71]

This provision comes with certain qualifications concerning, for example, cases where processing is necessary to protect the vital interests of the data subject or for the purposes of preventive medicine and medical diagnosis:

> "(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
>
> (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
>
> (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
>
> (d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a

[70]Article 7, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"
[71] Ibid. Article 8(1)

third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed."[72]

The new proposals are based directly on those in Article 7 of Directive 95/46/EC, and are left broadly unchanged. However, there are some adjustments included with the intention of specifying more clearly the balance of interest criterion, and the compliance with legal obligations and public interest:

"1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject;
(e) processing 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;

[72] Ibid. Article 8(2-7)

> (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.
>
> 2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.
>
> 3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:
> (a) Union law, or
> (b) the law of the Member State to which the controller is subject. The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.
>
> 4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.
>
> 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child."[73]

While these adjustments will for many Member States require almost no alteration to their current practice, some states, such as the UK who have been operating more permissively, will require some adjustment to their business practice.

One area where a significant tightening of the rules will take place is the regime for obtaining valid consent. In Article 7 the new rules are laid out:

> "1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.
> 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.
> 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
> 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller."[74]

[73] "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012. Article 6(2)
[74] Ibid. Article 7(1)-(4)

Once again, the impact these amendments will have in individual Member States, will depend on the extent to which their current national legislation takes a stricter or more lenient position on consent.

The Right to be Forgotten (Article 17)

Article 1 of Directive 95/46/EC, defines blocking, erasure or destruction of data as classes of 'data processing' , and the Direction spells out the right of data subjects to have data concerning them erased, as well as the restrictions which might apply to that right, in Articles 12, 13, 28, and 32.

Under Article 12, which deals with the 'Right of Access', the Directive stipulates that national legislation should be enacted which ensures that data subjects may (on request) be given clear information on the data held on them by data controllers, the purposes to which it is being put, to whom it is being disclosed, and the source(s) from which it is gathered. Armed with this information data subjects are further entitled to have inaccurate or incomplete data erased or blocked. Article 12 lays out the general position as follows:

> "Member States shall guarantee every data subject the right to obtain from the controller:
> (a) without constraint at reasonable intervals and without excessive delay or expense:
> — confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
> — communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, — knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);
> (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
> (c) notification to third parties to whom the data have
> been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort."[75]

Article 13 attenuates these rights, permitting Member States to include in national legislation restrictions under seven general headings. The first six of these cover what may be loosely termed 'national interest'. The seventh permitted restriction allows for data subjects to be denied access to data held about them, or the right to have such data amended, to protect their own interests, or to protect the rights and freedom of other data subjects:

> "1 . Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard :
> (a) national security;
> (b) defence;
> (c) public security;
> (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
> (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

[75] Article 12, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"

> (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
> (g) the protection of the data subject or of the rights and freedoms of others .
>
> 2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistic."[76]

The Article 13 (g) restriction provisions are somewhat odd. Not only do they concern two distinct cases; one concerning the interests of the data subject, the other concerning third party data subjects, but it calls for a balance to be struck between the interests of different data subjects. Examples of the sort of competitive interests are not given, but one could easily imagine a job candidate asking for access to the contents of the confidential references provided by their referees. The argument for having access to this material is clear, as is the motivation for wanting to ensure that the information in question is both accurate and complete. However, people supplying confidential references have a reasonable expectation that their comments should remain confidential between themselves and the potential employer, particularly where they are expressing themselves candidly. Not every member state has thought it appropriate to implement directly or fully the Article 13 restrictions. For example, in the opinion of the Netherlands legislature, the Directive 95/46/EC principles are expressed flexibility enough already, without needing separate provision to made for restrictions. Overall, while there is widespread agreement on the need to protect data subjects, national laws diverge quite considerably, both in scope and in the tests applied.

There is widespread agreement that under the new proposals there should be provision made for the right to be forgotten, and, significantly, that search engines should be brought under the scope of the regulation. The general principles are spelt out in Recital 53 of the new proposals:

> "Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where

[76] Ibid. Article 13

there is a reason to restrict the processing of the data instead of erasing them."[77]

Recital 54 places on data controllers, who have made personal data publically available, an obligation to take all reasonable steps to ensure that third parties erase that data, or otherwise make it inaccessible, when circumstances require it:

> "To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party."[78]

The details of the 'right to be forgotten and erasure' are covered in nine sections of Article 17:

> "1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
> (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
> (c) the data subject objects to the processing of personal data pursuant to Article 19;
> (d) the processing of the data does not comply with this Regulation for other reasons.
>
> 2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.
>
> 3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:
> (a) for exercising the right of freedom of expression in accordance with Article 80;
> (b) for reasons of public interest in the area of public health in accordance with Article 81;
> (c) for historical, statistical and scientific research purposes in accordance with Article

[77] Recital 53, "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012
[78] Ibid. Recital 54

83;
(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;
(e) in the cases referred to in paragraph 4.

4. Instead of erasure, the controller shall restrict processing of personal data where:
(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;
(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;
(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;
(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.

7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:
(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;
(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;
(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4."[79]

It is clear that while, under the new regulations, data subjects are set to enjoy the right to be forgotten, this right is by no means unrestrained. Data controllers will be required to attenuate the right to be forgotten against, particularly, the right to freedom of expression when determining whether to accede to removal requests. Controllers will also have the option to 'restrict processing' of contested data rather than to remove it completely, but, in practice, the burden imposed on data controllers by expecting them to balance the right to be forgotten against the right to freedom of expression, and deciding whether it is

[79] Article 17, op.cit.

more appropriate to restrict processing or to complete erase data, is likely to be severe. This is, if anything exacerbated by cascading this responsibility down to secondary controllers.

The tension that exists between, on the one hand, society's right to remember, and on the other, an individuals' right to be forgotten, is of particular interest for the E-ARK project. Among those who have a responsibility for maintaining the authenticity of records is must be a ground for concern that rectification of inaccurate, incomplete, or just plain embarrassing data, will undermine authenticity. It is not yet clear that legislators have taken on-board this concern.

Data Portability (Article 18)

A completely new feature in the new proposed regulations, and one that has been the subject of much debate, is the concept of data portability. This notion, which has only really been discussed since around 2007, centres on interoperability, and may broadly be understood as giving data subjects the ability to ask for and receive their data in a re-usable format. Data subjects may, thereafter be able to move their personal data from one data controller to another without hindrance from the original data controller. In other contexts, this would amount to ensuring that 'vendors cannot impose 'customer lock-in', but in the context of data protection it is difficult to see how this model applies in the data protection arena. Nevertheless, it appears certain that, in one form or another, the right to data portability will feature in the final version of the new regulations.

Data portability is covered in three Recitals (59, 130, & 131) and in Article 18:

> "1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.
>
> 2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.
>
> 3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)."[80]

The right granted under Article 18 (1) is potentially weakened by the introduction of the clause "commonly used format". This leaves the question of what is to be understood by "commonly used" open, and also opens up the possibility of data controllers being able to claim an exemption if the format in which they process data is in some sense "uncommon". In Article 18 (3) this is addressed to some extent by granting the Commission the right to specify the format. It is perhaps worth noting that Article 18 (3) appears only to concern itself with the format of the transferred data, and the modalities of the transfer process, but not the format in which data controllers choose to process the data in the first place. It is this latter consideration which will determine whether or not data subjects have a right under "data portability".

Recital 59 outlines the general framework under which the right to data portability (and other rights) may be restricted:

> "Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data

[80] Article 18, "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012

> breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms."[81]

Recital 130, anticipating Article 18 (3), stipulates that the Commission should be empowered to specify "standard forms and procedures" in relation t the right of data portability:

> "In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; … Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers45. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises."[82]

Finally, Recital 131 stipulates that:

> "The examination procedure should be used for the adoption of specifying standard forms in relation to … standard forms and procedures in relation to … the right to data portability…"[83]

There remains considerable debate over the provisions for data portability, whether they would not sit more appropriately under competition law, and what limitations may apply. Undoubtedly, compliance with the regulations in their current form would impose on businesses a significance cost burden. The extent to which this is justifiable, particularly in the absence of any real evidence of "customer lock-in", is questionable. While we may be reasonably confident that data portability, in some form, will feature in the final version of the new regulation, it is far from clear what that form will be.

[81] Ibid. Recital 59
[82] Ibid. Recital 130
[83] Ibid. Recital 131

Automated Individual Decisions / Profiling (Articles 19 & 20)

The final shape of the proposals on Automated Individual Decisions or Profiling is harder to discern than with other areas of the new regulations. Opinions are still very divided, and the outcome of the discussions are likely to have profound effects on key areas of the European economy such as advertising, and insurance provision, where customer (or potential customer) profiling is a vital tool.

Under the current regime, Directive 95/46/EC does not deal in any great depth with Automated Individual Decisions:

> "1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
>
> 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
>
> (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
>
> (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests."[84]

While at first glance this would appear substantially to protect individuals from automated profiling, the conditions that are applied to the rights weaken considerably the level of protection that is, in practice, available. In those cases where automated decision-making is based, however slightly, on criteria other than on the, largely unspecified, "certain personal aspects relating to him", no protection whatsoever is afforded by the Directive. Similarly, where Clause 2(a) speaks of "suitable measures to protect his legitimate interests", it is not spelled out what would count as "suitable or "legitimate", omissions which could, in practice, result in a considerable diminution of the protection which the Directive purports to provide. It is worth noting the extent to which the growth in the use of 'big data' and 'data-mining' techniques has left the Directive's provisions looking somewhat dated.

Under the new proposals, key to protecting the rights of data subjects is Article 11, which deals with information transparency and communication:

> "1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.
> 2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and

[84] Article 15, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"

> plain language, adapted to the data subject, in particular for any information addressed specifically to a child."[85]

There is some discussion going on at present as to whether this article may be removed from the final version of the regulation. However, any diminution of this provision runs the risk of leaving data subjects in a position where they are denied their rights because they are unable to understand what rights they have.

Recital 51 sets out that:

> "Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject."[86]

And in so doing, is fully in accord with the Article 11 intentions. Profiling is covered in a number of other Recitals, including Recital 58, which lays out some of the circumstances in which a data subject's right to free of profiling might be limited:

> "Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child."[87]

Further limitations are addressed in Recital 59, where in addition to introducing a number of "public security" exemptions, exceptions of the grounds of "economic or financial interest" are also laid out:

> "Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated

[85] Article 11, "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012
[86] Ibid. Recital 51
[87] Ibid. Recital 58,

> professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms."[88]

In the main body of the proposed regulation, the whole of Section 4 is given over to the Right to Object and Profiling. Article 19 provides the right to object to the processing of personal data, but also undermines its own effectiveness by providing an exemption based on poorly spelled out "legitimate grounds". Article 19 does not offer any redress to data subjects other than the reassurance that processing successfully objected to, will no longer be carried out. This, however, does not address any harm which may have arisen from processing which has already taken place. For example, if an application for medical insurance was denied as the result of inappropriate automated profiling, and the data subject subsequently developed a medical condition which would have been covered by the policy for which they were applying. The assurance that the profiling in question would not happen again, would not restore to the data subject their lost cover – now unobtainable elsewhere because of the existence of the (newly developed) prior illness. The text of Article 19 is as follows:

> "1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.
>
> 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.
>
> 3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned."[89]

Article 20, turns directly to Measure based on profiling, and Section (1) grants that:

> "1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour."[90]

Section 2 of Article 20, concerns exceptions to this right. Of concern is the vagueness of the expression "suitable measures" in Section (2b), which does much to undermine Section 1. This terminology represents a sort of 'catch-all' under which a great deal that may not be immediately recognisable in one Member

[88] Ibid. Recital 59
[89] Ibid. Article 19
[90] Ibid. Article 20 (1)

State as a "suitable" measure to protect the interests of data subjects may be offered in an another as a justification for permitting profiling to be carried out.

> "2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:
>
> (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or
> (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards."[91]

As indicated at the start of this section, it is not yet possible to have any clear idea what the final shape of the new regulations will be with respect to profiling. A balance needs to be struck between proving, on the one hand, rights for data subjects to object to automated profiling, and on the other the interests of businesses who depend for the viability on being able to 'target' audiences, or discriminate between potential customers. What that balance will look like is by no means clear.

[91] Ibid. Article 20 (2)

Data protection officials/officers (Articles 22 & 35)

Under Article 18 of Directive 95/46/EC Member States may be granted a simplification of, or complete exemption from the usual notification requirements, if they data protection official to ensure internal data protection compliance and to keep a register of processing operations.

> "Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:
> - where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or
> - where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
>
> - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
> - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the procesing operations."[92]

Building on this, Article 22 of the proposed new regulations requires Controllers to introduce a data protection officer pursuant to Article 35 (1), which states:

> "The controller and the processor shall designate a data protection officer in any case where:
> (a) the processing is carried out by a public authority or body; or
> (b) the processing is carried out by an enterprise employing 250 persons or more; or
> the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects."[93]

The appointment of a Data Protection Officer represents a significant administrative, and cost overhead on businesses[94], in consequence of which, there has been a robust debate as to whether the new regulations should require them to be employed, or to permit organisations to continue with the current voluntary arrangements. Counter-proposals include limiting the mandatory appointment of a Data Protection Officer to cases where a certain threshold of data processing activity has been crossed in addition to limiting the

[92] Article 18 (2), "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"
[93] Ibid. Article 35 (1)
[94] The UK Ministry of Justice has estimated the cost (to the UK alone) of complying with the requirement for data controllers to employ data protection officers and carry out data protection impact assessments together at £130-£320 million p.a. in 2012/13 earnings terms. See Ministry of Justice Impact Assessment "Proposal for an EU Data Protection Regulation" 22nd November 2012. Available online at: https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf

requirement to public bodies and larger enterprises. It is simply not clear at this point how this particular aspect of the proposed new regulations will be resolved in the final text.

Data protection by design and by default (Article 23)

Privacy by Design (PdD) is an approach to systems engineering which promotes privacy and data protection compliance from the outset and involves the whole engineering process. It was pioneered during the 1990's by the former Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian. PbD is extremely useful for minimising security risks, and for establishing trust. It enables organisations to identify potential problems earlier than is otherwise possible, and by doing so lowers the cost of correcting problems before they have become difficult to address. By permitting a proactive approach to be taken to data protection, PbD also lowers the risk of failing to comply with data protection regulation, and lowers exposure to penalties for non-compliance.

A key element of a PbD approach is the 'privacy impact assessment', which is a tool which may be used to identify and reduce the privacy risks. Privacy by design works best when it is integrated into existing risk management approaches.

The Canadian Privacy by Design Centre of Excellence has produced seven 'foundational principles of privacy by design'[95] which illustrate clearly the general approach expected in a PbD system:

> "1. Proactive not Reactive; Preventative not Remedial
> The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. …. In short, Privacy by Design comes before-the-fact, not after.
>
> 2. Privacy as the Default Setting
> … Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact...
>
> 3. Privacy Embedded into Design
> Privacy is … an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
>
> 4. Full Functionality – Positive-Sum, not Zero-Sum
> … Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.
>
> 5. End-to-End Security – Full Lifecycle Protection
> … Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.
>
> 6. Visibility and Transparency – Keep it Open
> Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. … Remember, trust but verify.
>
> 7. Respect for User Privacy – Keep it User-Centric
> Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost …."[96]

[95] Abridged from: https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/
[96] See https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

When Directive 95/46/EC was produced, PbD had not yet reached a sufficient level of maturity and acceptance to be incorporated. However, in the years since there has been plenty of discussion about PbD, and it has featured in the thinking of both the Commission, and the Article 29 Working party. For example, in the Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU), there are a number of exhortations supporting PbD. For example, Member States are instructed to "support data controllers in developing and adopting Data Protection by Design and Data Protection by Default solutions enabling effective data protection." [97] Similarly, the Article 29 Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things, makes numerous mentions of PbD, including opining that "Every stakeholder in the IoT should apply the principles of Privacy by Design and Privacy by Default"[98]

In view of the upsurge of interest in PbD, it is not surprising to discover its inclusion in the new Data Protection proposals. PbD, which in this context is called 'Data protection by design and by 'default', attempts to ensure that when a user receives a product or service, privacy settings should be as strict as possible, without the user having to change them.

The new regulations require controllers to take responsibility for implementing PbD:

> "1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
> 2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals."[99]

These proposals fall some way short of capturing all seven of the Privacy by Design Centre of Excellence foundational principles, and reflect to some extent the debate which has been going on between the European Commission, Parliament and Council as to the scope and detail of the PbD requirements.

Nevertheless, it is clear that the new regulatory framework will require organisations to take full "account of developments in technology and solutions for privacy by design and data protection by default…"[100] and will no longer be satisfied to see privacy and security as something of a post hoc addition to products and processes.

[97] Article (6), Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU)
[98] Article 29 Data Protection Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things, Page 21
[99] Article 23, "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012
[100] Ibid. Article 30(3)

Jurisdictional scope: Controllers not established in the Union (Article 25)

Article 25 of the new regulatory system requires most non-EU data controllers to appoint representatives in the EU. The principal exceptions are for small enterprises and countries where the Commission deems there to be an adequate level of protection in place. The current version of the text is as follows:

> "Representatives of controllers not established in the Union
>
> 1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.
>
> 2. This obligation shall not apply to:
> (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or
> (b) an enterprise employing fewer than 250 persons; or
> (c) a public authority or body; or
> (d) a controller offering only occasionally goods or services to data subjects residing in the Union.
>
> 3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.
>
> 4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself."[101]

It is possible that by the time the final text of the regulations is agreed, non-EU processors conducting business within the EU, and processing EU data subjects' personal data will also be brought under the scope of the law.

Bringing non-EU controllers (and possibly non-EU processors) within the scope of the new regulation is one thing, but it will not be clear for some time after the introduction of the new rules whether it is possible, in practice, to enforce the rules. Some commentators have questioned whether sufficient resources will be available to enforcement agencies to bring to a successful conclusion prosecutions outside the geographical boundaries of the European Union. Nevertheless, the much more severe sanctions which regulators are likely to have at their disposal (up to 5% of annual global turnover) mean that in cases where the rules can enforced successfully, the consequences are potentially very serious indeed.

[101] Article 25. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"

The Obligations of Data Controllers and Data Processors (Articles 26-29)

Directive 95/46/EC has very little say on the direct obligations of processors. In Article 16, it speaks to their responsibilities with respect to confidentiality of processing:

> "Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law."[102]

In Article 17 (Security of Processing) we are told:

> "the processor shall act only on instructions from the controller"[103]

Most of the obligations mentioned in Directive 95/46/EC apply to data controllers, or are delegated to national legislation. Controllers must ensure that processors "must be governed by a contract or legal act binding the processor to the controller" [104], but the contacts serve for the most to merely echo obligations which apply directly to controllers. As with many other aspects of the implementation of Directive 95/46/EC, variations in the way in which different Member States implement the Directive in their own National legislation, give rise to a legal landscape that is somewhat inconsistent.

Under the proposed regulation Article 26 deals specifically with the obligations apply to data processors. Section 1 restates the Directive 95/46/EC requirement for the controller to obtain from processors 'sufficient' assurances that they can meet the obligations the regulations will require of them:

> "1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures."[105]

Section 2, places eight distinct obligations on data processors, ranging from the familiar Directive 95/46/EC obligation to act only under the direction of the data controller, through ensuring that their employees are placed under a statutory obligation of confidentiality, to ensuring they report properly to controllers:

> "2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:
> (a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;
> (b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

[102] Ibid. Article 16
[103] Ibid. Article 17 (3)
[104] Ibid. Article 17 (3)
[105] Article 26 (1), "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012

> (c) take all required measures pursuant to Article 30;
> (d) enlist another processor only with the prior permission of the controller;
> (e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
> (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;
> (g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;
> (h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article."[106]

Sections 3-5 round out the obligations of data processors as follows:

> "3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.
> 4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.
> 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting."[107]

Article 27 restates the Directive 95/46/EC Article 16 requirement for the processor to act only under the instructions of the controller:

> "The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law."[108]

Article 28 introduces a number of obligations to controllers and processors as to the documentation of processing operations:

> "1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.
> 2. The documentation shall contain at least the following information:
> (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
> (b) the name and contact details of the data protection officer, if any;
> (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
> (d) a description of categories of data subjects and of the categories of personal data

[106] Ibid. Article 26 (2)
[107] Ibid. Article 26 (3)-(5)
[108] Ibid. Article 27

> relating to them;
> (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;
> (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;
> (g) a general indication of the time limits for erasure of the different categories of data;
> (h) the description of the mechanisms referred to in Article 22(3).
> 3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority. "[109]

Two exemptions are also provided for:

> "(a) a natural person processing personal data without a commercial interest; or
> (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities" [110]

Finally, in Article 28, the Commission is given powers to specify further the documentary requirements, and lay down standard form for documentation:

> "5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.
> 6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)."[111]

Article 29, places obligations on both controllers and processors to co-operate with supervisory bodies, and to reply to them within a 'reasonable' period.

> "1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.
> 2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority."[112]

[109] Ibid. Article 28 (1)-(3)
[110] Ibid. Article 28 (4),
[111] Ibid. Article 28 (5)-(6)
[112] Ibid. Article 29

Further obligations are laid on controllers and processors with respect to “Security of Processing” under Article 30. Similarly, processors will have obligations to report personal data breaches to the data controller, and constraints will be placed on the content and format of such reports. Both controllers and processors will need to comply with the data export mechanisms set out in Article 40. These have been covered elsewhere in this report and will therefore not be restated here.

Altogether, the new regulations represent a fundamental rebalancing of liabilities, placing responsibilities directly on processors, which formerly were laid either on data controllers, or national legislatures. The net effect of all this is likely to be felt keenly by organisations all over the EU. The documentation requirements introduced in Article 28 will bring in their wake considerable new cost burdens on processors, and will, inevitably, expose them, under the new regime, to a much higher degree of risk than is currently the case under Directive 95/46/EC. The changes proposed will touch on most of the business cycle from procurement, through supply, into after sales activity; they will affect suppliers, contractors, and sub-contractors, each of whom will, in the future, have to take individual legal responsibility for their data processing activity.

Security of Processing (Article 30)

Recital 46 of Directive 95/46/EC requires controllers to ensure:

> ".. appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected"[113]

This is further spelled out in Article 17:

> "1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
>
> Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
>
> 2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
>
> 3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
>
> - the processor shall act only on instructions from the controller,
> - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
>
> For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form."[114]

How these measures are implemented in practice differs between the various Member States. It should be noted that the coverage of security in Directive 95/46/EC, is somewhat non-specific with little by way of detailed guidance. Under the new proposals "Security of Processing" is dealt with in Article 30, and while

[113] Recital 46. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"
[114] Ibid. Article 17

the Directive 95/46/EC approach is broadly repeated there is some movement in the direction of indicative compliance benchmarks:

> "1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
> 2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.
> 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.
> 4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:
> (a) prevent any unauthorised access to personal data;
> (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;
> (c) ensure the verification of the lawfulness of processing operations.
> Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)."[115]

[115] Ibid. Article 30

Personal Data Breach Notification (Articles 31 & 32)

Recital 46 of Directive 95/46/EC requires that:

> "appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected" [116]

It is left to individual Member States to determine the particular security measures which they deem "appropriate". As ever, this has led to some divergence in implementation of the Directive's intentions.

Article 22 asserts that a judicial remedy must be provided for breaches when they occur:

> "Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question."[117]

Directive 95/46/EC does not directly define personal data breaches. However Article 17 (Security of Processing) says that :

> "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."[118]

From which a definition might be inferred, and this does closely match the text of the Privacy and Electronic Communications Directive 2002/58/EC[119] which in Article 2 (i) defines a personal data breach as:

> "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."[120]

[116] Ibid. Recital 46
[117] Ibid. Article 22
[118] Ibid. Article 17
[119] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
[120] Ibid. Article 2 (i)

Directive 95/46/EC does not directly speak about the modalities of breach notification but, once again, Directive 2002/58/EC is more helpful, and requires such breaches to be notified to the competent national authority. In cases where the personal data breach is likely to affect adversely the personal data or privacy of a data subject, the data controller is also required to notify the data subject of the breach without undue delay[121].

The new proposals on Data Protection follow closely the scheme set out in Directive 2002/58/EC. They are contained in two Articles, the first of which, Article 31, covers Notification of a personal data breach to the supervisory authority:

> "1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.
> 2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.
> 3. The notification referred to in paragraph 1 must at least:
> (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;
> (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;
> (c) recommend measures to mitigate the possible adverse effects of the personal data breach;
> (d) describe the consequences of the personal data breach;
> (e) describe the measures proposed or taken by the controller to address the personal data breach.
> 4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.
> 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.
> 6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure

[121] This is understood to mean that notification to the authority should happen no later than 24 hours after the detection of the personal data breach, although this may, in some cases be extended to 72 hours. Similarly, notification to the data subject must be made without undue delay after the detection of the data breach. Notification to the data subject is not be dependent on the notification to the competent national authority.

referred to in Article 87(2)."[122]

Article 32, deals with communication of a personal data breach to the data subject:

> "1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.
> 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).
> 3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.
> 4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.
> 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.
> 6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)." [123]

While there may be some amendment of the precise time periods within which notification to the competent authority, and the data subject must take place, there is little doubt that the new regulations will require controllers and processors to make notification of breaches within a relatively short time. Mindful of the sanctions proposed for non-compliance these deadlines will need to be respected.

It will take some time after the new regulation comes into effect before it is clear whether this aspect of the new rules will be workable in practice. On the one hand, notification within 24-72 hours may prove to be too challenging, while on the other, concern over the possible consequences of found in breach of an obligation to notify may lead controllers/processors to err on the side of caution and notify so frequently that the system fails in practice.

[122] Article 31. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
[123] Ibid. Article 32

Transfer of personal data to a third country (Articles 39-45)

Directive 95/46/EC tries to harmonise the Member States' approach to transfers of personal data from their territories (i.e. from the territory of the Community) to other (so-called "third") countries.124 It permits the transfer of personal data to a third country, provided that this does not give rise to a diminution of the safeguards that would have been in place had the data remained wholly within the EC. Attention is therefore directed to ensuring that the level of protection, which is provided by third countries, is adequate.

The Council and the European Parliament have given the Commission the power to determine whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. It is the responsibility of Member States to ensure they comply with the decision of the Commission. Member States are required either to satisfy themselves that a sufficient protection exists, or to ensure that transfer of personal data to the third country is prevented. Member States are also given authority to work with third countries to improve the level of protection they offer.

These provisions are laid out in Article 25 of Directive 95/46/EC, which stipulates that:

> "1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
>
> 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
>
> 3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
>
> 4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
>
> 5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
>
> 6. The Commission may find, in accordance with the procedure referred to in Article

[124] Nevertheless substantial differences remain between the "applicable law" provisions in the laws of different Member States. For example, in respect of cross-border transfers, some Member States treat the non-EU EEA States (Iceland, Liechtenstein and Norway) exactly as they would EU Member States, while others regard them as "third countries".

> 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.
>
> Member States shall take the measures necessary to comply with the Commission's decision."[125]

In order to be recognized as complying with the Directive 95/46/EC requirements, a four-stage process must be followed:

> (1) a proposal must come from the Commission;
> (2) support must be received from the Member States' data protection authorities and the European Data Protection Supervisor, in the framework of the Article 29 Working Party;
> (3) approval must be obtained from the "Article 31 Committee", composed of representatives of Member States, under the comitology[126] "examination procedure";
> (4) the decision must be adopted by the College of Commissioners;

It is always open to the European Parliament and the Council to request that the Commission should maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the Directive.

When approval is obtained, personal data can be transferred from any of the Member States[127] to the third country in question without requiring any further safeguards. So far, very few 'third' countries have received approval: Andorra, Argentina, Canada, Eastern Republic of Uruguay, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, and Switzerland. Additionally, If the transfer is to the United States of America, it must be determined whether the US recipient of the data has signed up to the US Department of Commerce Safe Harbor Scheme[128]. The Safe Harbor scheme has hitherto been recognised by the European Commission as providing adequate protection for the rights of individuals in connection with the transfer of their personal data to signatories of the scheme in the USA but this is beginning to be called into question. For example on the 25th July the High Court of Ireland was asked for a preliminary ruling in the case of Maximillian Schrems v Data Protection Commissioner.[129]

The question at issue was:

> "Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the

[125] Article 25, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"
[126] Comitology in the European Union refers to a process by which EU law is modified or adjusted and takes place within "comitology committees" chaired by the European Commission.
[127] This allows applies to the three EEA member countries (Norway, Liechtenstein and Iceland)
[128] These adequacy decisions do not cover data exchanges in the law enforcement sector.
[129] Case C-362/14. At the time of writing (5th June 2015) no decision has been delivered.

> data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC1) having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union (2000/C 364/012), the provisions of Article 25(6) of Directive 95/46/EC3 notwithstanding?
>
> Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?"[130]

Article 26 of Directive 95/46/EC sets out:

> "1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:
>
> (a) the data subject has given his consent unambiguously to the proposed transfer; or
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
> (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
> (e) the transfer is necessary in order to protect the vital interests of the data subject; or
> (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case."[131]

It is worth noting that there are marked differences in how Member States treat the situation when neither the Commission nor their national authorities have yet determined the adequacy of the arrangements in place in third countries. For example, Austria, Greece, Portugal and Spain work on the basis that transfers of data to third countries are prohibited unless and until either the Commission or their national authorities have made a determination that the third country's arrangements are adequate. By contrast, the remaining Member States permit individual data controllers to make their own assessments in the absence of a ruling by the Commission or their national authorities.

It is expected that the new proposals will retain the look and feel of the current regulatory framework but

[130] See (http://bit.ly/1cBSqpi) or http://curia.europa.eu/juris/document/document.jsf?text=&docid=157862&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=318716

[131] Article 26, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"

with the addition of some clarification, and enhanced support for binding corporate rules, codes of conducts and seals. The new arrangements are contained in Articles 39-45 of the draft regulation[132]. The new process continues to rely on adequacy decisions based on determinations concerning the safeguards provided in third countries. In the absence of these, derogations are provided.

Article 40 lays out the general principle, which will govern international transfers:

> "Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation."[133]

Each of the next three articles deals in detail with a particular category of transfer, beginning with transfers with an adequacy decision:

> "1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.
>
> 2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:
> (a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and
> (c) the international commitments the third country or international organisation in question has entered into.
>
> 3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
>
> 4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of

[132] "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012
[133] Ibid. Article 40

paragraph 2.

5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).

6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.

7. The Commission shall publish in the Official Journal of the European Union a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.

8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission."[134]

Sole responsibility for establishing which countries have adequate safeguards in place, is currently envisaged as being given over to the Commission. Decisions of the Commission, once taken, continue to be subject to future revision and, when circumstances change, may be repealed, amended, or suspended. The general intention of the regulators to establish continuity with the spirit of Directive 95/46/EC is made very clear by indent 8.

Article 42, is concerned with transfers by way of "appropriate safeguards":

"1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.
2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:
(a) binding corporate rules in accordance with Article 43; or
(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in

[134] Ibid. Article 41

> Article 87(2); or
> (c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article
> 62(1); or
> (d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.
> 3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.
> 4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.
> 5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority."[135]

No reading of the Article 42 proposals, may be considered complete without taking into account Article 39, which sets outs suggestions for 'Certification':

> "1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.
> 2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.
> 3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing

[135] Ibid. Article 42

> acts shall be adopted in accordance with the examination procedure set out in Article 87(2)."[136]

There appears to be widespread support for the notion of a European Data Protection Seal, an idea originally introduced by way of an amendment by the European Parliament. Legal opinion seems to be that businesses will be able to transfer data more freely if both the EU-based data controller and the non-EU recipient have been granted a valid European Data Protection Seal.

Another way in which international transfers of personal data may take place, is under 'binding corporate rules'. These are internal rules, such as codes of conduct, adopted by multinationals, which set out their policy with regard to (in this case) international transfers of personal data within the corporation, to parts of the same corporation which are located in countries that do not provide an adequate level of protection. Binding corporate rules are used to help demonstrate that adequate safeguards[137] exist for the protection of the privacy and fundamental rights and freedoms of individuals.

Binding corporate rules are a way of ensuring that all transfers made within a group benefit from an adequate level of protection, and represent a less cumbersome alternative to requiring companies to sign standard contractual clauses each time a transfer needs to be made to a member of its own group. It should be noted that in order to be valid, binding corporate rules must be approved under the EU cooperation procedure, and are not considered to provide adequate protection for transfers made outside the corporation.

According to the European Commission, binding corporate rules make it possible to be in compliance with the principles set out in Articles 25 and 26, of Directive 95/46/EC for all internal data flows covered by the scope of the BCR, to:

> "harmonise practices relating to the protection of personal data within a group, prevent the risks resulting from data transfers to third countries, avoid the need for a contract for each single transfer, communicate externally on the company's data protection policy, have an internal guide for employees with regard to the personal data management, make data protection integral to the way the company carries out its business."[138]

Under the new proposals, Article 43 deals to the arrangements that are expected to govern transfers by way of binding corporate rules.

> "1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:
> (a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;
> (b) expressly confer enforceable rights on data subjects;
> (c) fulfil the requirements laid down in paragraph 2.
> 2. The binding corporate rules shall at least specify:

[136] Ibid. Article 39

[137] Within the meaning of Article 26(2) of Directive 95/46/EC "where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses."

[138] See http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

(a) the structure and contact details of the group of undertakings and its members;
(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
(c) their legally binding nature, both internally and externally;
(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;
(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;
(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;
(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;
(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;
(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;
(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.
4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2)."[139]

[139] Article 43 "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012

Eight grounds for derogation are set out in the first indent of Article 44. These, can briefly summed up as depending on the consent of the data subject, necessity of various kinds, and over-riding public or other third-party interest:

> "1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:
> (a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or
> (d) the transfer is necessary for important grounds of public interest; or
> (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or
> (f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or
> (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or
> (h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary."[140]

A further 6 indents provide general clarification of these grounds:

> "2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.
>
> 3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of

[140] Ibid. Article 44 (1)

personal data, where necessary.

4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.

6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1."[141]

The treatment of international transfers in the main body of the new proposals is brought to a close in Article 45, covers international co-operation for the protection of personal data, and places a number of responsibilities on the Commission, and other supervisory authorities:

"1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;
(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;
(d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3)."[142]

Overall, it is clear that the intention is that, with respect to the general principles for international transfers, the new regulation will build on the current framework. It is perhaps worth noting that the new rules are being extended to apply to processors and to onward transfers of personal data to third countries or international organisations. This will place a responsibility on organisations who are acting solely in the

[141] Ibid. Article 44 (2-7)
[142] Ibid. Article 45

capacity of data processors to be just as mindful of the rules which govern international data transfers, as data controllers. In both cases, significant penalties may be incurred for breaches of the regulations.

It is noteworthy that under the new proposals the Commission will have sole authority to determine which countries are deemed to provide adequate safeguards for personal data, and that decisions once taken will continue to be subject to being overturned or revised. There is general approval for the idea of a European Data Protection Seal, and this will be only one of a number of new mechanisms for certifying that data processing is adequately safeguarded. An important distinction has been drawn in the new proposals between safeguards (such as one-off contractual clauses) which will continue to require authorization from a data protection authority, and those (such as legally binding and enforceable instruments between public authorities) which will not, It is also worth highlighting that data transfer may, if the Council has its way, henceforward require explicit consent to count as valid.

Legal enforcement (Article 63) & Penalties (Article 78)

The current EC data protection regime has at its centre, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In common with all EC Directives, this does not regulate directly, nor does it mandate in detail the legal sanctions, which may be taken in the event of a breach, but instead places Member States under an obligation to put in place, using their own discretion, national regulation that reflects the principles laid out in the Directive. Consequently, the legislative frameworks in place across the EC Member States exhibit a wide degree of divergence from one another in they way they legislate to ensure data protection, and in the way they respond to data breaches.

Article 24 of Directive 95/46/EC is relatively vague on the subject of sanctions saying only:

> "The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive."[143]

Under the new General Data Protection Regulation proposals, the regime is set to become much clearer. Article 63 states:

> "1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.
> 2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable."[144]

Article 78, further stipulates:

> "Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.
>
> Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller.
>
> …Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them."[145]

[143] Article 24 "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"
[144] Article 63 "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012
[145] Ibid. Article 78

Administrative sanctions (Article 79)

In general, the available sanctions under Directive 95/46/EC, are relatively modest, particularly when compared to, say, laws on anti-competitive behaviour, where the UK is not untypical in legislating to allow company agreements to be declared unenforceable, together with a possible fine of 10% of group global turnover, and exposure to possible damages actions. Individuals may be disqualified from acting as company directors, and in particularly serious cases, may also face criminal charges.

Along similar lines, under Irish law, the operation of cartels was first made illegal in 1996. In 2007, an investigation into the activities of the Citroën Dealers Association, the Director of Public Prosecutions (DPP) brought criminal charges against 14 of the Association's members. One of the members was convicted and given a 15 month prison sentence, suspended for five years and fined €80,000 for his involvement in the cartel.

Under the Directive 95/46/EC regime, one of the most effective sanctions available to data regulators, in practice, is the threat of public censure, and consequent exposure to unfavourable publicity. In Article 79 of the new proposals a range of potential penalties are outlined ranging in severity from a cases where written warning

> "may be given and no sanction imposed, where:
>
> (a) a natural person is processing personal data without a commercial interest; or
>
> (b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities." [Art.79, Section 3]"[146]

to the more draconian measures set out in Article 9, Section 6:

> "The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:
> (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;
> (b) processes special categories of data in violation of Articles 9 and 81;
> (c) does not comply with an objection or the requirement pursuant to Article 19;
> (d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;
> (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;
> (f) does not designate a representative pursuant to Article 25;
> (g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;
> (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;
> (i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory

[146] Ibid. Article 79

authority pursuant to Articles 33 and 34;
(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;
(k) misuses a data protection seal or mark in the meaning of Article 39;
(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;
(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);
(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);"[147]

Originally, the commission proposed fines amounting to 2% of annual global turnover be imposed in the most serious cases, but that figure seems to have been abandoned in favour of these even more severe penalties. While it is too soon to say what sanctions regime will finally be agreed, it does seem clear that sanctions under the new scheme will be much greater than under Directive 95/46/EC, and will be set at a level which compels data holders to take very seriously the potential legal consequences of paying insufficient attention to (particularly) their corporate data protection responsibilities.

The Regulation also introduces a number of new governance requirements. The Commission's original text obliges data controllers to carry out impact assessments for certain higher-risk processing (Article 33). The EP's version only requires an impact assessment if a mandatory risk assessment (Article 32a) indicates any "specific" risk. These higher-risk areas include (in the EP's extended list): data processing relating to more than 5000 data subjects during any consecutive 12-month period; the processing of sensitive data; or processing operations which contain a risk by virtue of their nature. In some cases there is also a duty to consult the supervisory authority prior to the data processing (Article 34). The EP's version enables data controllers to carry out the prior consultation with the DPO (if there is one) instead of the supervisory authority. In addition, the EP's version obliges data controllers to assess the impact assessment on a regular basis, at least every two years. The Council's version, being more risk-based, requires a "high" risk to trigger the implementation by the controller of a mandatory personal data impact assessment, allowing certain leeway to supervisory authorities to determine a public list of processing operations not requiring an impact assessment, except in cases where it is expressly required by the Regulation. In terms of record-keeping and red tape, Article 28 of the Commission's draft proposes requirements for the controller and processor to document the detail of the processing. The Council's version is similar, while the EP's version of the Regulation is lighter-touch and has deleted several of these record-keeping duties.

[147] Ibid. Article 9(6)

Processing for historical, statistical and scientific research purposes (Article 83)

Under Directive 95/46/EC exemptions are provided for processing which is necessary intended for historical, statistical and scientific research purposes:

Recital 29 couches this is somewhat indirect terms:

> "Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual"[148]

Article 6(b) mandates that personal data may be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, but explicitly notes that:

> "Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards"[149]

Article 11, which deals with processing information where the data have not been obtained from the data subject, also provides an exemption:

> "for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards."[150]

The new proposals continue with the same permissive attitude towards processing for historical, statistical and scientific research purposes, as was evident under Directive 95/46/EC. They allow[151] (but do not require) Member States to introduce legislation relating to the processing of personal data concerning health. However processing which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred set out in Article 83, which mandates that personal data may be processed for historical, statistical or scientific research purposes only if:

> "(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;
> (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be

[148] Recital 29 "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". This is also taken up in Recital 40.
[149] Ibid. Article 6(b)
[150] Ibid. Article 11(2)
[151] Ibid. Article 81

fulfilled in this manner." [152]

Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if the data subject has given consent, and

> "the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or (c) the data subject has made the data public."[153]

[152] Article 83 (1) "Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels 25th Jan 2012

[153] Ibid. Article 83(2)

7. Law on the Re-use of Public Sector Information

Introduction

Public Sector Information (PSI) can be understood as the information that public sector bodies collect, produce, reproduce and disseminate in many areas of activity while accomplishing their institutional tasks. Examples include: "social, economic, geographical, weather, tourist, business, patent and educational information."[154]

Legal Background

The general approach to the re-use of Public Sector Information which was later evident in Directive 2003/98/EC, can be discerned clearly in the introduction to the so-called 'Synergy Guidelines' produced in 1989 by Commission of the European Communities, DG for Telecommunications, Information Industries and Innovation:

> "Governments and public sector bodies collect large amounts of data and information, as part of their routine functions, which could be made available to the private sector for the construction and marketing of electronic database services. The private sector is well placed to combine information from a variety of government sources, and its prime function is to produce and distribute information products oriented to the needs of the market. In order to develop and strengthen the information industry, a positive initiative is required from governments, to encourage the use and exploitation of public sector data and information. However, there are few convergent policies or guidelines within Member States relating to the role of the public sector in this area. In addition, if there are different policies operating in the different Member States, then it will be very difficult to develop the market. It is therefore desirable that national policies, as far as they exist, be coordinated at the Community level in order to allow the majority of the EC countries not yet having such a policy to follow these orientations on a national level."[155]

The Synergy Guidelines characterise the public sector as a producer of basic data and information, which may have commercial value for private industry:

> "Public administrations regularly and systematically collect basic data and information in the performance of their governmental functions. These collections have value beyond their use by governments, and their wider availability would be beneficial both to the public sector and to private industry. Public organizations should, as far as is practicable and when access is not restricted for the protection of legitimate public or private interests, allow these basic information materials to be' used by the private sector and exploited by the information industry through electronic information services."[156]

[154] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. Recital 4

[155] Guidelines for improving the synergy between the public and private sectors in the information market. Commission of the European Communities, DG for Telecommunications, Information Industries and Innovation. 1989

[156] Ibid. P.7

The emphasis throughout is on improving the performance of the European market (in this case the information market). There is, of course, a clear economic case which can be made for ensuring that European public expenditure directed at generating information materials is also utilised, where possible, to benefit European business. However given that European regulations generally prohibit State aid unless it is justified by reasons of general economic development the concentration is directed instead, as it must be, on improving the performance of the market, rather than trying to privilege directly European businesses.

Political and economic background

The public sector is the largest single producer of information in Europe and legislators had a clear appreciation of the potential for social and economic benefits if this information were to be made available for access and re-use. In order for this to happen, it was necessary to introduce clear policies and uniform practices in relation the re-use of public sector information. Furthermore, there was a perception that European firms involved in the aggregation of information resources into value-added information products were at a competitive disadvantage to their US counterparts. Among the reasons often cited for this was a lack of harmonisation of policies and practices among the EU Member States. This was seen a presenting an impediment to the development of information-based products and services based on information obtained from different countries. There were also problems arising from response times to requests for information, pricing, existing exclusive deals and an overall lack of transparency

This was the background against which Directive 2003/98/EC on the re-use of public sector information (known as the 'PSI Directive') was developed, and from its introduction on 31 December 2003, it provided a common legal framework for the European market for public sector information.

Directive 2003/98/EC on the re-use of public sector information

Directive 2003/98/EC deals with information held by public sector bodies at national, regional and local levels, as well as wholly or partly State-funded organisations or those coming under the auspices of public authorities (e.g. meteorological institutes). Written material, databases, and audio-visual material all fall within the scope of Directive 2003/98/EC, but, significantly for the E-ARK project, it does not apply to the educational, scientific, broadcasting, and cultural sectors.

While Directive 2003/98/EC encourages EU Member States to make as much public sector information available for re-use as possible, it does not oblige Member States to permit the re-use of documents. Rather, it only applies to documents that Member States have already made accessible. Directive 2003/98/EC provided a common legislative framework for this area, with the aim of removing barriers that hinder the re-use of public sector information throughout the Union.

The Directive claims to set out to establish:

> "a minimum set of rules governing the re-use and the practical means of facilitating reuse of existing documents held by public sector bodies of the Member States."[157]

It mandates that there should be clarity about any charges to be levied for re-use (with an explanation of basis of the charge being available on request) and places limits on charges, so that:

[157] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. Article 1

> "the total income from supplying and allowing re-use of documents shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment. Charges should be cost-oriented over the appropriate accounting period and calculated in line with the accounting principles applicable to the public sector bodies involved."[158]

It further stipulates the re-use of documents in a timely, open and transparent manner:

> "Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the timeframes laid down for the processing of requests for access to documents."[159]

Article 10 of Directive 2003/98/EC requires Member States to ensure the application of fair, consistent and non-discriminatory processes:

> "Any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use."[160]

Generally, the Directive frowns on the creation of exclusive arrangements:

> "The re-use of documents shall be open to all potential actors in the market, even if one or more market players already exploit added-value products based on these documents. Contracts or other arrangements between the public sector bodies holding the documents and third parties shall not grant exclusive rights."[161]

However, in those cases where an exclusive right must be granted it is required that the terms and conditions are made transparent:

> "… where an exclusive right is necessary for the provision of a service in the public interest, the validity of the reason for granting such an exclusive right shall be subject to regular review, and shall, in any event, be reviewed every three years. The exclusive arrangements established after the entry into force of this Directive shall be transparent and made public."[162]

Transparency must also exist with respect to the terms and conditions that apply to the terms, conditions and charges that are applied for re-use:

> "Any applicable conditions and standard charges for the re-use of documents held by public sector bodies shall be pre-established and published, through electronic means where possible and appropriate. On request, the public sector body shall indicate the

[158] Ibid. Article 6
[159] Ibid. Article 4
[160] Ibid. Art 10 (1)
[161] Ibid. Art 11 (1)
[162] Ibid. Art 11 (2)

> calculation basis for the published charge. The public sector body in question shall also indicate which factors will be taken into account in the calculation of charges for atypical cases. Public sector bodies shall ensure that applicants for reuse of documents are informed of available means of redress relating to decisions or practices affecting them."[163]

Furthermore, Directive 2003/98/EC, requires Member States to ensure that information, which is available for re-use, is readily identifiable as such:

> "Member States shall ensure that practical arrangements are in place that facilitate the search for documents available for reuse, such as assets lists, accessible preferably online, of main documents, and portal sites that are linked to decentralised assets lists."[164]

While it is true to say that Directive 2003/98/EC made considerable progress in establishing an EU-wide legal framework governing policies and practices relating to re-use of public sector information, it was not by any means the only EU initiative designed to make digital content in Europe more accessible, usable and exploitable. For example, in 2005 the European Commission's Directorate-General for Information Society and Media, established a 4 year program called eContentplus, supported by a budget of €149m, which, according to the published programme abstract, had:

> "the overall aim of making digital content in Europe more accessible, usable and exploitable, facilitating the creation and diffusion of information, in areas of public interest, at Community level. It will create better conditions for accessing and managing digital content and services in multilingual and multicultural environments. It will broaden users' choice and support new ways of interacting with knowledge-enhanced digital content, a feature which is becoming essential to make content more dynamic and tailored to specific contexts (learning, cultural, people with special needs, etc.).
>
> The programme will pave the way for a structured framework for quality digital content in Europe - the European Digital Content Area - by facilitating transfer of experiences, best practice and cross-fertilisation between content sectors, content providers and users."[165]

The eContentplus program addressed three lines of action:

- Facilitating at Community level access to digital content, its use and exploitation;
- Facilitating improvement of quality and enhancing best practice related to digital content between content providers and users, and across sectors;
- Reinforcing co-operation between digital content stakeholders and awareness.[166]

The eContentplus programme concluded at the end of 2008. Community funded activities designed to make digital content in Europe more accessible, usable and exploitable, are now managed through the Information and Communications Technologies Policy Support Programme (ICT PSP), one of whose

[163] Ibid. Article7
[164] Ibid. Article9
[165] See http://cordis.europa.eu/programme/rcn/840_en.html
[166] Ibid. "Subdivision"

programmes, the Competitiveness and Innovation Framework Programme, supports the E-ARK Project.

Assessing the performance of Directive 2003/98/EC

Even after the PSI Directive came into force, interested parties continued to experience difficulties in gaining access to, and making use of, Public Sector Information. Not only were public authorities still reluctant to disclose information, but the Directive also suffered from the same inconsistency of implementation in national laws, as do most other EC Directives. In the period since the introduction of the Directive in 2003, the amount of data in the world, including public data, had grown exponentially, and there has been a considerable change in the technologies used to access and interrogate these data. In short, the Directive was no longer keeping pace with the real world developments.

The untapped potential of PSI

Against a widespread recognition that Directive 2003/98/EC was not working as well as had been hoped, the European Commission launched, in 2010, a public consultation to measure the impact of Directive 2003/98/EC. The responses to the consultation indicated that although considerable progress had been made in certain Member States, notably in the UK, barriers remained which prevented the full potential of PSI from being realised. The Commission concluded that further work was required in order to maximise the potential of PSI, and therefore published proposals for amendments to the PSI Directive in December 2011.

Some 90% of the respondents agreed that the Commission needed to take further action to open up data resources and to facilitate the re-use of Public Sector Information. The overall findings of the consultation were summarized as follows:

> "… the picture that emerges from the survey is of a community increasingly characterised by expectations of an open and transparent system in which all the relevant parts cooperate rather than compete. Whilst it is understandable that the expectations of commercial re-users will be different to those of public data holders, there is an increasing trend in making sure that the rights of both sides are respected. It is for instance telling that there has been a wide acceptance of the new provisions of the revised PSI Directive, with few comments openly challenging the compromise reached as a result of a lengthy legislative process."[167]

In addition to the public consultation, a number of studies also showed the untapped potential of PSI. For example, a meta-analysis conducted by Graham Vickery in 2011[168], came to the conclusion that there had been a relatively rapid growth in PSI-related markets, with an overall market of c.€32bn in 2010, with an economic "footprint" which was much larger still. He opined that:

> "… removing current barriers to access and improving the underlying infrastructure could achieve considerable gains. In the geospatial sector, economic benefits could be increased by some 10-40% by improving access, data standards, and building skills and

[167] Final Report: Results of an online consultation on the guidelines on recommended standard licences, datasets and charging for the re-use of public sector information. P.16. Available online at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=3896

[168] Vickery, G., "Review of Recent Studies on PSI Re-Use and Related Market Developments", Information Economics, Paris, 2011

> knowledge. Productivity gains from geospatial applications in local government could double over the next 5 years if better policies were adopted. Large new markets could also develop in financial, energy and construction sectors if access to information were improved."[169]

In terms of efficiency gains in existing operations:

> "…improving accessibility of information necessary for obligatory environmental impact assessments could potentially reduce EU27 costs by 20% or around EUR 2 billion per year, open access to R&D results could result in recurring gains of around EUR 6 billion per year, and if European citizens each saved as little as 2 hours per year by more rapid and comprehensive access to public information, this would be worth at least EUR 1.4 billion per year."[170]

He concluded that:

> "There is emerging evidence that improving access and lowering prices dramatically have positive impacts on the number of users and development of new uses. At the same time, changing access and pricing policies provide opportunities for reviewing the role of the public task in generating and distributing PSI and implementing other changes to make PSI more accessible."[171]

De Vries, M. et al., in their 2011 'POPSIS' study[172] assessed different models of supply and charging for PSI and their effects through the analysis of 21 case studies. The cases covered a wide range of public sector bodies (PSBs) and different PSI sectors (meteorological data, geographical data, business registries and others) across Europe. Ranging from zero and marginal cost models to partial and full cost-recovery regimes, the case study analysis focused on the effects of PSI charging models on the downstream market, PSI re-users and end-users and impacts on the PSB itself.

The POPSIS analysis indicated that the potential benefits of lowered charges for PSI re-use can be high, and have the potential to increase economic activity, market dynamism, innovation and employment. By contrast, the potential disadvantages of lowering PSI charges appear to be low.

> "Unless zero cost pricing is applied, the price mechanism may actually increase the revenues rather than lowering them. The costs of a transition to lower PSI charges appear to be relatively low. This is because, to a large extent, the knowledge and infrastructure needed by the PSBs already exist. The main effort lies in an adjustment of processes and mindsets to serve PSI re-users most effectively."[173]

Also in 2011, Clapton, G. et al conducted a study for the European Commission on Public Sector Information

[169] Ibid. p.4
[170] Ibid. p.4
[171] Ibid. p.4
[172] De Vries, M. et al., "POPSIS Pricing Of Public Sector Information Study: Models of Supply and Charging for Public Sector Information (ABC)", Deloitte on behalf of European Commission Information Society and Media Directorate-General, 2011.
[173] Ibid. p.7

re-use in the cultural sector.[174] The objectives of the study of the study were to:

> "estimate the importance of re-use in terms of revenues for cultural institutions;
> estimate trends in the development of the re-use market for cultural material."[175]

In total, they had 66 respondents drawn mostly (86%) from the GLAM[176] sector, many of whom confirmed poor understanding of the PSI directive together with concerns about the applicability of the PSI directive to the cultural sector. Concern was also expressed about the potential impact on their income that inclusion within the directive would cause, and the administrative burden that inclusion within the directive would bring:

> "These concerns particularly related to the effort required to clear Intellectual Property Rights, the effort required to negotiate complex third party re-uses, and a concern about receiving a large number of requests from members of the public."[177]

Directive 2013/37/EU (amending Directive 2003/98/EC) on the re-use of public sector information

With the various reviews and studies having made it clear that more binding rules were necessary to create a true European information market based on PSI, the Commission set about strengthening its PSI policy by linking it to the popular 'open data' concept. The proposals to amend Directive 2003/98/EC took place under the umbrella of the Europe 2020 ten-year jobs and growth strategy, and were part of the flagship initiative "A Digital Agenda for Europe". The overall priorities were (and remain):

> "Smart growth: developing an economy based on knowledge and innovation.
>
> Sustainable growth: promoting a more resource efficient, greener and more competitive economy.
>
> Inclusive growth: fostering a high-employment economy delivering social and territorial cohesion."
> [178]

Within this overall context, the European Commission adopted the Open Data Strategy, which it interprets as:

> "focussing on generating value through re-use of a specific type of data – public sector information, sometimes also referred to as government data. That is all the information that public bodies produce, collect or pay for. Examples are: geographical information, statistics, weather data, data from publicly funded research projects, and digitised books from libraries."[179]

This was the context against which t Directive 2013/37/EC of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information was introduced.

---

[174] Clapton, G., Hammond, M., & Poole, N., "PSI re-use in the cultural sector", Curtis+Cartwright Consulting Ltd on behalf of the European Commission, 2011
[175] Ibid. P.1
[176] Galleries, Libraries, Archives, and Museums
[177] Ibid. p.5
[178] Communication from the Commission "Europe 2020: A strategy for smart, sustainable and inclusive growth.", March 3rd 2010. p.5
[179] See http://ec.europa.eu/digital-agenda/en/open-data-0

The position with respect to Open data policies is spelled out clearly in the preamble to Directive 2013/37/EU:

> "Open data policies which encourage the wide availability and re-use of public sector information for private or commercial purposes, with minimal or no legal, technical or financial constraints, and which promote the circulation of information not only for economic operators but also for the public, can play an important role in kick-starting the development of new services based on novel ways to combine and make use of such information, stimulate economic growth and promote social engagement."[180]

The Commission also expressed concern that the benefits of Open data policies cannot be fully achieved while differences continue to exists between the ways in which Member States exploit PSI. To help businesses take full advantage of the economic potential of Public Sector Information, the Commission set out to provide an optimal legal framework to stimulate the digital content market for PSI-based products and services, including its cross-border dimension. Furthermore, they aimed to prevent distortions of competition in the market for the reuse of PSI.

The amendments to the original text of Directive 2003/98/EC are fairly extensive, indeed only Article 10 (Non-Discrimination) and Article 12 (Implementation) survives unchanged.

Directive 2013/37/EU for the first time brings 'cultural information' under the remit of PSI:

> "For documents in which libraries, including university libraries, museums and archives hold intellectual property rights, Member States shall ensure that, where the re-use of such documents is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV." [181]

As noted above, Directive 2003/98/EC placed no obligation on Member States concerning access to documents or their re-use, leaving such determinations entirely within the remit of the States themselves. . Under Directive 2013/37/EU, this position was somewhat modified, with the Directive laying down a clear obligation for Member States to make all documents re-usable unless access is restricted or excluded under national rules on access to documents.[182]

Recital 20 of Directive 2013/37/EU outlines the intention to facilitate re-use by obliging public sector bodies to make documents available in machine readable formats and together with their metadata, wherever possible, in formats that support interoperability. One way in which this might be achieved would be to process Public Sector Information in line with principles set out in Directive 2007/2/EC (INSPIRE):

> "To facilitate re-use, public sector bodies should, where possible and appropriate, make documents available through open and machine-readable formats and together with their metadata, at the best level of precision and granularity, in a format that ensures interoperability, e.g. by processing them in a way consistent with the principles governing the compatibility and usability requirements for spatial information under Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community

[180] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information. Recital 3.
[181] Ibid. Article3(2)
[182] Ibid. Recital 8

(INSPIRE)"[183]

A number of changes are introduced in Directive 2013/37/EU to the way in which charges may be levied:

> "Where charges are made by public sector bodies for the re-use of documents, those charges should in principle be limited to the marginal costs. However the necessity of not hindering the normal running of public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks or of the costs relating to the collection, production, reproduction and dissemination of certain documents made available for re-use should be taken into consideration. In such cases, public sector bodies should be able to charge above marginal costs. Those charges should be set according to objective, transparent and verifiable criteria and the total income from supplying and allowing re-use of documents should not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment. The requirement to generate revenue to cover a substantial part of the public sector bodies' costs relating to the performance of their public tasks or of the costs relating to the collection, production, reproduction and dissemination of certain documents, does not have to be a legal requirement and may stem, for example, from administrative practices in Member States. Such a requirement should be regularly reviewed by the Member States."[184]

This is implemented in Article 6(1) of Directive 2013/37/EU:

> "Where charges are made for the re-use of documents, those charges shall be limited to the marginal costs incurred for their reproduction, provision and dissemination."[185]

It is worth noting that Article 6(2c) exempts libraries, including university libraries, museums, and archives, from this regime.

Directive 2013/37/EU expands the provision made available for the redress of grievances, introducing a new requirement for an impartial oversight body at the national level, granted regulatory powers, and able to make binding decisions on public sector bodies concerning the re-use of public sector information, and to whom re-users can turn in case of denial of requests for re-use:

> "The means of redress should include the possibility of review by an impartial review body. That body could be an already existing national authority, such as the national competition authority, the national access to documents authority or a national judicial authority. That body should be organised in accordance with the constitutional and legal systems of Member States and should not prejudge any means of redress otherwise available to applicants for re-use. It should however be distinct from the Member State mechanism laying down the criteria for charging above marginal costs. The means of redress should include the possibility of review of negative decisions but also of decisions which, although permitting re-use, could still affect applicants on other grounds, notably by the charging rules applied. The review process should be swift, in accordance with the needs of a rapidly changing market."[186]

[183] Ibid. Recital 20.
[184] Ibid. Recital 22.
[185] Ibid. Article 6(1)
[186] Ibid. Recital 28.

Finally, under Article 13 of Directive 2013/37/EU, Member States are placed under an obligation to report ever three years on the extent to which Public Sector Information is being re-used, as well as the conditions under which it is being re-used:

> "Member States shall submit a report every 3 years to the Commission on the availability of public sector information for re-use and the conditions under which it is made available and the redress practices. On the basis of that report, which shall be made public, Member States shall carry out a review of the implementation of Article 6, in particular as regards charging above marginal cost."[187]

[187] Ibid. Article 13(2)

8. Legal Context of European Copyright Law[188]

The Purpose of Copyright Law

Copyright laws generally aim to strike a balance between, on the one hand, ensuring a reward for creativity and investment, and on the other, the dissemination of knowledge for the general good. The preamble to the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, makes clear that the overriding purpose of harmonising copyright regulation within the EC is to ensure that competition in the internal market is not distorted. This is fully in line both with the Treaty establishing the European Community, and with general notion that the primary purpose of copyright law is to promote knowledge by establishing, for authors and creators, a temporary monopoly over their output thereby permitting them to protect and stimulate the development and marketing of new products and services and the creation and exploitation of their creative content.

The rights granted to authors, while very extensive, are not unrestricted since there is a recognition that creating an absolute monopoly would have the effect of stifling rather than promoting markets. Where the rights of authors are seen as conflicting with the public interest, various exemptions are provided. However, the onus is on those who wish to make use of exemptions to copyright protection to demonstrate clearly that they are properly entitled to do so, and that they have complied with any restrictions placed on the use of material reproduced under a copyright exemption. For a variety of reasons this can, in practice, be somewhat difficult to accomplish. For example, it is common for complex digital objects such as computer games, or multi-media products to have equally complex rights arrangements associated with them. The regulations governing IP that apply to music, differ from those which apply to text, video, or normal graphical elements such as logo design and so on. Trying to establish which rights need to be taken into consideration, identifying the various rights holders whose permission may be required, and understanding completely which laws apply, is far from straightforward. There are few economies of scale available. The situation, which is difficult enough when dealing with individual cases, can easily become unmanageable for memory institutions whose preservation responsibilities require them to process digital objects by tens of thousands (or more) rather than singly.

Legal Landscape

Digital preservation activity in the European Union takes places within a complex and often contradictory legislative landscape. Of most immediate concern to preservationists is the national legislation under which they operate day to day. Different nation states have their own laws and the understanding of key terms that prevails in one country often does not conform to that which holds elsewhere. Over and above national law, stands the European Community framework – which, although meant to be incorporated into member state legislation, is not uniformly or completely implemented across the whole of the EU. Here again, there is some disagreement over the interpretation of key terms. Finally, there is non-EU legislation, and international treaties and obligations such as the Paris Convention for the Protection of Industrial Property (1883), and the Berne Convention for the Protection of Literary and Artistic Works (1886), to consider.

[188] The material provided in this section relies heavily on Anderson, D.P., "A layman's guide to the KEEP legal studies" 2011

The principle of the supremacy of Community Law

In 1964, the European Court of Justice established the principle of supremacy of Community law over national legislation[189]. Something of the complexity of the law in this area may be understood by carrying out a keyword search at legislation.gov.uk to see how many pieces of UK legislation touch on a given topic. Results of a relevant search are listed in the table below:

Keyword	Pieces of legislation
Copyright	>200
Software	>200
Data Protection	>200
Privacy	>200
Database	167
Intellectual Property Rights	163
Trademark	74

The complexity indicated by the result of this search should make us hesitant in assuming that it is possible, within the context of this report, to arrive at anything other than the most tentative of conclusions of what *the law* requires in any given case. With so much law to consider, and with multi-layered jurisdictional questions involved, there is a high likelihood of finding situations where there is no unambiguously clear legal interpretation to be found.

Uniform law and international reciprocal protection.

The overwhelming majority of nations are signatories to at least one of various international conventions dealing with Intellectual Property Rights (IPR). A number of these conventions are administered by the World Intellectual Property Organisation (WIPO) under the auspices of the United Nations. According to the World International Property Organisation (WIPO):

> "the need for international protection of intellectual property became evident when foreign exhibitors refused to attend the International Exhibition of Inventions in Vienna in 1873 because they were afraid their ideas would be stolen and exploited commercially in other countries."[190]

This highlights the underlying commercial imperative to balance the stimulation of economic growth which may be derived from the exploitation of novel ideas and inventions, against the reasonable commercial interests of innovators, and inventors. This is what drives most copyright and intellectual property law, and is also evident in aspects of Data Protection regulation, as well as in the law governing the Re-Use of Public Sector Information.

The Paris Convention for the Protection of Industrial Property 1883.

The Paris Convention[191] is one of the highly influential international agreements which is administered by WIPO. It was concluded in 1883, revised at Brussels in 1900, at Washington in 1911, at The Hague in 1925, at London in 1934, at Lisbon in 1958 and at Stockholm in 1967, and amended in 1979. This agreement applies to industrial property in the widest sense, including patents, marks, industrial designs, utility models

[189] Established in Case 6/64, Costa v. Enel [1964], Court of Justice of the European Communities
[190] See http://www.wipo.int/treaties/en/general/
[191] http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html

(a kind of “small patent” provided for by the laws of some countries), trade names (designations under which an industrial or commercial activity is carried on), geographical indications (indications of source and appellations of origin) and the repression of unfair competition.
The substantive provisions of the Convention fall into three main categories: national treatment, right of priority, common rules.

(1) Under the provisions on national treatment, the Convention provides that, as regards the protection of industrial property, each contracting State must grant the same protection to nationals of the other contracting States as it grants to its own nationals. Nationals of non-contracting States are also entitled to national treatment under the Convention if they are domiciled or have a real and effective industrial or commercial establishment in a contracting State.

(2) The Convention provides for the right of priority in the case of patents (and utility models, where they exist), marks and industrial designs. This right means that, on the basis of a regular first application filed in one of the contracting States, the applicant may, within a certain period of time (12 months for patents and utility models; 6 months for industrial designs and marks), apply for protection in any of the other contracting States; these later applications will then be regarded as if they had been filed on the same day as the first application. In other words, these later applications will have priority (hence the expression “right of priority”) over applications which may have been filed during the said period of time by other persons for the same invention, utility model, mark or industrial design. Moreover, these later applications, being based on the first application, will not be affected by any event that may have taken place in the interval, such as any publication of the invention or sale of articles bearing the mark or incorporating the industrial design. One of the great practical advantages of this provision is that when an applicant desires protection in several countries, he is not required to present all his applications at the same time but has six or 12 months at his disposal to decide in which countries he wishes protection and to organize with due care the steps he must take to secure protection.

(3) The Convention lays down a few common rules, which all the contracting States must follow. The most important are the following:

(a) As to Patents: Patents granted in different contracting States for the same invention are independent of each other: the granting of a patent in one contracting State does not oblige the other contracting States to grant a patent; a patent cannot be refused, annulled or terminated in any contracting State on the ground that it has been refused or annulled or has terminated in any other contracting State.

The inventor has the right to be named as such in the patent.

The grant of a patent may not be refused, and a patent may not be invalidated, on the ground that the sale of the patented product, or of a product obtained by means of the patented process, is subject to restrictions or limitations resulting from the domestic law.

Each contracting State that takes legislative measures providing for the grant of compulsory licenses to prevent the abuses which might result from the exclusive rights conferred by a patent may do so only with certain limitations. Thus, a compulsory license (license not granted by the owner of the patent but by a public authority of the State concerned) based on failure to work the patented invention may only be granted pursuant to a request filed after three or four years of failure to work or insufficient working of the patented invention and it must be refused if the patentee gives legitimate reasons to justify his inaction.

Furthermore, forfeiture of a patent may not be provided for, except in cases where the grant of a compulsory license would not have been sufficient to prevent the abuse. In the latter case, proceedings for forfeiture of a patent may be instituted, but only after the expiration of two years from the grant of the first compulsory license.

(b) As to Marks: The Paris Convention does not regulate the conditions for the filing and registration of marks which are therefore determined in each contracting State by the domestic law. Consequently, no application for the registration of a mark filed by a national of a contracting State may be refused, nor may a registration be invalidated, on the ground that filing, registration or renewal has not been effected in the country of origin. Once the registration of a mark is obtained in a contracting State, it is independent of its possible registration in any other country, including the country of origin; consequently, the lapse or annulment of the registration of a mark in one contracting State will not affect the validity of registration in other contracting States.

Where a mark has been duly registered in the country of origin, it must, on request, be accepted for filing and protected in its original form in the other contracting States. Nevertheless, registration may be refused in well-defined cases, such as when the mark would infringe acquired rights of third parties, when it is devoid of distinctive character, when it is contrary to morality or public order, or when it is of such a nature as to be liable to deceive the public.

If, in any contracting State, the use of a registered mark is compulsory, the registration cannot be cancelled until after a reasonable period, and only if the owner cannot justify his inaction.

Each contracting State must refuse registration and prohibit the use of marks which constitute a reproduction, imitation or translation, liable to create confusion, of a mark considered by the competent authority of that State to be well known in that State as being already the mark of a person entitled to the benefits of the Convention and used for identical or similar goods.

Each contracting State must likewise refuse registration and prohibit the use of marks which consist of or contain without authorization, armorial bearings, State emblems and official signs and hallmarks of contracting states, provided they have been communicated through the International Bureau of WIPO. The same provisions apply to armorial bearings, flags, other emblems, abbreviations and names of certain intergovernmental organizations.

Collective marks must be granted protection.

(c) As to Industrial Designs: Industrial designs must be protected in each contracting State, and protection may not be forfeited on the ground that the articles incorporating the design are not manufactured in that State.

(d) As to Trade Names: Protection must be granted to trade names in each contracting State without the obligation of filing or registration.

(e) As to Indications of Source: Measures must be taken by each contracting State against direct or indirect use of a false indication of the source of the goods or the identity of the producer, manufacturer or trader.

(f) As to Unfair Competition: Each contracting State must provide for effective protection against unfair competition.

The Paris Union was one of the first intellectual property treaties. It established a Union for the protection of industrial property. It was established by the Convention, and has an Assembly and an Executive Committee. Every State member of the Union, which has adhered to at least the administrative and final provisions of the Stockholm Act (1967) is a member of the Assembly. The members of the Executive Committee are elected from among the members of the Union, except for Switzerland, which is a member ex officio.

The establishment of the biennial program and budget of the WIPO Secretariat—as far as the Paris Union is concerned—is the task of its Assembly.

The Convention is open to all States. Instruments of ratification or accession must be deposited with the Director General of WIPO.

Berne Convention for the Protection of Literary and Artistic Works (1886)

The Berne Convention[192], which is also administered by WIPO, was concluded in 1886, completed at Paris in 1896, revised at Berlin in 1908, completed at Berne in 1914, revised at Rome in 1928, at Brussels in 1948, at Stockholm in 1967 and at Paris in 1971, and was amended in 1979.

The Convention rests on three basic principles and contains a series of provisions determining the minimum protection to be granted, as well as special provisions available to developing countries which want to make use of them.

The three basic principles are:

(a) Works originating in one of the contracting States (that is, works the author of which is a national of such a State or works which were first published in such a State) must be given the same protection in each of the other contracting States as the latter grants to the works of its own nationals (principle of "national treatment")[193].

(b) Such protection must not be conditional upon compliance with any formality (principle of "automatic" protection).

(c) Such protection is independent of the existence of protection in the country of origin of the work (principle of the "independence" of protection). If, however, a contracting State provides for a longer term than the minimum prescribed by the Convention and the work ceases to be protected in the country of origin, protection may be denied once protection in the country of origin ceases.

[192] http://www.wipo.int/treaties/en/ip/berne/summary_berne.html

[193] Under the Agreement on Trade-Related Aspects of Intellectual Property (TRIPS Agreement), the principles of national treatment, automatic protection and independence of protection also bind those World Trade Organization (WTO) Members which are not party to the Berne Convention. In addition, the TRIPS Agreement imposes an obligation of "most-favoured-nation treatment," under which advantages accorded by a WTO Member to the nationals of any other country must also be accorded to the nationals of all WTO Members. It is to be noted that the possibility of delayed application of the TRIPS Agreement does not apply to national treatment and most-favoured-obligations.

The minimum standards of protection relate to the works and rights to be protected, and the duration of the protection:

> (a) As to works, the protection must include "every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression" (Article 2(1) of the Convention).
>
> (b) Subject to certain permitted reservations, limitations or exceptions, the following are among the rights which must be recognized as exclusive rights of authorization:
>
> - the right to translate,
> - the right to make adaptations and arrangements of the work,
> - the right to perform in public dramatic, dramatico-musical and musical works,
> - the right to recite in public literary works,
> - the right to communicate to the public the performance of such works,
> - the right to broadcast (with the possibility of a contracting State to provide for a mere right to equitable remuneration instead of a right of authorization),
> - the right to make reproductions in any manner or form (with the possibility of a contracting State to permit, in certain special cases, reproduction without authorization provided that the reproduction does not conflict with the normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author, and with the possibility of a contracting State to provide, in the case of sound recordings of musical works, for a right to equitable remuneration),
> - the right to use the work as a basis for an audio-visual work, and the right to reproduce, distribute, perform in public or communicate to the public that audio-visual work[194].

The Convention also provides for "moral rights," that is, the right to claim authorship of the work and the right to object to any mutilation or deformation or other modification of, or other derogatory action in relation to, the work which would be prejudicial to the author's honour or reputation.

(c) As to the duration of protection, the general rule is that protection must be granted until the expiration of the 50th year after the author's death. There are, however, exceptions to this general rule. In the case of anonymous or pseudonymous works, the term of protection expires 50 years after the work has been lawfully made available to the public, except if the pseudonym leaves no doubt as to the author's identity or if the author discloses his identity during that period; in the latter case, the general rule applies. In the case of audio-visual (cinematographic) works, the minimum term of protection is 50 years after the making available of the work to the public ("release") or—failing such an event—from the creation of the work. In the case of works of applied art and photographic works, the minimum term is 25 years from the creation of such a work[195].

Countries regarded as developing countries in conformity with the established practice of the General Assembly of the United Nations may, for certain works and under certain conditions, depart from these minimum standards of protection with regard to the right of translation and the right of reproduction.

The Berne Union has an Assembly and an Executive Committee. Every country member of the Union, which

[194] Under the TRIPS Agreement, an exclusive right of rental must be recognized in respect of computer programs and, under certain conditions, audio-visual works.

[195] Under the TRIPS Agreement, any term of protection which is calculated on a basis other than the life of a natural person, must be at least 50 years from the first authorized publication of the work, or—failing such an event—50 years from the making of the work. However, this rule does not apply to photographic works, or works of applied art.

has adhered to at least the administrative and final provisions of the Stockholm Act is a member of the Assembly. The members of the Executive Committee are elected from among the members of the Union, except for Switzerland, which is a member ex officio.

The establishment of the biennial program and budget of the WIPO Secretariat—as far as the Berne Union is concerned—is the task of its Assembly.

The Convention is open to all States. Instruments of ratification or accession must be deposited with the Director General of WIPO[196].

The Berne "three-step test"

The three-step test, which first appeared in the Berne Convention, is regarded as a cornerstone of international copyright regulation, and imposes on constraints on the possible limitations and exceptions to exclusive rights under national copyright laws.

The three-step test applies to limitations and exceptions to copyright protection and specifies they will :

- be confined to certain special cases
- not conflict with a normal exploitation of the work
- not unreasonably prejudice the legitimate interests of the rights holder

The Legal Corpus

Key European Community regulation includes:

- Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society (the "Information Society Directive")
- Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs (Codified version replacing the abrogated Directive 91/250/ EEC of 14 May 1991, known as the "Computer Programs Directive")
- Directive 96/9/EC of 11 March 1996 on the legal protection of databases (the "Database Directive") (Collectively referred to as the "Community Framework")
- Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art
- Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property

[196]WTO Members, even if they are not party to the Berne Convention, must comply with the substantive law provisions of the Berne Convention, except that WTO Members not party to the Convention are not bound by the moral rights provisions of the Convention. Least developed countries may until July 1, 2013, delay the application of most of the obligations provided for in the TRIPS Agreement (Article 65). Naturally, States party to the Berne Convention cannot delay the application of their obligations provided for in the Berne Convention.

Protected Rights

The following rights are protected by European Union law:

- right of reproduction for authors, performers, producers of phonograms and films and broadcasting organisations[197]
- right of communication to the public for authors, performers, producers of phonograms and films and broadcasting[198]
- right of distribution for authors and for performers, producers of phonograms and films and broadcasting organisations[199]
- right of fixation for performers and broadcasting right of rental and/or lending for authors, performers, producers of phonograms and films[200]
- right of broadcasting for performers, producers of phonograms and broadcasting organisations[201]
- right of communication to the public by satellite for authors, performers, producers of phonograms and broadcasting organisations[202]
- The rights of reproduction, distribution and rental for authors of computer programs[203]

The Community Framework

Problematically, the Community framework does not recognize the notion of multimedia works as a specific type of protected content. As a result, no definition or specific framework related to multimedia works is available under EU law. Reproduction of multimedia works is addressed at the Community level through the various copyright and related rights directives as they apply to the constituent elements of a multimedia work: e.g., software programs, databases, sound, and images. This is a pattern that is replicated in national legislation.

Limitations and exceptions to copyright provided by the Information Society Directive

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. (also known as the Information Society Directive or the InfoSoc Directive) is a highly controversial Directive[204] that provides just one limitation to copyright protection:

- Temporary acts of reproduction which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:
    - a transmission in a network between third parties by an intermediary, or

[197] For example, Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property. Article 7.
[198] For example, Ibid. Article 8
[199] For example, Ibid. Article 9
[200] For example, Ibid. Articles 6 & 7
[201] For example, Ibid. Article 8
[202] For example, Idid. Article 6 & 8
[203] For example, Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. Article 4
[204] For example, see Hugenholtz, Bernt (2000). "Why the Copyright Directive is Unimportant, and Possibly Invalid". European Intellectual Property Review: 501.

    - a lawful use of a work or other subject-matter to be made, and which have no independent economic significance

The directive permits Member States to make provision exceptions or limitations to the right of reproduction and/or communication in some twenty cases. Of these the following four are of direct relevance to institutional digital preservation activity:

- in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage (Art. 5, 2(c));
- incidental inclusion of a work or other subject-matter in other material (Art. 5, 3(i));
- use in connection with the demonstration or repair of equipment (Art. 5, 3(l));
- use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections (Art. 5, 3(n))

In all of these cases, the exceptions and limitations provided are subject to the Berne 'three-step test' (Art. 5, 5).

The Directive therefore permits limited rights for memory institutions to make copies for the purpose of preservation, but not for general communication. For reproduction to be permissible it would not have to be permitted under national law, and should not conflict with a normal exploitation of the work, nor unreasonably prejudice the legitimate interests of the rights holder. The Information Society Directive is generally regarded by the academic community as a victory for copyright-owning interests (publishing, film, music and major software companies) over content users' interests.

The list of exceptions outlined in the Directive has achieved a certain degree of harmonization but it should be noted that Member States have no power to introduce new limitations not already included in the Directive. This has the unwelcome effect that Member States have no independent ability to keep their legislative frameworks up to date with unforeseen technological developments.

Limitations and exceptions to copyright provided by the Computer Programs Directive

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (also known as the Computer Programs Directive) gives the rights holder the exclusive right to authorize:

- the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole; in so far as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction
- the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program
- any form of distribution to the public, including the rental, of the original computer program or of copies thereof

However, the lawful acquirer of a program is assumed to have a licence to:

- create a backup copy where necessary to use the program and to alter the program within its

intended purpose (e.g. for error correction) [205]

- make a back-up copy for his or her personal use to "observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do" [206]
- decompile the program if this is necessary to ensure its operates with another program or device, but not for any other purpose.[207]

None of the exceptions set out in the Directive expressly serve the purpose of stakeholders engaged in digital preservation, and the Directive does not provide for any exceptions related to legal deposit requirements or for scientific, study or education purposes that would be similar or close to those set out by Article 5.2 (c) and 5.3 (n) of the Information Society Directive.

In view of the supremacy of Community law, it must be assumed that the requirements of the Directive take precedence over more (or less) permissive national legislation. Therefore, reproduction of computer programs carried out by institutions like libraries and museums, even when authorized under national laws, must be considered to be in conflict with the Directive.

Limitations and exceptions to copyright provided by the Database Directive.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (also known as the Database Directive) harmonizes the treatment of databases under copyright law, and creates a new *sui generis* right for the creators of databases which do not otherwise qualify for copyright protection.

A database is defined as "*a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means*" (Article 1).

The overall objective of the Directive is to provide:

- copyright protection for the intellectual creation involved in the selection and arrangement of materials
- *sui generis* protection for an investment (financial and in terms of human resources, effort and energy) in the obtaining, verification or presentation of the contents of a database, whether or not these have an intrinsically innovative nature.

The Database Directive gives the rights holder the exclusive right to authorize:

- temporary or permanent reproduction by any means and in any form, in whole or in part;
- translation, adaptation, arrangement and any other alteration;
- any form of distribution to the public of the database or of copies thereof (subject to the exhaustion of rights)[208].
- any communication, display or performance to the public;

[205] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. Article 5(2)
[206] Ibid. Article 5(3)
[207] Ibid. Article 6
[208] The first sale in the Community of a copy of the database by the rights holder or with his consent exhausts the right to control resale of that copy within the Community.

- any reproduction, distribution, communication, display or performance to the public of a translation, adaptation, arrangement or other alteration

Member States are allowed to provide limitations of rights in the following cases:

- in the case of reproduction for private purposes of a non-electronic database
- where there is use for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved
- where there is use for the purposes of public security of for the purposes of an administrative or judicial procedure

It is reasonable to assume that a significant portion of databases, whether made available on a standalone basis or embedded in a multimedia device, will be protected by copyright. Databases put on the market or otherwise made available to the public on tangible media generally offer more than a simple list or catalogue of items or data and are likely to be eligible to copyright protection under national laws within the EU to the extent the selection and arrangements of the contents thereof as decided by the authors is a key factor to, *inter alia*, their merchantability.

None of the copyright related exceptions or *sui generis* rights offered by the Directive are relevant for most digital preservation activity. Consequently, the reproduction of a database for preservation purposes fails to comply with the provisions of the Directive.

Technological Measures of Protection (TMP)

Many works are made available in a form to which technical measures have been applied to prevent or restrict the use that may be made of them. This might take the form of a simple password protection scheme, or may involve considerable technical sophistication. Broadly speaking, there are two categories of TMP: access control, which seeks to prevent unauthorised access to material; and copy control, the aim of which is to prevent unauthorised copying.

Recital 47 of the Information Society Directive (2001/29/EC) recognises the "need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect"[209]. It stipulates that:

> "Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective." However it also permits Member States to be given the option of "providing for certain exceptions or limitations for cases such as educational and scientific purposes, for the benefit of public institutions such as libraries and archives"[210]

The potential for exemptions is quite limited and does not extend to permitting the creation or use of tools by individuals to bypass TMP generally, nor to even limited consultation of protected multimedia works under emulation.

[209] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. Recital 47
[210] Ibid. Article 6(2)

Implications of the rules on Technological Measures of Protection

Provisions related to technological measures and rights management information originate from the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). These state that Members shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures[211]. The WCT and WPPT also mandate the provision of adequate and effective legal remedies against anyone knowingly performing an act that may induce, enable, facilitate or conceal an infringement of any right related to rights management information.

Following the WCT and WPPT, the Information Society Directive adopted a framework for the recognition and protection of TMP. However right holders who use TMP must allow otherwise legal reproduction.

Preliminary findings under the Community Framework

Although the Information Society Directive is stated to be without prejudice to provisions concerning legal deposit requirements (Article 9), neither the Programs Directive nor the Database Directive hand down provisions concerning legal deposit or any similar exceptions.

Accordingly, reproduction of computer programs, databases and multimedia works such as videogames (to the extent they include computer programs or database elements) even for legal deposit purposes is not compliant with the Community framework.

With respect to the Community framework:

- None of the exceptions set out at the Community level serves adequately the purposes of memory organisations in going about their digital preservation activity.
- The Community framework does not provide for legal deposit requirements.
- The Community framework does not provide for scientific, study or education purposes across the full range required for memory organisations.
- Reproduction of computer programs and databases even when carried out by memory organisations and authorized under national laws, is in conflict with the Community framework

[211] See WIPO Copyright Treaty (adopted in Geneva on December 20, 1996). Article 11. See also WIPO Performances and Phonograms Treaty (WPPT) (adopted in Geneva on December 20, 1996) Article 18

9. Appendix 1: National Data Protection Authorities (Feb 2017)[212]

European Data Protection Supervisor

Rue Wiertz 60

1047 Bruxelles/Brussel

Office: Rue Montoyer 63, 6th floor

Tel. +32 2 283 19 00

Fax +32 2 283 19 50 e-mail: edps@edps.europa.eu

Website: http://www.edps.europa.eu/EDPSWEB/

Art 29 WP Member: Mr Giovanni BUTTARELLI, European Data Protection Supervisor

Austria

Österreichische Datenschutzbehörde
Hohenstaufengasse 3
1010 Wien
Tel. +43 1 531 15 202525
Fax +43 1 531 15 202690
e-mail: dsb@dsb.gv.at
Website: http://www.dsb.gv.at/

Art 29 WP Member: Dr Andrea JELINEK, Director, Österreichische Datenschutzbehörde

Belgium

Commission de la protection de la vie privée
Rue de la Presse 35
1000 Bruxelles
Tel. +32 2 274 48 00
Fax +32 2 274 48 10
e-mail: commission@privacycommission.be
Website: http://www.privacycommission.be/

Bulgaria

Commission for Personal Data Protection
2, Prof. Tsvetan Lazarov blvd.

[212] Taken from http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

Sofia 1592
Tel. +359 2 915 3523
Fax +359 2 915 3525
e-mail: kzld@cpdp.bg
Website: http://www.cpdp.bg/

Art 29 WP Member: Mr Ventsislav KARADJOV, Chairman of the Commission for Personal Data
Art 29 WP Alternate Member: Ms Mariya MATEVA

Croatia

Croatian Personal Data Protection Agency
Martićeva 14
10000 Zagreb
Tel. +385 1 4609 000
Fax +385 1 4609 099
e-mail: azop@azop.hr or info@azop.hr
Website: http://www.azop.hr/

Art 29 WP Member: Mr Anto RAJKOVAČA, Director of the Croatian Data Protection Agency

Cyprus

Commissioner for Personal Data Protection
1 Iasonos Street,
1082 Nicosia
P.O. Box 23378, CY-1682 Nicosia
Tel. +357 22 818 456
Fax +357 22 304 565
e-mail: commissioner@dataprotection.gov.cy
Website: http://www.dataprotection.gov.cy/

Art 29 WP Member: Ms Irene LOIZIDOU NIKOLAIDOU Curriculum vitae(230 kB)
Art 29 WP Alternate Member: Mr Constantinos GEORGIADES

Czech Republic

The Office for Personal Data Protection
Urad pro ochranu osobnich udaju
Pplk. Sochora 27
170 00 Prague 7
Tel. +420 234 665 111
Fax +420 234 665 444
e-mail: posta@uoou.cz
Website: http://www.uoou.cz/

Art 29 WP Member: Ms Ivana JANŮ, President of the Office for Personal Data Protection
Art 29 WP Alternate Member: Mr Ivan PROCHÁZKA, Adviser to the President of the Office

Denmark

Datatilsynet
Borgergade 28, 5
1300 Copenhagen K
Tel. +45 33 1932 00
Fax +45 33 19 32 18
e-mail: dt@datatilsynet.dk
Website: http://www.datatilsynet.dk/

Art 29 WP Member: Ms Cristina Angela GULISANO, Director, Danish Data Protection Agency (Datatilsynet)
Art 29 WP Alternate Member: Mr Christian Vinter HAGSTRØM, Head of Section

Estonia

Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)
Väike-Ameerika 19
10129 Tallinn
Tel. +372 6274 135
Fax +372 6274 137
e-mail: info@aki.ee
Website: http://www.aki.ee/en

Art 29 WP Member: Mr Viljar PEEP, Director General, Estonian Data Protection Inspectorate
Art 29 WP Alternate Member: Ms Kaja PUUSEPP

Finland

Office of the Data Protection Ombudsman
P.O. Box 315
FIN-00181 Helsinki
Tel. +358 10 3666 700
Fax +358 10 3666 735
e-mail: tietosuoja@om.fi
Website: http://www.tietosuoja.fi/en/

Art 29 WP Member: Mr Reijo AARNIO, Ombudsman of the Finnish Data Protection Authority
Art 29 WP Alternate Member: Ms Elisa KUMPULA, Head of Department

France

Commission Nationale de l'Informatique et des Libertés - CNIL
8 rue Vivienne, CS 30223
F-75002 Paris, Cedex 02
Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00

e-mail:
Website: http://www.cnil.fr/

Art 29 WP Member: Ms Isabelle FALQUE-PIERROTIN, President of CNIL
Art 29 WP Alternate Member: Ms Florence RAYNAL

Germany

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Husarenstraße 30
53117 Bonn
Tel. +49 228 997799 0; +49 228 81995 0
Fax +49 228 997799 550; +49 228 81995 550
e-mail: poststelle@bfdi.bund.de
Website: http://www.bfdi.bund.de/
The competence for complaints is split among different data protection supervisory authorities in Germany. Competent authorities can be identified according to the list provided under https://www.bfdi.bund.de/bfdi_wiki/index.php/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte

Art 29 WP Member: Ms Andrea VOSSHOFF, Federal Commissioner for Freedom of Information
Art 29 WP Alternate Member: Prof. Dr. Johannes CASPAR, representative of the federal states

Greece

Hellenic Data Protection Authority
Kifisias Av. 1-3, PC 11523
Ampelokipi Athens
Tel. +30 210 6475 600
Fax +30 210 6475 628
e-mail: contact@dpa.gr
Website: http://www.dpa.gr/

Art 29 WP Member: Mr Petros CHRISTOFOROS, President of the Hellenic Data Protection Authority
Art 29 WP Alternate Member: Dr.Vasilios ZORKADIS, Director

Hungary

Data Protection Commissioner of Hungary
Szilágyi Erzsébet fasor 22/C
H-1125 Budapest
Tel. +36 1 3911 400
e-mail: peterfalvi.attila@naih.hu
Website: http://www.naih.hu/

Art 29 WP Member: Dr Attila PÉTERFALVI, President of the National Authority for Data Protection and Freedom of Information
Art 29 WP Alternate Member: Mr Endre Győző SZABÓ Vice-president of the National Authority for Data

Protection and Freedom of Information

Ireland

Data Protection Commissioner
Canal House Station Road
Portarlington
Co. Laois
Lo-Call: 1890 25 22 31
Tel. +353 57 868 4800
Fax +353 57 868 4757
e-mail: info@dataprotection.ie
Website: http://www.dataprotection.ie/

Art 29 WP Member: Ms Helen DIXON, Data Protection Commissioner
Art 29 WP Alternate Members: Mr John O'DWYER, Deputy Commissioner; Mr Dale SUNDERLAND, Deputy Commissioner

Italy

Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121
00186 Roma
Tel. +39 06 69677 1
Fax +39 06 69677 785
e-mail: garante@garanteprivacy.it
Website: http://www.garanteprivacy.it/

Art 29 WP Member: Mr Antonello SORO, President of Garante per la protezione dei dati personali
Art 29 WP Alternate Member: Ms Vanna PALUMBO, Head of Service for EU and International Matters

Latvia

Data State Inspectorate
Director: Ms Signe Plumina
Blaumana str. 11/13-15
1011 Riga
Tel. +371 6722 3131
Fax +371 6722 3556
e-mail: info@dvi.gov.lv
Website: http://www.dvi.gov.lv/

Art 29 WP Member: Ms Signe PLUMINA, Director of Data State Inspectorate
Art 29 WP Alternate Member: Ms Aiga BALODE

Lithuania

State Data Protection
Žygimantų str. 11-6a
011042 Vilnius
Tel. + 370 5 279 14 45
Fax +370 5 261 94 94
e-mail: ada@ada.lt
Website: http://www.ada.lt/

Art 29 WP Member: Mr Algirdas KUNČINAS, Director of the State Data Protection Inspectorate
Art 29 WP Alternate Member: Ms Neringa KAKTAVIČIŪTĖ-MICKIENĖ, Head of Complaints Investigation and International Cooperation Division

Luxembourg

Commission Nationale pour la Protection des Données
1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette
Tel. +352 2610 60 1
Fax +352 2610 60 29
e-mail: info@cnpd.lu
Website: http://www.cnpd.lu/

Art 29 WP Member: Ms Tine A. LARSEN, President of the Commission Nationale pour la Protection des Données
Art 29 WP Alternate Member: Mr Thierry LALLEMANG, Commissioner

Malta

Office of the Data Protection Commissioner
Data Protection Commissioner: Mr Joseph Ebejer
2, Airways House
High Street, Sliema SLM 1549
Tel. +356 2328 7100
Fax +356 2328 7198
e-mail: commissioner.dataprotection@gov.mt
Website: http://www.dataprotection.gov.mt/

Art 29 WP Member: Mr Saviour CACHIA, Information and Data Protection Commissioner
Art 29 WP Alternate Member: Mr Ian DEGUARA, Director – Operations and Programme Implementation

Netherlands

Autoriteit Persoonsgegevens
Prins Clauslaan 60
P.O. Box 93374
2509 AJ Den Haag/The Hague

Tel. +31 70 888 8500
Fax +31 70 888 8501
e-mail: info@autoriteitpersoonsgegevens.nl
Website: https://autoriteitpersoonsgegevens.nl/nl

Art 29 WP Member: Mr Aleid WOLFSEN, Chairman of Autoriteit Persoonsgegevens

Poland

The Bureau of the Inspector General for the Protection of Personal Data - GIODO
ul. Stawki 2
00-193 Warsaw
Tel. +48 22 53 10 440
Fax +48 22 53 10 441
e-mail: kancelaria@giodo.gov.pl; desiwm@giodo.gov.pl
Website: http://www.giodo.gov.pl/

Art 29 WP Member: Ms Edyta BIELAK-JOMAA, Inspector General for the Protection of Personal Data

Portugal

Comissão Nacional de Protecção de Dados - CNPD
R. de São. Bento, 148-3°
1200-821 Lisboa
Tel. +351 21 392 84 00
Fax +351 21 397 68 32
e-mail: geral@cnpd.pt
Website: http://www.cnpd.pt/

Art 29 WP Member: Ms Filipa CALVÃO, President, Comissão Nacional de Protecção de Dados

Romania

The National Supervisory Authority for Personal Data Processing
President: Mrs Ancuţa Gianina Opre
B-dul Magheru 28-30
Sector 1, BUCUREŞTI
Tel. +40 21 252 5599
Fax +40 21 252 5757
e-mail: anspdcp@dataprotection.ro
Website: http://www.dataprotection.ro/

Art 29 WP Member: Ms Ancuţa Gianina OPRE, President of the National Supervisory Authority for Personal Data Processing
Art 29 WP Alternate Member: Ms Raluca POPA, Department of International Affairs

Slovakia

Office for Personal Data Protection of the Slovak Republic
Hraničná 12
820 07 Bratislava 27
Tel.: + 421 2 32 31 32 14
Fax: + 421 2 32 31 32 34
e-mail: statny.dozor@pdp.gov.sk
Website: http://www.dataprotection.gov.sk/

Art 29 WP Member: Ms Soňa PŐTHEOVÁ, President of the Office for Personal Data Protection of the Slovak Republic
Art 29 WP Alternate Member: Mr Jozef DUDÁŠ, Vice President

Slovenia

Information Commissioner
Ms Mojca Prelesnik
Zaloška 59
1000 Ljubljana
Tel. +386 1 230 9730
Fax +386 1 230 9778
e-mail: gp.ip@ip-rs.si
Website: https://www.ip-rs.si/
Art 29 WP Member: Ms Mojca PRELESNIK, Information Commissioner of the Republic of Slovenia

Spain

Agencia de Protección de Datos
C/Jorge Juan, 6
28001 Madrid
Tel. +34 91399 6200
Fax +34 91455 5699
e-mail: internacional@agpd.es
Website: https://www.agpd.es/

Art 29 WP Member: Ms María del Mar España Martí, Director of the Spanish Data Protection Agency
Art 29 WP Alternate Member: Mr Rafael GARCIA GOZALO

Sweden

Datainspektionen
Drottninggatan 29
5th Floor
Box 8114
104 20 Stockholm
Tel. +46 8 657 6100
Fax +46 8 652 8652

e-mail: datainspektionen@datainspektionen.se
Website: http://www.datainspektionen.se/

Art 29 WP Member: Ms Kristina SVAHN STARRSJÖ, Director General of the Data Inspection Board
Art 29 WP Alternate Member: Mr Hans-Olof LINDBLOM, Chief Legal Adviser

United Kingdom

The Information Commissioner's Office
Water Lane, Wycliffe House
Wilmslow - Cheshire SK9 5AF
Tel. +44 1625 545 745
e-mail: international.team@ico.org.uk
Website: https://ico.org.uk

Art 29 WP Member: Ms Elizabeth DENHAM, Information Commissioner
Art 29 WP Alternate Member: Mr Steve WOOD, Deputy Commissioner