doi: 10.17234/INFUTURE.2015.14 Preliminary communication

E-ARK Legal Issues Report: European Cultural Preservation in a Changing Legislative Landscape

David Anderson
University of Portsmouth
2 Winston Churchill Avenue, Portsmouth, Hampshire, UK
cdpa@btinternet.com

Summary

This paper summarizes the main findings of a report on the legal issues relating to digital preservation within the European Union that arise as a result of the many items of national and EC legislation, but principally from the proposed changes in data protection currently being discussed by the European Parliament, the Commission, and the Council. This report has been prepared as a Public Deliverable (D2.2) by the EC Policy Support Programme Project "E-ARK (European Archival Records and Knowledge Preservation) number 620998 (1 February 2014 – 31 January 2017). The full report is available for download free of charge from the E-ARK Project website – http://www.eark-project.com/resources/project-deliverables.

Keywords: legislation, data protection, data governance, European Community, digital preservation, E-ARK

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 strokes 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 the full 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.

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 (PbD) 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 princi-

ples, 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, lim-

ited 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.