CLOUD
ACCOUNTABILITY
PROJECT

D:B-5.1 White paper on the proposed data protection regulation

Deliverable Number:	D25.1
Work Package:	WP25
Version:	Final
Deliverable Lead Organisation:	QMUL
Dissemination Level:	PU
Contractual Date of Delivery (release):	31 March 2014
Date of Delivery:	28 February 2014

Editor

Kuan Hon (QMUL)

Contributors

Kuan Hon (QMUL), Eleni Kosta (TiU), Christopher Millard (QMUL), Dimitra Stefanatou (TiU)

Reviewer(s)

Amy Holcroft (HP), Simone Fischer-Hübner (KAU)

A4Cloud

www.a4cloud.eu

Accountability For Cloud and Other Future Internet Services

FP7-ICT-2011-8-317550-A4CLOUD

SEVENTH FRAMEWORK PROGRAMME

Abbreviations

A29WP – the Article 29 Data Protection Working Party, see p 9

Art - Article

BCRs – binding corporate rules, see p 32

Commission – the European Commission

Council – the Council of the European Union

DPA – the national supervisory authority ie data protection authority or regulator for a Member State

DPD – Data Protection Directive, see p 6

DPIA – data protection impact assessment, see p 11

EDPB – European Data Protection Board, see p 9

EDPS – European Data Protection Supervisor, see p 9

EEA – European Economic Area

EU – European Union

LIBE – the European Parliament's Civil Liberties, Justice and Home Affairs Committee

Rec - recital

WP196 – A29WP's Opinion 05/2012 on Cloud Computing, see n 16.

Executive Summary

This White Paper considers the implications for cloud accountability of the current proposals to modernise the EU Data Protection Directive. Many issues are problematic because outdated assumptions about technologies and business models underlie both the Directive and these proposals. Our main recommendations are:

- For technology neutrality, only persons with logical access to intelligible personal data should be regulated. Physical access is not necessary or sufficient to access intelligible personal data.
- With digital data, different degrees of deletion are possible. References to erasure or restriction should therefore be to removing or restricting access to intelligible personal data as appropriate to the risks involved. Cloud computing data are often replicated for integrity and availability reasons.
- The 'personal data' definition triggers applicability of the data protection regime in an 'all or nothing' fashion, but could encompass most data. A concept of pseudonymous data is one way to calibrate obligations, but definitions and obligations for each data type need further consideration.
- Clarity is needed regarding which obligations should trigger 'strict liability' for any non-compliance regardless of fault, and which should be risk-based, ie requiring only the taking of measures appropriate to the individual situation, reasonable measures to industry standards and the like.
- We support a more focused risk-based approach, as opposed to requiring privacy impact assessments etc in a broad range of situations that may not warrant it from a risks perspective.
- To incentivise adoption of accountability measures such as codes of conduct, certifications and seals, consequences of adoption should be made clear. In particular, defences or reductions in liability should be available to those who have obtained and complied with such measures.
- Cloud infrastructure providers may be neutral intermediaries. Defences available to intermediaries under the E-Commerce Directive should therefore be available to providers if they do not know that data stored with them by their users are personal data, or do not or cannot access intelligible personal data. Also, provisions regarding 'instructions' to processors should instead target the underlying mischief, namely misuse or disclosure of intelligible personal data by processors.
- Rather than impose joint liability on processors and co-controllers, a more fault-based allocation of liability is recommended. Careful consideration is needed of exactly which obligations should be imposed on processors, and the availability of insurance could be taken into account.
- Proposed provisions on international data transfers are retrograde and threaten to restrict cloud computing further. Consideration should be given to abolishing the data export restriction (and international agreement sought on jurisdictional conflicts and rules restricting (or compelling) government access to personal data). If the restriction is retained, 'transfer' should be defined by reference to intention to give or allow logical access to intelligible personal data to a third party recipient who is subject to the jurisdiction of a third country. Ex ante authorisations by data protection authorities are not practicable and should be required only in selective appropriate cases. Any 'legitimate interests' derogation should be based not on size or frequency but on risk-appropriate safeguards and a balancing against data subjects' rights and interests.

We have also noted other issues. The intended extra-territorial scope of EU data protection legislation needs careful definition. To avoid discouraging non-EU controllers and providers from using EU data centres and EU cloud providers or sub-providers, the status of data centres and hardware/software providers should be clarified explicitly, as should the key definitions of 'establishment', 'context of activities' and 'offering'. We support updating security requirements in line with general concepts of confidentiality, integrity and availability, but specific reference should be made to encryption and backups as example measures, to help raise user awareness. The requirements and scope of data protection by design and default also need clarification, and again they need to cater for infrastructure providers who may not necessarily know the nature of data processed using their infrastructure, and controllers and processors who may not have total control over relevant infrastructure. Clarification is also needed regarding the types of data breaches to be notified, thresholds and the detailed contents of any public register, but we support the deletion of 'hard' time limits. Processor representatives should be entitled to give input regarding codes of conduct, but more guidance is needed regarding certifications, codes and seals, and the provisions on certifications and seals could be merged. The right to data portability is very limited in scope, and this could be reconsidered, as well as its relationship with the right to erasure. Finally, new technologies should not be treated as risky per se – risks depend on their intended use and the type and sensitivity of the data concerned.

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this White Paper is to assess the implications of the current proposals for modernising the **Data Protection Directive**[1] (DPD), with a particular focus on assessing their likely impact on cloud accountability, and to make recommendations for amendments aimed at improving cloud accountability,[2] for submission to the European legislative institutions as a timely contribution to the reform process.

It analyses relevant provisions of the proposed new General Data Protection Regulation (**Reform Proposal**', which may refer to the various drafts as the context requires) based on the text of documents publicly available as at 14 Feb 2014, and in particular:

- The European Commission's proposed Regulation[3] (**Commission Draft**)
- Amendments by the European Parliament to the Commission Draft suggested in the report of its LIBE Committee[4] (**LIBE Draft**), and
- Amendments by the Council to the Commission Draft suggested in a 16 December 2013 note by the Lithuanian Presidency[5] (**Council Draft**). It should be noted that this document represents the latest draft being discussed within the Council, and the proposed amendments have not yet been agreed internally by the Council, which emphasises that 'no part of the proposed Regulation can be agreed until the whole text of the regulation is agreed'.[6]

After defining accountability for the purposes of this White Paper, we outline the scope of this White Paper. We then provide a brief overview of EU data protection law, and describe the legislative procedure involved in the current reform of EU data protection law to give insight into a realistic timeframe for adoption of the new law, which is likely to extend beyond 2014 and perhaps even beyond the lifetime of the A4Cloud project. Finally, we outline the key implications of the Reform Proposal (in its current state) for cloud accountability, bearing in mind that it may be in a state of flux for some time, and we make some recommendations on the Reform Proposal.

1.2 Accountability

For the purposes of the A4Cloud project, accountability will be understood in the data protection law context, as well as in relation to information that is not personal data, but in respect of which there is an obligation to some person to keep that information confidential (business sensitive information). Within this frame, the A4Cloud project has identified two legal elements:

- **Accountability obligations** - identification and specification at a conceptual level of the legal and regulatory characteristics of responsible stewardship by cloud and IT service providers of customer and user data, under data protection law and legal confidentiality obligations, and

[1] 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 [1995] OJ L281/31 (**DPD**).

[2] It may be noted that in several areas, various Member States have specifically queried the suitability of the Reform Proposal to cloud computing, or the extent it has taken cloud computing into account. Council Draft.

[3] Commission, 'Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM 2012 (011) final <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:en:NOT>.

[4] Committee on Civil Liberties, Justice and Home Affairs, European Parliament (rapporteur: Jan Philipp Albrecht), 'Report on the 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)' (2013) PE 501.927v05-00 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN>

[5] Council document 17831/13 <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2017831%202013%20INIT>

[6] Eg Council, '3244th Council meeting Justice and Home Affairs 6-7 June 2013' 10461/13, 9.

- **Delivery mechanisms** - legal structures and mechanisms which can be used to deliver effective accountability for such stewardship, such as contract, and enforcement mechanisms such as audits and fines.

The proposed measures to update the DPD aim both to expand accountability obligations and to bolster delivery mechanisms (particularly enforcement mechanisms) in relation to personal data in cloud computing. This White Paper deals only with reform of data protection law and does not address legal issues relating to confidential information that is not personal data.

1.3 Scope

This White Paper is aimed at non-lawyers. It does not cover the Reform Proposal's impact on cloud computing more generally, but will focus on the likely impact on cloud accountability. The A4Cloud project's working definition of cloud accountability is as follows:

> ***Conceptual Definition of Accountability:*** *Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.*
>
> ***A4Cloud Definition of Accountability****: Accountability for an organisation consists of accepting responsibility for the stewardship of personal and confidential data with which it is entrusted in a cloud environment, for processing, sharing, storing and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). In addition, it involves committing to legal, ethical and moral obligations, policies, procedures and mechanisms, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly.*

This White Paper will *not* cover the impact on cloud accountability of other proposed EU legislation, such as the EU cybersecurity strategy announced in Jan 2013, the draft Network and Information Security (NIS) Directive (proposing new requirements for cloud computing providers and others to notify data breaches to regulators), or the proposed Regulation on electronic identification and trust services for electronic transactions in the internal market.

'Data protection' in the legal sense, which is explained further below, is *not* the same as 'data protection' (or data loss prevention) in the technological sense, although there is some overlap. Also, in law, 'data protection' is not the same as 'privacy', although again they may overlap. Similar ground may also be covered by other laws on areas such as confidentiality obligations, or the right to private life under the European Convention on Human Rights. This White Paper deals only with the DPD and reform proposals affecting obligations under the DPD, and not with similar issues under other national or EU-wide laws.

2 EU data protection law – overview and legislative reform process

This section provides the background context for the subsequent discussion of proposed data protection law reform measures.

The DPD identifies three main classes of person to whom EU data protection law applies: **data controllers** ('**controllers'**), who are those persons who determine the purposes for which and the means whereby personal data are collected and processed; **data processors** ('**processors'**), who act under the instruction of controllers and do not themselves decide the processing purposes; and **data subjects**, the individuals whose personal data is being processed. Data protection law in the EU is addressed mainly by the DPD, which was adopted in 1995.[7] Accountability obligations may be owed to national data protection authorities ('**DPAs'**) as well as to data subjects. The DPD was intended to promote the free flow of personal data within the EU whilst preserving the privacy of individuals (ie **data subjects**) by ensuring a consistently high level of data protection across the EU. In fact, the DPD applies within the whole of the European Economic Area ('**EEA**'), ie the EU plus Iceland, Liechtenstein and Norway (and references in this White Paper to 'Member States' and 'EU' will be taken to include

[7] n 1.

those countries). A Directive is not directly applicable in EU Member States, who generally need to implement the Directive by passing local laws.[8] In contrast, a Regulation becomes directly enforceable as law in Member States on its effective date, without their having to take any action to implement it nationally. Directives can be maximum harmonisation or minimum harmonisation measures. With maximum harmonisation, Member States are not allowed to exceed the Directive's requirements. With minimum harmonisations, Member States may impose further requirements, going beyond the ones set out in the Directive, if they so choose. The DPD is a minimum harmonisation Directive. Also, some Directives may give Member States specific discretion to implement certain issues as they think fit, and furthermore there may be room for interpretation where the drafting is not completely clear. This means that, although EU legislation generally aims to harmonise laws in certain areas across Member States, normally there are differences in implementation, and the DPD is well known for having been implemented inconsistently by different Member States. For example, Belgium and the Czech Republic impose data protection obligations directly on processors, going beyond the DPD, whereas most other Member States impose such obligations only on controllers. As another example, Italy has laid down detailed security requirements for personal data, whilst the UK's security requirements are brief and general, relying on the principles stated in the DPD.

The EU data protection regime applies only to '**personal data'**, information relating to identified or identifiable natural persons. No data protection rules will apply at all where data are not 'personal data' but are 'anonymous' data, ie (according to Rec 26 of the DPD) 'data rendered anonymous in such a way that the data subject is no longer identifiable'. Conversely, where data are 'personal data', the whole regime regarding personal data applies irrespective of context or degree of risk, with additional specific rules applying where personal data belong to so-called 'special categories' personal data (often called '**sensitive data**), eg data on health, ethnicity or sex life. Processing of sensitive data is in principle prohibited, and there are additional rules allowing their processing only in restricted circumstances. The definition of 'personal data' has caused practical concerns given the increasing ease of identifying individuals from supposedly 'anonymous' data, and anonymisation and pseudonymisation are likely to be much debated in relation to the Reform Proposal.[9]

With certain exemptions,[10] the DPD directed Member States to impose legal obligations on **controllers** to protect personal data by complying with certain principles when processing personal data. These principles, in brief, require the following (again, subject to various exceptions).[11] Processing of personal data must be fair and lawful. Personal data must be collected for specified lawful purposes only, and be adequate, relevant and not excessive for those purposes. Personal data must be accurate and kept updated as necessary, not be kept for longer than required for the purpose, processed in accordance with certain data subject rights, eg to access their own personal data, secured against unauthorised or unlawful processing, and not transferred to a country outside the EU that does not ensure an adequate level of protection. In order to meet the fair and lawful processing requirement, controllers must give individuals notice of the processing (to the extent they do not have it already) and meet one of the conditions required to render the processing lawful. These include data subject consent, or where the processing is necessary to perform a contract to which the data subject is party, to comply with a legal obligation, or for the purposes of the legitimate interests of the controller or the third party or parties to whom the data are disclosed. A controller may engage a '**processor**' to process personal data for it, but it must choose a processor providing 'sufficient guarantees' in respect of the technical security measures and organisational measures governing the processing to be carried out, and the controller must ensure compliance with those measures. Furthermore, the controller's contract with the processor must be in writing, and must require the processor to act only on the controller's instructions and to take certain security measures. As mentioned above, most Member States impose data protection obligations only on controllers (eg, to ensure that their contracts with processors meet the preceding requirements). Because few Member States impose data protection obligations directly on processors, in most Member States processors are accountable only to controllers under the controller-processor contract.

A controller who uses cloud computing to process personal data remains responsible for the data under data protection laws. Although cloud services typically involve self-service use of a third party provider's computing resources, providers would normally be regarded as 'processors' because even

[8] Eg Personal Data Act 1998 (Personuppgiftslagen 1998:204) (SE) and Data Protection Act 1998 (UK).

[9] See 4.1 below.

[10] Eg processing activities for national security, and 'purely personal or household activity'.

[11] Eg for journalistic purposes or artistic or literary expression.

passive, temporary storage of personal data is considered 'processing', regardless of whether the provider *knows* that stored data are personal data.[12] Data transmission or disclosure is also 'processing'. A provider may even be considered a controller, with correspondingly greater legal obligations, if it uses for its own purposes personal data stored by a cloud user, or discloses such data to third parties without the controller's authority. Any contractual designation of the parties' status, eg that the provider is only a processor, is relevant but not determinative of the legal status of the provider, because factual circumstances are important in attributing the roles above.[13],[14]

The role of the **Article 29 Data Protection Working Party** ('A29WP') merits mention. This group was set up under DPD Art 29. It is an independent body, tasked to advise on issues such as harmonisation of national measures, level of protection in the EU and other countries, codes of conduct and other data protection issues. Its members comprise national DPAs and the **European Data Protection Supervisor** ('EDPS'), who regulates EU institutions' data protection compliance.[15] Therefore, the A29WP's opinions, such as on cloud computing (**WP196**),[16] are very influential. However, courts, Member States and DPAs are not legally required to follow these opinions, and, because its decisions are approved by simple majority, an individual regulator who disagrees with the majority may decide not to follow the A29WP's interpretation. Under Commission Draft Arts 64-72, the A29WP would become the **European Data Protection Board** ('EDPB'), with enhanced role and powers.

In brief, for the Reform Proposal to be adopted, the legislative text must be agreed between the Commission, European Parliament (elected members, ie MEPs) and the Council of Ministers (comprising representatives of EU member state governments at ministerial level), each of whom have been considering it separately.[17] the European Parliament's Civil Liberties, Justice and Home Affairs Committee ('**LIBE**') has approved a report proposing certain changes (agreed between the Parliamentary committees involved) to the Commission Draft. The full Parliament in plenary session is expected to adopt the LIBE Draft in April 2014.[18] The Council is still discussing amendments to the Commission Draft. If the three EU institutions cannot agree on a legislative text before the May 2014 European Parliament elections, the next Parliament will decide whether to continue with the proposals. The Commission is also changing membership in autumn 2014. Therefore, if the text is not agreed by all three EU institutions before May 2014, as recent reports indicate may be the case, the fate of the

[12] W. Kuan Hon, Christopher Millard and Ian Walden, 'The problem of "personal data" in cloud computing: what information is regulated?—the cloud of unknowing' (2011) 1(4) International Data Privacy Law 211 <http://idpl.oxfordjournals.org/content/1/4/211.full>; updated version 'What Is Regulated as Personal Data in Clouds?', Ch 7 in Christopher Millard (ed), *Cloud Computing Law* (OUP 2013).

[13] A29WP, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) WP169 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf>.

[14] W. Kuan Hon, Christopher Millard and Ian Walden, 'Who is responsible for "personal data" in cloud computing? - The cloud of unknowing, Part 2' (2012) 2(1) International Data Privacy Law 3 <http://idpl.oxfordjournals.org/content/2/1/3.full>; updated version 'Who Is Responsible for Personal Data in Clouds?', Ch 8 in Millard (n 12).

[15] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1.

[16] A29WP, 'Opinion 05/2012 on Cloud Computing' (2012) WP196 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf> (**WP196**).

[17] In more detail, each EU institution considers the Commission's legislative proposals and discusses it during one or two 'readings' in order to reach consolidated views internally. They may propose amendments, and the Commission may produce amended text in consequence. If the three institutions cannot agree the legislative text after two readings, the proposals are considered by a Conciliation Committee (comprising equal numbers of representatives of the Council and Parliament, with Commission representatives also involved). If this Committee reaches agreement, the agreed joint text will return to Parliament and the Council for a third reading. Even at this stage, Parliament may still reject the joint text by a majority of votes cast. The conciliation procedure is also known as a 'Third reading'. The latest European Parliament statistics show that 3% of agreements went through the conciliation procedure between July 2009 and March 2013 and took an average of 29 months to complete - European Parliament, 'Conciliations and Codecision - Statistics on concluded codecision procedures (by signature date)' (Europarl) <http://www.europarl.europa.eu/code/about/statistics_en.htm> accessed 25 February 2014. A flowchart of the ordinary legislative procedure (formerly called the codecision procedure) is available at <http://www.europarl.europa.eu/external/appendix/legislativeprocedure/europarl_ordinarylegislativeprocedure_howitworks_en.pdf>.

[18] Eg Commission, 'Data Protection Day 2014: Full Speed on EU Data Protection Reform' (27 January 2014) MEMO/14/60 <http://europa.eu/rapid/press-release_MEMO-14-60_en.htm>.

Reform Proposal is uncertain, although there may be political will to adopt it before the end of 2014.[19] Appendix 1 details the history and background to the current proposals to reform EU data protection law, the legislative procedure and its current status, including the position if the Reform Proposal is not adopted before the May 2014 elections.

The DPD, a much less complex measure than the Reform Proposal, was first proposed in 1990 but was not finally adopted until 1995. Moreover, at that time there were only 15 Member States. Given such experience, the end of 2014 looks very optimistic for finalising the Reform Proposal, particularly as 28 Member States will be involved in the process of settling what have, so far, been highly controversial proposals. Indeed, reportedly one high-level representative of a Member State government considers that it may take up to 10 years to complete the legislative procedure![20]

3 Impact of proposed reform on cloud accountability

3.1 Overview

This section covers the general implications of the Reform Proposal for cloud accountability.

3.2 Accountability obligations

The Reform Proposal will change some accountability obligations, modify accountability relationships and create new relationships, including new non-contractual accountability obligations for third parties. Although the Commission Draft does not include the term 'accountability' in its text, Art 22 of the Commission Draft[21] 'takes account of the debate on a 'principle of accountability' and details the obligation of the controller 'to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance'.[22] Moreover, one major policy objective of the reform of the data protection framework was to strengthen responsibility and accountability for the processing of personal data:[23]

> *The proposals place clear responsibility and accountability on those who are processing personal data, throughout the information life cycle. In the Regulation, we have included incentives for controllers to invest, from the start, in getting data protection right. For example, we have foreseen data protection impact assessments, data protection by design and data protection by default, which will encourage data controllers to think about data protection from the very beginning when designing new applications or services. We have also clarified and strengthened citizens' rights. We clarify the notion of consent, introduce a general transparency principle and enhance redress mechanisms. And we introduce an obligation to notify clients or users in the event of a data breach which will apply to all sectors.*[24]

We list below the key aspects of the Commission Draft that would be likely to have an impact on 'accountability' obligations. Data subject rights would be enhanced, including greater transparency such as broader obligations regarding information required to be given to data subjects, but in this White Paper we focus on the proposed new rights regarding data breach notification, certifications,

[19] Eg Nikolaj Nielsen, 'EU data bill delayed until after May elections' *EUobserver* (Brussels, 24 January 2014) <http://euobserver.com/justice/122853> accessed 25 February 2014. See also Viviane Reding, 'A data protection compact for Europe' (CEPS, Brussels, 28 January 2014) SPEECH/14/62: 'European leaders could only agree to complete the data protection reform in a "timely" manner, and at the latest by the end of 2014' <http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm>

[20] Cedric Burton, Christopher Kuner and Anna Pateraki, 'The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report' (2013) 12 Privacy & Security Law Report 99 <http://www.wsgr.com/publications/PDFSearch/proposed-EU-0113.pdf>.

[21] Entitled 'Responsibility of the controller'.

[22] Commission Draft [3.4.4.1].

[23] Commission Staff Working Paper, 'Impact Assessment' SEC(2012) 72 final, 116 <http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf>: 'A central objective of the data protection reform package is to increase the effectiveness of data protection rights, by enhancing the responsibility and accountability of data controllers'. See also Appendix 1.

[24] Viviane Reding, 'Strong and independent data protection authorities: the bedrock of the EU's data protection reform' (Spring Conference of European Data Protection Authorities, Luxembourg, 3 May 2012) SPEECH/12/316 <http://europa.eu/rapid/press-release_SPEECH-12-316_en.htm>.

seals and codes of conduct, erasure and data portabiliity. We also cover other provisions which could affect legal accountability obligations in a broader sense, although not explicitly described by the Commission as such. Each of the key issues listed below will be covered in more detail later:

Who is accountable and in what circumstances?

1. Personal data definition
2. Controller accountability
3. Processor obligations and joint controllers
4. Jurisdictional applicability of data protection law

Internal accountability measures

5. Security requirements
6. Privacy by design and default
7. Data protection impact assessments (‘**DPIAs’**)
8. International data transfers

External accountability measures - data subject rights

9. Data breach notification
10. Certifications, seals and codes of conduct
11. Right to erasure
12. Data portability.

3.3 Delivery mechanisms

In terms of delivery mechanisms, the key changes would also affect *to whom* accountability obligations would be owed, and *how.* One major change would involve enhancing national DPAs' independence and powers, including the controversial ability to impose fines (administrative sanctions) of up to 2% of global turnover in certain circumstances (which LIBE would increase to 100 million euros or 5% of global turnover if higher,[25] while the position is still being debated by the Council), and investigatory powers for DPAs. Both LIBE (Art 29(2c)) and the Council (Art 79(2a)) would introduce explicit criteria to be considered when determining the type, level and amount of sanctions, including the degree of responsibility of the natural or legal person and their previous infringements and the technical and organisational measures and procedures taken for privacy by design or default and security – ie, any accountability measures implemented. The Council would take account of adherence to codes of conduct or certification mechanisms (Art 79(2a)(j)) and would limit administrative sanctions to situations involving intentional or negligent default (Art 79a), whereas LIBE would allow lack of negligence or intention to be taken into account only in imposing fines on those with European Data Protection Seals.[26]

The Commission Draft also aims to make authorities' roles and powers more consistent across Member States. It would create a ‘one-stop shop' for controllers or processors which operate in multiple Member States based on the controller or processor's ‘main establishment' in the EU (so that it should have to answer to only one national authority, effectively), and establish a ‘consistency mechanism' to harmonise data protection rules better across the EU. Data subjects would be able to complain to the data protection authority of any Member State (Article 73(1)), not necessarily the State of their residence or the relevant controller or processor's establishments (whereas they could only sue in one of the latter two States – Article 75). However, the one-stop shop concept has proved controversial and is still in a state of flux.

[25] Art 79(2a).

[26] LIBE Draft Art 79(2a)-(2c); Council Draft Arts 79(2a), 79a

3.4 Summary of LIBE and Council positions

Although the LIBE Draft would ease restrictions for controllers in a few specific areas, in general LIBE wishes to enhance data subject rights[27] and restrict processing of personal data further. Accountability obligations would be expanded and delivery mechanisms reinforced as shown, for example, through requirements to conduct data protection impact assessments, consult competent authorities prior to certain processing of personal data, and provide evidence of top management commitment. The EDPS recognised 'the need for introducing more flexibility in respect of organisations that have put in place accountability mechanisms, such as the appointment of a data protection officer (DPO) or the implementation of recognised certification mechanisms.'[28] In the Council, at least some Member States would prefer a Directive to a Regulation. The Council has been concerned about the impact of the proposals on SMEs and public sector processing, desiring a more risk-based approach and greater flexibility for the public sector. This approach would imply more prescriptive obligations should apply where the risk is high, and conversely fewer obligations where the risk is low. The EDPS stressed that the Council Draft's amendments regarding Art 22 of the Commission Draft on accountability aim to give more importance to the notion of accountability.[29] Commissioner Reding has indicated that she will make some concessions. The Commission is willing to consider ways to cut red tape further without affecting protection for personal data, by introducing a more flexible, risk-based approach taking into account quantity and sensitivity of data processed, broader exemptions for SMEs, and less prescriptiveness. The Commission is willing to allow more flexibility for public sector processing, acknowledging that specific rules for the public sector might be necessary sometimes, for instance in the case of a land registry which should be public. Nevertheless, it was adamant that there should be no general exemption for the public sector, giving the example of a local authority uploading personal data to a cloud provided by a private company, and citing numerous previous data breaches in the public healthcare sector.[30]

One overarching issue requires particular mention. A notable feature of these proposals is that they would give the Commission extensive powers to adopt further delegated or implementing acts ('**Commission empowerments'** or '**empowerments'**), whereby the Commission may prescribe further detailed requirements, criteria and/or conditions, or prescribe standard forms and standard procedures, regarding virtually all the areas described further below. Therefore, if any relevant proposed Commission empowerments are included in the legislation ultimately, it would be necessary also to consider the text of those future delegated or implementing acts. Both Parliament and Council have been united in opposing the large number of possible Commission empowerments, wishing to delete them or to empower the EDPB instead (which would replace the A29WP), or to require consultation with the EDPB. The A29WP has also raised objections, stating that 'adoption of implementing acts increases the prescriptive nature of the EU data protection framework, which may not be fully consistent with the introduction of the principle of accountability which aims at entrusting controllers with the practical aspects of complying with data protection obligations.'[31] Given the scale of the resistance, the Commission has indicated its willingness to review the proposed delegated acts individually, which could reduce its empowerments (ie the Commission's ability to adopt further rules

[27] In this context, LIBE requests more transparency with respect to the use of consent as the legal ground for lawful processing (Art 6), in particular on the 'reasons for believing that the interests of processing override the interests or fundamental rights and freedoms of the data subject.'

[28] EDPS, 'Additional EDPS comments on the data protection reform package' (2013) [31] <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf>.

[29] Ibid.

[30] Viviane Reding, 'Justice Council: Making good progress on our Justice for Growth agenda' (Justice Council Press Conference, Luxembourg, 26 October 2012) SPEECH/12/764 <http://europa.eu/rapid/press-release_SPEECH-12-764_en.htm> and Viviane Reding, 'The overhaul of EU rules on data protection: making the single market work for business' (3rd Annual European Data Protection and Privacy Conference, Brussels, 4 December 2012) SPEECH/12/897 <http://europa.eu/rapid/press-release_SPEECH-12-897_en.htm>. The A29WP also considers the public sector does not need more flexibility and there should not be a public/private sector distinction: A29WP, 'Statement of the Working Party on current discussions regarding the data protection reform package' (2013) 1 <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_reform_package_en.pdf>.

[31] A29WP, 'Input on the proposed implementing acts' (2013) WP200, 3 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp200_en.pdf>.

unilaterally) by up to 40%.[32] Therefore, generally this White Paper discusses only empowerments that are not opposed by LIBE and the Council and that are relevant to cloud accountability.

4 Specific cloud accountability issues

4.1 Personal data definition and pseudonymous data

4.1.1 Provisions

The concept of 'personal data' is central to data protection law, triggering the application of EU data protection laws: if information is 'personal data', then such laws apply to it; if it is not 'personal data', for example because it is 'anonymous' data which no longer identifies the data subject, then it may be processed without regard to such laws.[33] Data protection law accountability thus relates to, and only to, 'personal data'. All three EU institutions wish to encourage controllers to anonymise or pseudonymise personal data and thereby better protect data subjects while enabling processing – clearly a desirable goal, and in line with a risk-based approach.[34] Thus, Rec 23 would continue to recognise DPD Rec 26 concepts of anonymous data and anonymisation. LIBE would also explicitly cover means used to 'single out the individual directly or indirectly'; an important and necessary addition as individuals may now be tracked and singled out for differential treatment without their names or identities necessarily being known, provided the meaning of such singling out is clarified (eg action or inaction detrimentally affecting that individual materially). Both LIBE and the Council would, correctly, require account to be taken of 'all objective factors', such as costs, time required for identification, and available technology.

Both LIBE and the Council want further consideration of the treatment of anonymous data or pseudonymous personal data (and the personal data definition). One attempt to 'calibrate' data protection obligations in a more nuanced way, while maintaining protection,[35] is through a 'halfway house' concept of 'pseudonymous data', which both LIBE and the Council would introduce: namely, personal data that 'cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution' (Article 4(2a)).[36] The definition of 'pseudonymous data' is not without controversy.[37] The position remains unresolved, the critical issues being whether use of the concept is the best way to calibrate obligations, and if so which obligations should be reduced, and in what way, when processing pseudonymous data? Currently, under DPD Article 7(f), processing is permitted (amongst other justifications) where necessary for the purposes of legitimate interests pursued by the controller or third party to whom data are disclosed, unless overridden by data subjects' interests or fundamental rights. The Commission Draft would continue this concept (Rec 38, Article 6(1)(f)), although reference to legitimate interests of any *processor* should also be added, such as in Rec 39 on processing for network security, which is particularly important for the Internet and cloud computing.[38] LIBE would add another requirement, that processing based on legitimate interests must 'meet the reasonable expectations of the data subject based on his or her relationship with the controller';[39] but, provided data subject interests or fundamental rights are not overriding, processing limited to pseudonymous data would be *presumed* to meet data subjects' reasonable expectations. Generally, careful consideration needs to be given to what other obligations should be adapted for pseudonymous data. As scientific and research developments have made it more difficult

[32] Reding (SPEECH/12/764) n 30.
[33] DPD Rec 26.
[34] Commission Draft 200; LIBE Draft 200; Council document 17971/13 [3].
[35] Council (n 34) [3] – and strengthen a risk-based approach, ibid [5].
[36] The Council's formulation is slightly clearer.
[37] Several Member States have reservations, two query the necessity for the concept, one considers the definition so strict as to make pseudonymous data 'tantamount to anonymous data'. Council Draft fn 31; Council (n 34) [5]: one option is to replace 'pseudonymous data' with reference to a pseudonymisation process supporting compliance.
[38] It seems odd that processing for email spam filtering purposes is not specifically mentioned as permitted, either.
[39] But would this cover situations where there is no such pre-existing relationship? A better formulation may be, 'reasonable expectations of the data subject, including reasonable expectations based on any pre-existing or expected future relationship between the data subject and the controller..'

to truly anonymise personal data and guarantee anonymisation, and easier to re-identify data subjects from 'anonymous' data, more and more data may fall within the 'pseudonymous' rather than 'anonymous' category.

Another important foundational issue relates to the concept of access to *intelligible* personal data. The Commission Draft, like the DPD, largely seems to assume that, as with paper files, whoever has access to the 'file', or personal data, must invariably have access to intelligible personal data, eg DPD Art 16. However, with data such as encrypted personal data, persons with access to data will not have access to *intelligible* data, unless they also have access to the decryption key, or can break the encryption. The A29WP takes the view that encrypted personal data are always 'personal data',[40] without considering the relevance of how strongly the data may be encrypted, who has access to the key, and how securely the key is managed. Encrypted personal data should certainly remain 'personal data' to someone with the decryption key, such as a controller who encrypts data before upload to the cloud and who should remain accountable for the data, including ensuring appropriate backups to protect integrity and availability (discussed further below), dealing with subject access requests, etc. Encrypted personal data might well qualify as 'pseudonymous data' under the Reform Proposal (and this issue could be clarified). However, we consider that encrypted personal data should not be treated as personal data as regards those *without* the key, such as a cloud provider who may not know that encrypted data stored on its (or its sub-provider's) infrastructure, uploaded by its customer in self-service fashion, would constitute personal data when decrypted.[41] It seems unfair to hold cloud providers or other processors liable as 'processors' under the Reform Proposal, if they do not know that encrypted data stored on their infrastructure are personal data. Given the importance of 'personal data' as the trigger for the application of data protection laws, we strongly recommend that the opportunity should be taken to clarify that *access* to *intelligible* personal data should be a pre-requisite to such application, eg by amending the definition of 'personal data' or the definitions of 'data controller' and 'data processor' accordingly. The fundamental purpose of these laws is to protect personal data from use or disclosure prejudicing the privacy of data subjects.[42] However, neither use nor disclosure is possible without access to *intelligible* personal data, and we argue that it is inappropriate to impose data protection law obligations on those without such access. Data protection laws should only regulate those with access to intelligible personal data.[43]

It is true that encryption protects only data confidentiality, so that someone with access to encrypted personal data, but without the ability to decrypt the data to access intelligible personal data, could nevertheless corrupt or delete the encrypted data deliberately or inadvertently, thereby undermining data integrity or the availability of the data to the controller. However, this risk can and should be addressed as part of the controller's security obligations.[44] The controller who originally encrypted the data knows what the data are, has the decryption key, and should remain primarily responsible for protecting the encrypted data. Backups are a standard means of protecting data integrity and availability, with best practices involving taking different backups at different times to different locations, which in cloud computing could include taking backups internally and to different cloud services and/or geographical locations, with some services offering users the technical capability to automate their backups. Therefore, general obligations to ensure the security of personal data, and particularly in the form proposed by LIBE,[45] should suffice to require controllers to take backups of their encrypted personal data to different providers' infrastructure and/or locations (and to back up their keys), or to take other appropriate measures to protect data integrity and availability.

It is also true that some encryption methods have been broken, some encrypted data could be 'brute force' decrypted in time, and that a nation state that specifically targets certain encrypted data will probably be able access to access intelligible data through methods other than breaking decryption

[40] WP196 [3.4.3.3].

[41] Hon, Millard and Walden (n 12), and see 4.3.

[42] Commission, 'Communication on the protection of Individuals In relation to the processing of personal data In the Community and Information security' COM 1990 (90) 314 final SYN 287 and 288, generally including 34-35, 37; Commission, 'Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data' COM (92) 422 final SYN 287, 10.

[43] Even with technical ability to access intelligible personal data, eg because data are in unencrypted form, the position of cloud infrastructure providers who are mere intermediaries should be taken into account, as discussed in 4.3.

[44] Security obligations generally are discussed in 4.5.

[45] Ibid.

(eg obtaining the data at the 'endpoints' before encryption or after decryption, or tapping providers' internal cables transmitting unencrypted data). However, that does not mean that controllers should not apply encryption. On the contrary, controllers should be positively encouraged to implement measures such as encryption in order to secure personal data better. The more widely that encryption, even weak encryption, is applied, the costlier and more difficult it will be for those who seek to access intelligible data en masse.[46] Even though physical locks may be broken or doors kicked in, the vast majority of people still lock their doors, and rightly so.

Furthermore, in many situations data in the cloud must remain unencrypted in order to be useful, eg for operations such as indexing data to enable searching by the user. Here, tools such as encryption gateways or tokenisation gateways,[47] equipment at the user's premises which preserve some functionality such as searching but allow only encrypted or tokenised data to be processed in the cloud, are relevant, while much research effort is being directed towards finding practicable means to operate on data while remaining encrypted, so-called 'homomorphic encryption'.[48]

A related issue relates to deletion of personal data in digital form. Digital data are not 'handed over', but copied to other equipment or media, and deleted from previous equipment or media. Different degrees of deletion are possible: merely deleting 'pointers' to the fragments, stored in different physical locations (on the same or different storage equipment or media), which together comprise the data, with fragments being overwritten by other data over time; overwriting the fragments, with different overwriting methods being possible and multiple overwriting being more thorough than one 'pass'; and even destroying physical equipment used to store the fragments.[49] Provisions that implicitly aim to remove an actor's or actors' access to *intelligible* personal data, by requiring data eg to be 'erased', deleted or 'restricted',[50] or referring to 'data in a form that permits identification',[51] do not specify what degree of deletion would be good enough. We suggest that the solution, for technology-neutrality and a risk-based approach, is not to specify detailed degrees of deletion or restriction, or perhaps even to require erasure or deletion at all, but simply to require removal or restriction of the relevant actor's access to intelligible personal data to an extent and in a way that is appropriate to the risks involved in the particular circumstances.[52]

Finally, although anonymisation and pseudonymisation are to be encouraged as ways to reduce risks to data subjects,[53] it is uncertain whether the very procedure of anonymising or pseudonymising personal data itself constitutes 'processing', thereby requiring legal justification. If this procedure is considered 'processing', controllers may be discouraged from anonymising or pseudonymising data.[54] We therefore welcome the Council's proposed statement that anonymisation etc could constitute a legitimate interest of a controller.[55] However, this should also refer to processors, and state explicitly

[46] Indeed Edward Snowden, who blew the whistle on mass surveillance and wholesale data collection by the US National Security Agency and other intelligence agencies, stated that encryption was one of the few safeguards that could be relied on: 'properly implemented strong encryption works.' Edward Snowden, 'Edward Snowden: NSA whistleblower answers reader questions', The Guardian (London, 17 June 2013, 12.12 pm) <http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower> accessed 25 February 2014. See also Bruce Schneier, 'NSA surveillance: A guide to staying secure', The Guardian (London, 6 September 2013) <http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance> accessed 25 February 2014.

[47] W Kuan Hon and Christopher Millard, 'Control, Security, and Risk in the Cloud', Ch 2 in Millard (ed) (n 12), 22.

[48] Ibid, 20.

[49] Ibid, 24.

[50] Eg the Commission Draft refers to deletion in Rec 30, and (mainly) to 'erasure' in the provisions on the right to erasure (see 4.11) and in Recs 47, 48, 59, 129, Arts 4(3) ('processing' definition), 5(d), 13, 14(1)(d), 15(1)(e), 28(2)(g), 31(6), 53(1)(f), 79(5)(c); LIBE Draft's references to deletion in Recs 71a, 71b, Arts 23(1), 26(2)(g), 33(3), 82(1c); and Council Draft Recs 55, 125, 126, 129.

[51] Commission Draft Art 5(1)(e), echoing DPD Art 6(1)(e).

[52] Eg, sensitive data may require overwriting multiple times using more secure methods, while non-sensitive personal data may be adequately protected by deleting pointers coupled with contractual terms restricting the provider from reading or attempting to re-unite the consituent fragments.

[53] Eg Article 5(1)(c) Commission Draft would state expressly that personal data shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data – ie by processing pseudonymous or anonymous data. LIBE would explicitly term this 'data minimisation'.

[54] Hon, Millard and Walden (n 12).

[55] Rec 39. But it could be more emphatic ('would' include, or explicitly permitting such processing). Council (n 34) [4] second bullet suggests that its proposed insertion applies 'provided that the interests or the fundamental rights and freedoms of the data subject are not overridden', but that wording does not appear in Council Draft Rec 39.

that measures to secure confidentiality, integrity or availability of data[56] are permitted as being in the legitimate interests of controllers and processors.

4.1.2 Summary and recommendations

Because being classified as 'personal data' triggers the application of data protection laws, the Reform Proposal presents the opportunity to re-consider which kinds of data and uses should be regulated and how, such as singling out an individual for differential treatment based on their personal data. Since data are now much more easily linked to individuals than in the 1990's, far more data would qualify as personal data. If the test is set very broadly so that most information is 'personal data', then the obligations applicable need to be more carefully calibrated, as the Council has noted. Introducing the concept of pseudonymous data is one way, with fewer obligations applying to such data, but its definition needs care, and the obligations that are to be adapted for pseudonymous data should be considered carefully, as much data would be likely to fall within the 'pseudonymous' rather than 'anonymous' category. We support the aim of encouraging anonymisation or pseudonymisation of personal data. It should be made clear that the procedure of anonymisation or pseudonymisation is permitted (without any further legal justification) as well as the procedures of encryption and decryption. More fundamentally, EU data protection laws would be made more technologically-neutral and fair if they regulated only those who have access to *intelligible* personal data,[57] and how and to what extent such access should be removed or restricted in various circumstances based on appropriateness to the risks involved.

4.2 Controller accountability

4.2.1 The provisions

Under DPD Art 2(d), the controller is the entity that determines the 'purposes and means' of processing personal data. The Commission Draft would add to these, '*the conditions*' of processing. It is unclear what this would add and both the Council and LIBE would delete 'the conditions'.[58] We agree. Furthermore, it would seem timely to consider whether, from a policy perspective, 'means' is necessary, particularly as the Reform Proposal would regulate processors separately. Determining purposes seems widely-accepted as the critical criterion for controllership,[59] and the 'means' criterion has resulted in many problems in practice with distinguishing between controllers and processors. Arguably 'means' should be, not a criterion of controllership, but an *obligation* on controllers: ie, those who qualify as controllers, because they determine the processing purposes, should be obliged to process personal data in such a way as to comply with data protection laws, ie they should ensure that the processing *means* that they choose to use are such as to facilitate compliance (eg by implementing security measures).

Under Commission Draft Art 5(1)(f), personal data must be processed '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'.[60] LIBE would explicitly term this requirement 'accountability' and emphasise that the controller 'shall ensure and be able to demonstrate' compliance.[61] The Council would replace this provision simply with 'The controller shall be responsible for compliance with paragraph 1', ie the fundamental data protection law principles (Art 5(2)). Art 22, generally considered to be the main accountability provision, does not use the term 'accountability, but

Also, it is hard to see how anonymising or pseudonymising data would prejudice, rather than enhance, protection of data subject rights.

[56] Security requirements are discussed at 4.5 below.

[57] W Kuan Hon, 'Cloud Computing: Geography or Technology - Virtualisation and Control' (*Society for Computers and Law*, 2014) <https://www.scl.org/site.aspx?i=ed35439> accessed 25 February 2014.

[58] In the LIBE Draft, 'conditions' is also deleted from Art 24, 'conditions and means' from Rec 62, but only 'conditions' from the operative Art 4(5), while neither were deleted from Art 4(13). It is unclear whether the deletion of 'and means' was inadvertent.

[59] A29WP (n 13) 13. And see 4.3.

[60] Reflecting the A29WP view of accountability as ability to demonstrate compliance with rules – A29WP, 'Opinion 3/2010 on the principle of accountability' (2010) WP173 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf>.

[61] Generally, rather than per processing operation.

'takes account of the debate on a 'principle of accountability'' and details the controller's obligation to comply and to demonstrate compliance, 'including by way of adoption of internal policies and mechanisms for ensuring such compliance'.[62] Accordingly, Art 22 would require controllers to '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'. LIBE would, again, add express references to 'accountability' and 'transparent' demonstration and clarify that 'measures' means 'demonstrable technical and organisational measures'. Both LIBE and the Council would qualify 'policies' with 'appropriate'.[63] They emphasise a risk-based, contextual approach to 'policies' and 'measures', requiring regard to be had to the nature,[64] context, scope and purposes of processing, risks to data subjects' rights and freedoms, and (in LIBE's case) type of organisation. LIBE also wants regard to be had to the state of the art, at both the 'time of determination of the means of processing'[65] and the time of processing. The Council would delete 'to ensure', which seems to reflect better the risk-based approach: it is impossible to provide an absolute guarantee of total compliance; all that can be done is to take the measures most appropriate to the specific circumstances, in particular in light of the risks posed. Neither LIBE nor the Council would add 'cost of implementation' as a relevant factor here. However, both implementation cost and state of the art are expressly mentioned in a new Art 22(1a) proposed by LIBE, requiring the controller to take 'all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices[66] of data subjects'.[67]

Additionally, under Commission Draft Art 22(3), controllers must implement mechanisms to 'ensure the verification of the effectiveness of [such] measures', and 'If proportionate, this verification shall be carried out by independent internal or external auditors.' This means an audit requirement would apply to controllers, 'if proportionate'. The Council would change this to enable a controller to demonstrate compliance with its obligations[68] by means of adherence to codes of conduct or a certification mechanism (Art 22(2b)). This seems a positive way to incentivise controllers to adhere to codes etc.[69] However, LIBE would retain the verification provision, but require controllers to 'demonstrate the adequacy and effectiveness of the measures'. This seems superfluous; such wording may be better added to Art 22(1). LIBE would also delete the audit requirement, instead requiring in Art 22(3) that 'Any regular general reports of the activities of the controller, such as the obligatory reports by publicly traded companies, shall contain a summary description of the policies and measures referred to in paragraph 1'. It is difficult to see how a summary description could be meaningful, but conversely providing too much information about security measures may itself undermine security.[70]

[62] Commission Draft 10.

[63] The Council would replace the obligation to adopt policies with a requirement that the measures 'shall include the implementation of appropriate data protection policies by the controller' where proportionate to the processing - Art 22(2a). Four Member States had reservations on the whole chapter including Art 22. One felt that Art 22 was unnecessary as it overlapped with existing obligations, and focused overmuch on procedures rather than outcomes. There was concern that the Commission Draft would not reduce controllers' compliance burdens/costs, and that the obligation was too vague and the risk concept insufficiently detailed, without exceptions for SMEs or social media users. Council Draft fn 187-194.

[64] The nature of personal data processing specifically, in the LIBE Draft. Recommendation: delete this qualification, because the nature of the data (eg sensitive data) should be considered, not just the nature of the processing.

[65] Surely this should be purposes? See paragraph containing n 59.

[66] This wording is also used in relation to DPIAs – see 4.7. However, it is unclear what 'respecting' the 'autonomous choices of data subjects' means and what this provision would add; perhaps this was intended to refer to data subjects' rights under the legislation.

[67] To be reviewed for updates every 2 years.

[68] It is unclear which obligations are meant – presumably obligations under Art 22(1), rather than the whole Reform Proposal?

[69] The importance of incentivising controllers to comply, at least regarding codes of conduct and technological protection measures, is also in principle recognised by LIBE. LIBE Draft explanatory memorandum 206 and 208.

[70] W Kuan Hon, Christopher Millard and Ian Walden, 'Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now', 16 Stanford Technology Law Review 81 (2012) <http://stlr.stanford.edu/2013/01/negotiating-cloud-contracts> accessed 25 February 2014, updated version 'Negotiated Contracts for Cloud Services', ch 4 in Millard (n 12), [5.5.1].

4.2.2 Summary and recommendations

We support deleting the proposed additional criterion of determining 'conditions' of processing.[71] We further recommend considering whether 'means' should be deleted also, particularly as explicit obligations on processors are to be introduced. There seems common ground that the accountability obligation relates to taking concrete measures towards compliance. Both LIBE and the Council seem to recognise that 100% compliance is impossible, so that measures must be appropriate to the circumstances. It is important to consider what factors should be taken into account, including whether policies as well as measures should be required,[72] and to what extent implementation costs and the state of the art should be taken in to account. We support the LIBE Draft here.[73] Regarding how compliance may be demonstrated, there seems too much uncertainty regarding any audit requirements. LIBE's proposal to require a summary of measures in controllers' general reports may not yield meaningful information.

We support the Council's proposal to incentivise adherence to codes of conduct or certification schemes by providing that such participation is sufficient to demonstrate compliance.[74] However, these raise a general point of importance: compliance needs incentivisation, so legal consequences of adhering to codes etc need to be made explicit, as LIBE acknowledged (LIBE Draft explanatory statement 202). It is important to consider to what extent (if at all) controllers' liability should be reduced, or defences afforded to them, if they adhere to a code but still breach data protection laws, should this depend on the measure and/or rule concerned, and if so how. There is a more fundamental issue regarding accountability for breach of data protection law obligations, namely the strictness of the obligations and resulting liability. As a policy matter, it should be considered and made clear whether *any* failure to satisfy an obligation 100% would result in liability, ie effectively strict liability, for the benefit of data subjects,[75] or whether the approach be more nuanced and risk-based, so that if there is a breach but the controller has taken all appropriate measures designed to prevent the breach, then it should not be held liable. The many references in the Reform Proposal to 'ensure', 'steps to' etc, and proposals to delete or insert such wording, and proposals regarding certifications, codes and seals (covered below), highlight the essential issue that needs to be addressed, and the tensions between the three EU institutions in this regard. It may be timely to subject data protection law obligations to detailed individual scrutiny to decide which obligations should be 'strict liability' ones, and which should require only 'all reasonable measures appropriate to the risk' or the like.

We support proposals by LIBE and the Council to expand the factors to be taken into account in imposing administrative sanctions,[76] in particular compliance with certifications, codes of conduct and seals and 'the degree of technical and organisational measures',[77] including security measures under Art 30. However, we suggest further that consideration should be given to requiring these factors to be taken into account in relation to enforcement and remedies generally (Ch. VIII, eg Arts 77 on compensation and Council Draft Art 79b on other penalties), and not just administrative sanctions.

4.3 Processor obligations and joint controllers

4.3.1 The provisions

Commission Draft Art 26 would impose new detailed obligations (and liability) directly on processors. This would be a significant change. Currently, in most Member States, processors are only subject to legal obligations under their contracts with controllers. Processors would be accountable not only to regulators but also, under Art 75(2), to data subjects, who would be entitled to take legal proceedings in the country of the data subject's residence (not necessarily the processor's country). In the Council,

[71] Consequential drafting changes from this deletion should also be followed through eg in Art 4(13).

[72] And what is meant by 'implementation of policies', if those are not 'measures'.

[73] Ie, by adding reference to implementation costs, deleting 'of personal data processing', and clarifying in Art 22(1) that the demonstration required is of 'the adequacy and effectiveness' of required measures.

[74] Adding clarification that this means compliance with Art 22(1) rather than all data protection obligations, and adding reference to European Data Protection Seals if adopted (on seals, see 4.10.2).

[75] If so, the nature of the harm that may be claimed for needs clarification, eg non-financial harm?

[76] See 3.3.

[77] Which could also refer specifically to whether industry standards and best practices were followed.

several Member States have reservations regarding this provision.[78] They noted 'difficulties in distinguishing the roles of controllers and processors, in particular in the context of cloud computing, where the controller often can not exercise (full) control over the way in which the processor handles the data', and thought the provision did not reflect cloud computing realities. The Council would delete a requirement[79] that controllers 'shall ensure compliance' with the processor's technical and organisational measures. Coupled with the Council's proposed Art 26(1a) providing that 'sufficient guarantees' could be demonstrated by adherence[80] to codes of conduct or certification mechanisms, these again seem to reflect recognition that 100% guarantees cannot be ensured in practice, and a desire to incentivise context-appropriate compliance measures. LIBE would also insert an almost identical provision as Art 26(3a), showing general support for this approach. Similarly, LIBE would qualify certain provisions[81] with 'appropriate and relevant' and 'taking into account the nature of the processing and the information available to the processor'.

LIBE would also clarify expressly that 'The controller and the processor shall be free to determine respective roles and tasks with respect to the requirements of this Regulation'.[82] The Council would require the controller-processor contract to cover 'the subject-matter and duration of the contract, the nature and purpose of the processing, the type of personal data and categories of data subjects'. This echoes WP196 but does not suit self-service infrastructure cloud services, where the provider would not know the subject matter, nature or purpose of processing, etc, unless it inspected data or monitored processing, which the controller would positively *not* wish the provider to do; nor would the controller wish to give such information to the provider, let alone be required to do so in the contract.[83] Under Commission Draft Art 16(1)(a), the contract must provide that the processor may 'act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited' (ie transfers of personal data outside the EU).[84] LIBE would also clarify 'act only on instructions…' by changing that paragraph to, 'process personal data only on instructions from the controller, unless otherwise required by Union law or Member State law'. The Council would similarly change this[85] to, 'process the personal data only on instructions from the controller, unless required to do so by Union or Member State law *to which the processor is subject and in such a case, the processor shall notify the controller unless the law prohibits such notification'.* One Member State queried the 'instructions' requirement's feasibility in the context of social media.[86] However, how appropriate is this requirement more generally? In cloud computing, controllers 'rent' IT resources which they use on a self-service basis, so it makes little sense to say that they give 'instructions' to providers; providers do not actively process personal data in accordance with instructions from controllers.[87] The Reform Proposal would perpetuate the 'instructions' requirement, but arguably it should be abolished. From the DPD's history and the Swedish DPA's cloud decisions,[88] the legislative purpose of the instructions requirement seems clear: it was intended to prevent processors from using or disclosing personal data entrusted to them for purposes not authorised by the controller, eg for the provider's own purposes. Accordingly, the legislative objective of the 'instructions' provision may still be achieved, while making the provision more appropriate to cloud computing, by rephrasing the requirement to forbid use or disclosure (except with controller authorisation, eg regarding sub-providers, or when required by law) and to require notification to the controller of such disclosures, unless prohibited by law. 'Instructions from the

[78] With one suggesting its deletion. Council Draft fn 210-214.
[79] Mirroring the wording of Art 17 DPD. Two Member States felt 'sufficient guarantees' (again also wording from the DPD) was unclear and needed detailing.
[80] Presumably by processors, but this should be spelt out.
[81] Arts 26(2)(e) and (f).
[82] Although it seems implicit, it would be helpful to add 'in the contract'.
[83] WP196 12-13, and Hon, Walden and Millard (n 14).
[84] Discussed at 4.8 below.
[85] But with some additional wording at the end, shown in italics above.
[86] Council Draft fn 216.
[87] Hon, Walden and Millard (n 14).
[88] Datainspektionen, 'Tillsyn enligt personuppgiftslagen (1998:204) – Salems kommunstyrelseSalems' (28 September 2011) 263-201<http://www.datainspektionen.se/Documents/beslut/2011-09-30-salems-kommun.pdf> and 'Tillsyn enligt personuppgiftslagen (1998:204) – Uppföljning av beslut i ärende 263-2011' (31 May 2013) 1351-2012 <http://www.datainspektionen.se/documents/beslut/2013-05-31-salems-kommun.pdf> and 'Tillsyn enligt personuppgiftslagen (1998:204) – Behandling av personuppgifter i molnet' (9 September 2013) 890-2012 regarding Sollentuna <http://www.datainspektionen.se/press/nyheter/2013/skola-maste-sluta-anvanda-molntjanst/>, all accessed 25 February 2014.

controller' are also referred to elsewhere in the Commission Draft[89] but the same point applies regarding its inappropriateness in the context of self-service cloud use.

The contract must stipulate that the processor may 'enlist another processor only with the prior permission of the controller' (Art 26(1)(d)). While reflecting WP196,[90] with layered cloud services (eg SaaS built on IaaS or PaaS) 'prior permission' makes no sense; many cloud services will have already been constructed atop existing sub-providers' services. Cloud providers would need to obtain (and document) controllers' permission to pre-existing sub-providers in advance of the contract, which seems meaningless and would only increase bureaucracy. Providers are hardly likely to accept contract terms which require them to re-engineer their services should controllers take exception to an existing sub-provider, and therefore are likely to offer their services only on a 'take it or leave it' basis. Cloud providers with large-scale commoditised services are also unlikely to accept terms entitling controllers to determine which sub-providers they may switch to. The Council would change 'enlist another processor…' to 'determine the conditions for enlisting another processor only with the prior permission of the controller';[91] and LIBE would do the same, appending to that changed wording 'unless otherwise determined'. These changes would enable more context-relevant terms than requiring prior permission in all cases, but more clarity is needed on the meaning of 'determine the conditions for enlisting'.[92] Like the DPD, the Reform Proposal also seems to assume all sub-providers may access controllers' personal data. However, if controllers apply proper IT security measures to their data,[93] control over sub-providers becomes less important. Where the controller's use case requires data to remain unencrypted in the cloud, contractual restrictions on sub-providers may indeed be advisable. However, to require such restrictions in *all* situations involving sub-processors, rather than when appropriate to the situation, seems unnecessary and counter-productive. In particular, urgent clarification is needed specifically regarding the extent, if at all, to which data centre operators and suppliers of hardware, even software etc, used in data centres or as part of cloud services, would be considered 'another processor'. At worst, to avoid risks of direct liability as processors under the Reform Proposal, third country cloud providers may withdraw or refuse their services to EU controllers, thereby denying them the potential agility, flexibility and cost-saving benefits of cloud. Alternatively, controllers may not use cloud computing for fear of non-compliance, where providers refuse to agree to the contract terms required by the Reform Proposal due to conflicts with their technological or business models. Or, controllers may conclude that compliance is impossible, but decide to use cloud anyway, resulting in widespread non-compliance where practical enforcement may be impossible if it occurs on a large enough scale, undermining respect for laws.[94]

Other processor obligations, many of which will be covered below, would include record-keeping (ie maintaining certain documentation regarding the processing - Art 28), co-operation with DPAs including providing information, implementing security measures, data breach notification, and appointing data protection officers in certain circumstances. Processors may also be involved in data protection impact assessments and obtaining prior authorisation for certain processing, but the circumstances and scope are unclear.[95] Issues with processor obligations arise largely because it is problematic to treat as 'processors' cloud providers who merely rent out IT infrastructure,[96] particularly as such infrastructure providers may not know what kind of data their customers process – unless they inspect data or monitor usage, which controllers would not wish, as mentioned above. A related problem is that the Commission Draft assumes that, as with the 1970s outsourcing models on which the DPD was based, processors have *exclusive* access to the personal data they process, and that controllers cannot access data except through processors. This is not true in cloud computing: controllers retain direct self-service access to their data. Provisions to ensure controller access to fulfil

[89] Art 26(3) and Art 27.
[90] WP196 10.
[91] Although several Member States have issues or reservations here. Council Draft fn 217.
[92] Eg is it aimed at cloud providers who have built their services on pre-existing sub-providers' services? Is 'unless otherwise determined' intended to cover the situation where sub-providers' services are already in use and therefore 'otherwise determined'?
[93] Particularly backups and encryption for confidentiality and integrity – see 4.5.
[94] Chris Reed, *Making Laws for Cyberspace* (OUP 2012).
[95] See 4.7.
[96] Many SaaS providers knowingly process personal data, eg social networking services and advertising-funded webmail services, and should be liable as 'processors'. Our comments regarding infrastructure providers do not apply to them, but only to providers of IaaS, PaaS and pure 'passive' SaaS storage. See Hon, Walden and Millard (n 14).

data subject access obligations,[97] or requiring processors to 'assist' controllers with access requests, are inappropriate in cloud computing. Similarly, provisions requiring processors to 'assist' controllers to comply with obligations regarding security, data breach notifications, data protection impact assessments and duties of prior authorisation or consultation[98] are impracticable with large-scale use of shared infrastructure by multiple customers, where providers may be unaware of the nature or sensitivity of their users' data and where, for security, confidentiality, and logistical reasons, providers may decline to give each of a possible multiplicity of controllers detailed insight into the provider's internal arrangements, let alone agree to be bound contractually to do so.[99] Third party certifications or audits by independent experts, whose summary results may be shared with controllers, may make sense in such cloud situations, as WP196 has acknowledged.[100] Similar issues arise with cloud sub-providers. LIBE would helpfully qualify the 'assistance' obligation to require account to be taken of the nature of processing and information available to the processor, but the Council Draft would be better, simply requiring the contract to 'determine the extent' to which the processor must assist the controller. Applying any 'assistance' provisions only 'where appropriate' would be even better. The obligation to 'make available to the controller and the DPA all information necessary to control compliance with the obligations laid down in this Article'[101] seems tantamount to an audit right for controllers and their DPAs,[102] which is problematic in cloud computing. Obligations on cloud providers to provide information to or permit audits by individual controllers may be impractical and may even prejudice security, and consideration should be given to allowing reliance on audits or certifications by independent third party experts to industry standards – again spelling out what types may be relied on, the consequences if such audits or certifications are obtained, and the consequences (particularly regarding liability) if data protection laws are breached notwithstanding audits or certifications. Thus, we argue that, even if cloud providers should be considered 'processors', not all data protection law obligations should be imposed on processors.[103] It is important to consider carefully which obligations should or should not apply to processors, and which exemptions or relaxations should be available to or be considered in the legitimate interests of processors, eg scanning data for network security.

Many cloud providers are neutral intermediaries, and their position as such should be recognised. Therefore, if it is thought too radical to rule that cloud providers should not be treated as 'processors', our recommendation is to modernise Art 5(b) of the E-Commerce Directive,[104] which currently excludes data protection law matters from its scope, so that it includes such matters, or to introduce similar defences for processors in relation to data protection laws,[105] so that liability defences for mere intermediaries would also apply expressly to data protection law matters (including services *not* provided for remuneration, eg free storage services). This would make knowledge and control of personal data (including access to intelligible personal data) pre-requisites to cloud provider liability under data protection laws, but providers would lose this defence based on a modified form of 'notice and takedown'. We suggest a modified form is needed, based on a careful analysis of which obligations should apply to processors, as discussed above. This is because, where a provider is unaware of the nature of data processed using its service, it would be unfair if mere notification to it that its service was in fact being used to process personal data should, without more, bind it immediately to comply with ongoing processor obligations regarding security etc. Currently (and under the Reform Proposal), it would seem that even if a provider required its customers to warrant that no personal data would be processed using its service, it would still be liable as a processor if such data

[97] Contractual terms required on creating 'the necessary technical and organisational requirements' to fulfil the controller's data subject access obligations - Arts 26(2)(e), similar to WP196 requirements: 13, 16, 21.

[98] Art 26(2)(f). These controller obligations will be discussed in detail below.

[99] Also, it seems implicit, but it would be helpful to clarify, that the Art 26(2)(f) 'assistance' obligation (see previous note) should be limited to apply only to personal data that the processor processes on behalf of the controller, and not to any other personal data processed by the *controller* internally or through other processors.

[100] Hon, Millard and Walden (n 70), WP196 [4.2].

[101] Art 26(2)(h). Presumably 'the supervisory authority' should be 'its supervisory authority'.

[102] Which seems unnecessary: DPAs have powers to access premises under Art 53(2)(b). LIBE and the Council would change 'control compliance' to 'demonstrate' compliance. The Council would delete reference to the supervisory authority. LIBE would oblige the processor to 'allow on-site inspections'.

[103] Eg the Council would delete the requirement for *processors* to conduct Art 33(1) DPIAs, and similarly to consult with the DPA before processing in specific risky situations (Art 34(2)). On record keeping by processors and difficulties in cloud computing, see Council Draft fn 225.

[104] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1.

[105] Hon, Walden and Millard (n 14).

were in fact so processed, irrespective of the controller's breach of warranty and the provider's genuine belief that no personal data would be processed.

The points above (especially the inappropriateness of 'instructions' in cloud computing) are particularly important given that a processor who 'processes personal data other than as instructed by the controller' would be liable as a joint controller.[106] Joint controllership may be relevant to some cloud providers, who may be considered a joint controller through determining processing 'means'. Joint controllers would be required to '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' (Art 24). LIBE would add that the arrangement must duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, the 'essence of the arrangement' must be made available to data subjects, and in cases of uncertainty, the controllers must be jointly and severally liable. Similarly the Council would, regardless of arrangements between joint controllers, allow data subjects to exercise rights against any controller 'unless the data subject has been informed in a transparent manner which of the joint controllers is responsible' (Art 24(2)). However, several Member States have raised issues with this provision, with two thinking that it did not take sufficient account of cloud computing.[107]

Joint controllership should be considered together with provisions on compensation and liability (Art 77). Where an individual is damaged as a result of 'an unlawful processing operation or of an action incompatible with this Regulation' and more than one controller or processor is 'involved in the processing', each would be jointly and severally liable to compensate the individual for the entire amount of the damage (Art 77(1)). LIBE would extend this liability to non-monetary loss specifically, qualifying the joint and several liability by reference to 'an appropriate written agreement determining the responsibilities pursuant to Article 24',[108] and the Council would take a similar approach to recourse claims between joint controllers and/or processors.[109] The situation where one entity is 'more responsible' than another may be problematic;[110] eg, some Member States consider that controllers should remain (primarily, even) responsible and liable when using processors.[111] It may seem unfair if data subjects may claim the whole damage from an infrastructure cloud provider who may not have known that a controller (wrongfully) processed personal data using its infrastructure. From that perspective, again the recommendation made previously regarding E-Commerce Directive-type defences for data protection law breaches applies equally here. Indeed, the Art 77(1) phrase 'involved in the processing' seems too broad and may need careful redrafting – a cloud provider may be 'involved' if its infrastructure was used, yet not be responsible for actions taken by the controller using the infrastructure. A controller or processor 'may' be exempted from liability if it 'proves they are not responsible for the event giving rise to the damage',[112] but a more nuanced approach may be

[106] Art 26(4). The Council would delete this provision.

[107] Including its enforceability in the private sector outside a group, and insufficient clarity particularly for data subjects and regarding allocation of liability between controller and processor (and potential legal conflicts in that connection) - Council Draft fn 199. The Council Draft would also qualify this obligation to the extent Union or Member State law determined controllers' respective responsibilities. There were also issues regarding (prior) information to data subjects, clarity regarding the controller to which data subjects should have recourse, and which DPA should be involved – ibid fn 200.

[108] Also Rec 118.

[109] The Council Draft would change 'unlawful…' to 'non-compliant with this Regulation', and clarify that the liability must relate to 'the processing which gives rise to the damage' (although surely it would be more accurate to refer to the 'non-compliance which gives rise to the damage'). It would also provide expressly that the provision was without prejudice to recourse claims between controllers and/or processors (Art 77(2)), which one Member State felt should be left to national law. Council Draft fn 547.

[110] Ibid fn 546 and fn 547. Several Member States queried 'whether there was an EU concept of damage and compensation or whether this was left to Member State law', and there was uncertainty about what kind of damage would be covered, whether mere violation of the Regulation constituted damage or whether (as the Commission stated) the data subject must prove damage.

[111] Ibid fn 211, 214, 236, 543, 546.

[112] Rec 118, Art 77(3). Some Member States queried whether this provision should be mandatory, or expanded upon. Council Draft fn 548-549.

possible. For example, could it be provided that a factor to be taken into account should be the extent to which it was open to a controller or processor to cover itself by insurance?[113]

One Member State suggested restricting the possibility to seek compensation from processors to where the processor has processed personal data contrary to or in the absence of instructions from the controller. Subject to our point regarding the inappropriateness of referring to 'instructions', and possible expansion to cover eg breach of security measures, this may make sense in the cloud context.[114] Liability could be imposed in proportion to the individual actor's responsibility/fault, but there may be difficult issues of proof. The availability of insurance could be added as a factor. Careful consideration needs to be given to balancing the imposition of strict liability on controllers and processors jointly and severally for the benefit of data subjects, with the injustice of such imposition on an actor who is not at fault, bearing in mind that some controllers and processors may be SMEs.

4.3.2 Summary and recommendations

The processor provisions ill suit cloud computing, which means there is a real risk that cloud providers may refuse to allow their services to be used for personal data processing and/or that controllers may ignore the law in practice. These provisions need to cater for cloud infrastructure providers who may not know personal data are processed using their infrastructure, ideally by modernising the E-Commerce Directive to allow intermediary defences regarding personal data. They should also differentiate appropriately between situations where only processors have exclusive access to personal data (as with traditional outsourcing), and where controllers retain direct self-service access to data (as in cloud computing). Furthermore, they should differentiate between situations where providers can access intelligible personal data, and where they cannot, eg because of the use of encryption.[115] General wording could be added requiring account to be taken of the context, in particular whether the controller retains direct access to data and/or the provider can access intelligible personal data (eg in determining whether a provider is a 'processor'). The extent to which strict liability is effectively imposed, or only 'appropriate' or 'reasonable' measures are required, merits specific consideration. The 'instructions' provisions need to be modernised to apply more appropriately to cloud computing while preserving their legislative objective, namely preventing unauthorised use or disclosure, which presupposes access to intelligible personal data. Specifically addressing disclosure and use by processors would therefore seem more appropriate than 'instructions'. Provisions on use of sub-processors ('another processor') need further consideration, including clarification as to what extent if at all data centre operators and suppliers of hardware or software should be considered 'processors'. It is necessary to consider carefully exactly which obligations should apply to processors, and in which situations, taking into account the position of cloud infrastructure providers. It is clear that allocation of responsibilities and liabilities between controllers/processors and between joint controllers generally is a complex and multi-faceted matter requiring more debate and consideration. More work is needed to analyse and addresss uncertainties and possible problems, including different degrees of responsibility based on fault, the role of contractual allocations, the 'first port of call' for data subjects and involvement of national DPAs, the role of national law liability allocations, and the availability and possible role of insurance. It is very important to clarify which processing entity should be accountable to data subjects, national DPAs and/or other processing entities, in which circumstances, how, and for what. As with controller obligations, policymakers need to agree on exactly which processor obligations should be 'strict liability' and which ones 'best efforts' or 'all reasonable measures appropriate to the risk', and obligations should be clarified accordingly, and/or enforcement and remedies should take account of compliance with certifications and measures taken etc.

[113] Cf the Unfair Contract Terms Act 1977 (UK) sections 11(4)(b) and 24, which specifically provides that, when assessing reasonableness in relation to contractual terms or notices limiting a party's liability, regard must be had in particular to how far it was open to that party to cover itself by insurance.

[114] Ibid fn 539-544.

[115] In the latter situation it may be inappropriate to treat them as 'processors'.

4.4 Jurisdictional applicability of data protection law

4.4.1 Provisions

Art 4(1) DPD requires Member States to apply EU data protection laws to any controller who has an 'establishment' in the EU and processes personal data 'in the context' of that establishment's activities, or who does not have such an establishment but 'makes use of equipment' in the EU. Commission Draft Art 3(2) would continue the former[116] but delete the latter, instead covering those who process personal data of EU residents in relation to '(a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour'.

The Reform Proposal would perpetuate several jurisdictional legal uncertainties that currently affect cloud computing, regarding the meaning of 'establishment' and 'context' of the establishment's activities.[117] If a third country controller (directly or indirectly) uses an EU data centre, EU cloud provider or EU sub-provider to process personal data using cloud computing, it is unclear whether the controller would thereby become subject to EU data protection laws through the EU data centre, cloud provider or sub-provider being treated as its EU 'establishment' - even if the data processed are unrelated to EU residents. Similarly, if such controller has an EU subsidiary, it is unclear whether the third country controller itself (and not just its subsidiary) would be directly subject to EU laws through that subsidiary being considered its EU 'establishment'. The position is exacerbated because 'context of' activities often seems to be ignored, so that having *any* EU 'establishment' may subject a third country controller to EU data protection laws even if the establishment's activites are unrelated to the controller's personal data processing. The Commission Draft would also perpetuate a loophole in the DPD whereby the equipment ground (and new offering ground under Art 3(2)) omits reference to context of activities.[118]

Commission Draft Rec 27 states that 'the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment'. However, an EU data centre used by a third country controller may still be considered its 'main establishment' in the EU because Commission Draft Art 4(13) defines 'main establishment' for a controller such that (emphasis added) '…if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is *the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place'.* Such a place would seem to include data centres. If 'context' continues to be interpreted broadly, EU data protection laws could be applied to all third country controllers who process personal data using EU data centres, eg for backup purposes, and who have 'an establishment' in the EU, such as an EU subsidiary, even if the EU subsidiary's activities are unrelated to the processing. The Council Draft would retain the problematic sentence italicised above. We recommend that, to enhance legal certainty in cloud computing and avoid deterring third country controllers from using EU data centres or EU cloud providers or sub-providers,[119] or indeed from setting up EU 'establishments', the Reform Proposal should state explicitly[120] that use by a third country controller of an EU data centre or EU-established cloud provider or sub-provider would *not* in itself result in the controller being treated as 'established' in the EU *through* the data centre, provider or sub-provider.[121] This seems particularly important given the potential fluidity of cloud data:[122] a third country cloud user could be subject to EU data protection laws if its data are backed up to an EU data centre, but cease to be so subject if they are backed up instead to a third country data centre, or vice versa. References to 'context of activities' should be deleted, or else added to Art 3(2) (and (3)) and the phrase's meaning and scope explained. Similarly, it should be clarified expressly that having EU-

[116] LIBE would, helpfully, clarify this to apply whether or not the processing itself takes place in the EU.
[117] W Kuan Hon, Julia Hörnle and Christopher Millard, 'Which Law(s) Apply to Personal Data in Clouds?' Ch 9 in Millard (ed) (n 12).
[118] So that a controller who *is* 'established' in the EEA, but is not processing personal data *in the context of that establishment's activities*, may escape the application of EU data protection laws altogether. Ibid.
[119] Which may also conflict with the EU's strategy of encouraging, not just cloud computing use, but also the development of cloud computing infrastructure (eg data centres) in the EU. Commission, 'Unleashing the Potential of Cloud Computing in Europe' COM (2012) 529 final.
[120] As France has done in relation to use of French providers – see Hon, Hörnle and Millard (n 117) fn 90.
[121] Hon, Hörnle and Millard (n 117).
[122] Digital data may be moved 'out' of EEA data centres through high bandwidth links (or, more accurately, perhaps, copies deleted from such data centres) far more easily and quickly than data in paper form.

incorporated subsidiaries would not in itself subject third country controllers (as opposed to the EU subsidiaries) to EU data protection laws,[123] but if that is truly intended as a policy matter, it should be made explicit, and the consequences considered carefully first - eg may it deter third country organisations from establishing subsidiaries in the EU?[124]

The Commission Draft would extend EU data protection laws to *processors* with an 'establishment' in the EU, whose 'main establishment' would be taken to be 'the place of its central administration in the Union' (Rec 27, Art 4(13)) – even where their processing activities involve the personal data of non-EU residents, and/or personal data are processed for non-EU controllers. LIBE would further extend this to personal data processing by such processors that takes place *outside* the EU, but change the place of central administration to the establishment where main decisions on purposes etc are taken, consistently with the criteria for controllers. The Council would provide that, if the processor has no central administration in the EU, its main establishment would be 'the place where the main processing activities in the context of the activities of an establishment of the processor take place'.[125] As with controllers, this change seems to encompass data centres, which could deter third country cloud providers from setting up EU 'establishments' or using EU data centres. Clarification is needed as to whether a non-EU processor which only uses a data centre in the EU or uses an EU sub-provider would be caught by the Commission Draft.[126]

We welcome the proposed change from use of 'equipment' to offering or monitoring, which seems more focused and in keeping with modern realities.[127] However, we suggest referring to 'directing' or targeting rather than 'offering'. The former concept is better known and its meaning is clearer because various EU cases have explained the concept.[128] 'Directing' seems sufficient to address the underlying concerns without being over-broad. However, the provision may result in third country controllers refusing to provide services to EU data subjects, although query whether in practice the Reform Proposal may be enforceable against non-EU controllers without any 'establishment' in the EU.[129] LIBE would extend the 'offering' provision to *processors* not established in the EU. That seems a step too far. Coupled with the introduction of direct processor obligations and liabilities, it could result in third country cloud providers and other processors refusing to supply services to cloud users (in any country) who wish to offer goods or services into the EU, although again practical enforceability may be questionable. This approach may reflect a policy decision to apply EU data protection laws to third country providers that are used by EU controllers to process personal data. If so, that should be considered carefully and stated explicitly, rather than through extending the 'offering' provision to processors, as again it could discourage non-EU processors from setting up EU 'establishments' eg data centres. Also, logically it would seem that the EU controllers would be accountable in those cases in any event.

We do not discuss the one-stop shop proposal, which has proved fraught with difficulty, is still under discussion in the Council, and is not very relevant to cloud computing.[130] There is a final issue which requires mention, namely applicable law. Currently there are uncertainties as to which national law applies where establishments in multiple Member States are involved.[131] Even with a Regulation, there is scope for national laws to differ in various areas. Accordingly, the Reform Proposal needs to

[123] Hon, Hörnle and Millard (n 117), 240. Rec 19, which partly duplicates DPD Rec 19 on the legal form of such arrangements, does not assist and indeed suggests the opposite.
[124] But see Council Draft fn 416 for a contrary view.
[125] Although, unlike Art 4(13), Council Draft Rec 27 omits reference to context of activities. Conversely, Council Draft Rec 27 mentions (emphasis added) 'take place *in the Union*', but Art 4(13) does not stipulate that 'an establishment' must be in the Union – seemingly an inadvertent omission, as otherwise a third country establishment could be considered the 'main establishment' of the processor.
[126] See 4.3.
[127] As does the EDPS: 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) [100] <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf>.
[128] Hon, Hörnle and Millard (n 117).
[129] As with the approach to cookies and 'equipment use' currently. Hon, Hörnle and Millard (n 117).
[130] However, we do support the principles of one-stop shop and co-operation/consistency.
[131] Hon, Hörnle and Millard (n 117).

address, not just which Member State's DPA is competent to deal with a particular issue, but also which Member State's national law should apply to that issue.[132]

4.4.2 Summary and recommendations

There are many legal uncertainties regarding the territorial extent of accountability for EU data protection laws, particularly in cloud computing. The meanings of 'establishment' and 'established' need clarification. We recommend explicitly providing that a third country controller or processor would not be considered to have a 'main establishment' merely through owning or using an EU data centre, using a provider or sub-provider incorporated (or using a data centre) in the EU, or through having an EU subsidiary. The concept of 'context of activities' should be deleted, or (ideally) referred to in Arts 3(2) and (3) and its meaning and scope explained. We recommend 'offering' should be changed to targeting or directing. We suggest it would go too far if third country processors (particularly cloud providers), whose services are used by a controller that 'offers' goods or services to EU data subjects, were to be liable as 'processors', including for the controller's defaults; the consequences need careful consideration. More generally, while EU data protection laws may deliberately be applied extraterritorially for policy reasons, thought must be given to defining clearly the scope of such application, for comity and enforceablity reasons, if they are to have a chance of being respected.[133] In particular, the position of third country controllers or processors with no EU 'establishments' or 'main establishments' needs re-consideration. Finally, the issue of which national law is applicable in exactly which situations, not just which national DPA is competent, needs clarification.

4.5 Security requirements

4.5.1 Provisions

The Commission Draft would require both controllers and (a new obligation) processors to 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[134] and the costs of their implementation' (Art 30(1)) - paraphrasing the current DPD requirement. Several Member States considered that the controller, not processor, should have primary responsibility for security measures.[135] Infrastructure cloud providers may not know whether data stored on their service by customers are 'personal data' or sensitive personal data, so we reiterate previous recommendations regarding defences or exemptions for such providers.

A prior risk evaluation would be required.[136] The Council would delete this, but LIBE would stipulate a minimum list, including measures to 'protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure',[137] to ensure personal data 'can be accessed only by authorised personnel for legally authorised purposes',[138] and to ensure 'the implementation of a security policy with respect to the processing of personal data'.[139] LIBE would require the security policy to include certain specific

[132] Two Member States also considered that a main question is 'whether the allocation of competence to the supervisory authority of the main establishment was exclusive and whether it also implied a rule of applicable law'. Council Draft fn 415.

[133] Reed (n 94).

[134] The Council would change 'state of the art' to 'available technology' and require regard to be had to the 'nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects'. It would also mention using pseudonymous data as a possible measure – see 4.1.

[135] Council Draft fn 236.

[136] Aimed at protecting 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' - Art 30(2). This paraphrases DPD Art 17(1) on security, adding the risk evaluation requirement and references to 'dissemination' and 'alteration', but deleting reference to transmission over a network.

[137] Art 30(2)(b). It is unclear why this refers only to data 'stored or transmitted' (cf the broader 'processed'). Mentioning 'storage... access or disclosure' seems superfluous as the Art 4(3) 'processing' definition includes 'storage' and 'disclosure by transmission' (although not 'access').

[138] Ie implementing appropriate access controls (which could be specifically mentioned).

[139] Art 30(2)(a) and (c) respectively.

matters (Art 30(1a)), but these would benefit from clarification[140] and analysis of their practicability.[141] We welcome LIBE's Art 30(1a)(b) explication of 'security' in terms of the cornerstone IT objectives of confidentiality, integrity and availability, but suggest that it should refer to confidentiality, integrity and availability of data and processing as well as systems and services (eg securing data in transmission also, by securing communication channels), and that these objectives should be required in relation to implementation of measures, not just security policies. We strongly recommend adding specific wording eg 'such as by appropriately strong encryption (including secure key management), and ensuring data are backed up appropriately', to help raise awareness among controllers of the importance for data security of backups and encryption in particular.[142] Art 30(1a)'s preamble regarding security policy requirements requires regard to be had to the state of the art and cost of implementation, but other factors could be specified, eg nature of the data.[143] LIBE would also require a process for regularly testing and evaluating security policies, procedures and plans to ensure ongoing effectiveness.[144] We also suggest providing that processing to monitor or check compliance (whether of a controller or its processor) with data protection laws, eg where a controller checks logs of accesses to its data, including by a cloud provider's employees, or to test effectiveness of security measures, should be considered to be in the legitimate interests of the controller or processor as the case may be.

The Council would allow the controller and processor to demonstrate compliance by means of adherence to codes of conduct or a certification mechanism (Art 30(2a)). This should help incentivise adherence to such codes or certifications (or European Data Protection Seals[145]). It would assist providers of shared cloud infrastructure services,[146] and also potential cloud users who may not have expertise to assess cloud providers' security. However, it costs providers money to implement codes or obtain regular certifications from independent experts; therefore, to encourage their use, the detailed consequences of adherence to codes or certifications, particularly regarding liability, need to be made explicit. Would adherence to codes etc demonstrate compliance with Arts 22(2)(b) and 26(2)(c),[147] but only those requirements? If a code-adhering controller suffers a security breach, should it be liable for compensation,[148] eg where it was in breach of the certification's conditions (or even if it was not)? These factors need to be taken into account not only in relation to administrative sanctions, but liability and remedies more generally.[149]

The Commission Draft's Art 27 on confidentiality is almost identical to DPD Art 16,[150] but headed 'Processing under the authority of the controller and processor' instead of 'Confidentiality', and with additional wording to make clear that, eg, disclosure of personal data to US authorities is restricted even if *US* law requires it; only EU law would be relevant here. As discussed above, the provision should not refer to 'instructions' but to *use or disclosure*. Similarly, it should refer to access to 'intelligible personal data', as confidentiality should not be at risk if only unintelligible data may be accessed, such as encrypted data. Also, should the requirement be for 'appropriate steps', for a risk-based approach? Indeed, is this provision needed at all, given that explicit general obligations on confidentiality, integrity and availability would be imposed by LIBE?[151] Another issue affecting confidentiality is, to what extent may a processor access (and therefore potentially disclose or misuse) intelligible personal data after the processing arrangement terminates? Commission Draft Art 26(2)(g) would require a contract term obliging the processor to 'hand over all results to the controller after the

[140] Eg the meaning of 'resilience', which does not have as well accepted a meaning as confidentiality, integrity and availability, and 'situational awareness'.

[141] Eg 'near real time'; and 'Solutions that provide more resiliency seem to be economically impractical.' Matt Bishop and others, 'Resilience is More than Availability', in *Proceedings of the 2011 workshop on New security paradigms workshop*, NSPW 2011 (ACM 2011) <http://www.nspw.org/papers/2011/nspw2011-bishop.pdf>.

[142] Other types of measures may of course also be important for security, such as access control, authentication, intrusion prevention and detection, and logging of accesses etc.

[143] It is unclear whether the requirements listed are minimum requirements, or may be adapted in light of the state of the art, etc. It could also be stated explicitly that the *formulation* of any security policies should also take account of the stated factors in aiming to achieve the stated objectives.

[144] Art 30(1a)(e). We suggest adding, 'as appropriate to the risks'.

[145] See 4.10.2.

[146] Hon, Millard and Walden (n 70).

[147] See p 27.

[148] Art 77 - see 4.3.

[149] See 3.3.

[150] See also paragraph containing n 89.

[151] See 4.5.

end of the processing and not process the personal data otherwise'. This reflects traditional outsourcing and paper files. However, as discussed in 4.1, digital data are copied, rather than 'handed over' or 'returned'. In cloud computing, ensuring the controller 'gets back' its data is achievable not only through contractual obligations but also through direct retrieval, if the controller has enough time to do so;[152] and can also be assured through the controller continually taking backups internally or to another provider during the currency of the contract. Ensuring that the processor cannot use or disclose data after the user terminates its use of the service may be achieved by obliging the processor to delete its copies (and/or restricting such use or disclosure through contract terms that survive termination); the questions are, deletion to what degree or standard,[153] and what proof of deletion should or can be required? LIBE would amend this provision to 'return all results to the controller after the end of the processing, not process the personal data otherwise and delete existing copies unless Union or Member State law requires storage of the data'. The Council proposes similar wording, with an exception for legal data retention requirements binding the processor under Union or Member State law. The LIBE Draft, in referring to deletion (which however needs defining as already discussed), better reflects the realities of digital data than the Commission's 'hand over' provisions.

Given the key role encryption can play in securing data confidentiality, it seems important as a policy matter to incentivise controllers and processors to encrypt personal data in the cloud and elsewhere. The drafts address this in slightly different ways. The data breach notification provisions[154] should encourage controllers to encrypt personal data, but their formulation refers to unintelligibility as an absolute property, making no reference to encryption strength or key management (eg according to industry standards or best practices): yet both are critical to how intelligible (or not) encrypted data may be in practice, so it would be helpful to add reference to the degree of unintelligibility being appropriate to the risks in the circumstances. While not defining encrypted data, the Council Draft would add reference to encryption or use of pseudonymous data, as examples of appropriate technological protection measures absolving controllers from data breach notification obligations.[155]

4.5.2 Summary and recommendations

We recommend combining the contextual risk-based approach emphasised by the Council (and to some extent LIBE) with LIBE's helpful specific reference to requirements to maintain confidentiality, integrity and availability, but focusing more on those objectives than on processes, and with some drafting clarifications and other modifications, eg reference to confidentiality, security and availability of data and processing, not just systems and services, and in relation to implementation not just policy. We recommend that while confidentiality, integrity and availability should be mentioned as objectives in technologically-neutral terms, express reference in the Reform Proposal to encryption and backups as examples of security measures to protect confidentiality (for the former), and integrity and availability (for the latter) would help to raise awareness regarding these measures. Requirements regarding resilience, if retained, should be defined clearly, but again in general terms. The definition of 'personal data breach'[156] should be made consistent with any changes. Consideration needs to be given to the extent to which formal security policies as well as measures should be required, and whether there should be strict liability for 'ensuring' security, or alternatively requirements only to 'take all reasonable measures appropriate to the risk to ensure…'. Processing to protect security and check or monitor compliance with data protection laws generally should be stated to be in the legitimate interests of the controller or processor. The Council would allow compliance to be demonstrated by adherence to codes of conduct or certifications, which is a realistic approach with multi-tenant, shared infrastructure cloud computing. However, liability consequences should be spelled out if, despite such adherence or certification, a security breach occurs. Thought should be given to what must be ensured, who must ensure it, and who should be legally liable, and to what extent, if it is not ensured (eg, controllers primarily). As mentioned previously, allocating liability based on fault and consideration of the availability of insurance may be merited. Regarding various references to deletion, 'erasure' and

[152] So ideally controllers should seek a contractual post-termination grace period for data retrieval, and some have succeeded in doing so. Hon, Millard and Walden (n 70), 98.

[153] See paragraph containing n 49.

[154] Art 32(3), see 4.9 below. LIBE would introduce a definition of 'encrypted data' in Article 4(2b) but the phrase is used not in relation to data breach notification, but only in relation to information to be given to data subjects under Art 13a(f), which however refers to data in 'encrypted form' rather than 'encrypted data'

[155] Art 32(3)(a). See also Rec 68a, which does not seem to add anything further.

[156] Discussed in 4.9.1.

‘restricting’ processing, it would be helpful to clarify the nature and standard of deletion, eg requiring deletion of personal data to the standard ‘appropriate to the risks of the individual situation’, but bearing in mind that infrastructure cloud providers may not be aware of the nature of the data.

4.6 Data protection by design and by default

4.6.1 Provisions

The provisions regulating data protection by design and by default have triggered intensive debate regarding both their exact meaning as well as their practical implications. Commission Draft Art 23(1) introduces firstly an obligation for controllers to implement appropriate technical and organisational measures and procedures from the design phase of the deployment of applications and systems in order to ensure compliance with the data protection requirements foreseen in the Regulation and to safeguard the rights of the data subjects, although the word ‘design’ is not used in the provisions setting out the substantive requirements. This obligation should be read in conjunction with the security obligations of data controllers, above, as it requires the actual implementation of security measures described in Art 30. The Council would require the measures to be appropriate not only to the processing activity but also to the objectives of that activity, specifically including the use of pseudonymous data. LIBE would qualify that measures should also be ‘proportionate’ and, taking an expansive view of data protection by design, require regard to be had to the entire lifecycle management of personal data from collection to processing to deletion, focusing in particular on ‘comprehensive procedural safeguards’ that ensure respect for the data protection principles and safeguard the security of data (eg confidentiality, integrity, physical security and ‘deletion’). In this way LIBE would clearly link data protection by design with the implementation of security measures. It is insufficiently clear what data protection by design would require. Clarification or guidance along the lines of the A29WP’s specific suggestions regarding data protection by design would be helpful, eg in relation to data minimisation, controllability, transparency, user friendly systems, data confidentiality, data quality and use limitation,[157] as long as the characteristics of cloud computing are taken into account. For example, the A29WP has suggested that, wherever it is appropriate, ‘functionality should be included facilitating the data subjects' right to revoke consent, with subsequent data deletion in all servers involved (including proxies and mirroring)’[158]. This may be impracticable in cloud computing, as discussed already.

LIBE would also extend the obligation to implement data protection by design to processors. The extension of data protection by design to processors has been an issue of debate in the Council. It is interesting to note that the Council provides for administrative fines that may be imposed on controllers or *processors* in relation to non-implementation or poor implementation of Art 23 DPIA or Art 30 security measures (Art 79(2a)(e) Council Draft). While seeming to concur with the Commission Draft’s application of privacy by design only to controllers,[159] the Council nevertheless inserted reference to processors in Art 79(2a)(e). There is a clear need for alignment between the two provisions. In cloud computing, it may be difficult if not impossible for processors to comply with this obligation as they do not know the type of data processed using their infrastructure or the sensitivity of such data, and public cloud services are by nature standardised and commoditised and generally cannot be heavily customised to suit the individual requirements of a multiplicity of possible users.[160] In fact, for most public cloud services the controller will not be able to influence the design of the underlying base hardware and software infrastructure, making it practically impossible to implement in full the data protection by design principle. Similarly, providers who use sub-providers are unlikely to have control over their sub-providers’ infrastructure. The EDPS has also made this point, stating: ‘[i]n the case of a basic IaaS service, it seems particularly difficult for a business customer (especially if an SME) to influence the technical and organisational structure of the service. It is not realistic to expect … a large provider with many customers to tailor its technical infrastructure or organisation to meet the specific compliance requirements of each customer on the basis of individually negotiated

[157] A29WP and Working Party on Police and Justice, ‘The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data’ (2009) WP168 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf>.
[158] WP168, para. 52.
[159] This choice has been questioned by two Member States – Council Draft fn 195.
[160] Hon and Millard (n 47), 32.

contracts'[161]. However, controllers who use IaaS would generally have more control than with PaaS or SaaS, eg to install firewalls and patch the operating systems and applications that they choose to install in their virtual machines, etc, while PaaS users control their application code.[162] LIBE also linked data protection by design to DPIAs, requiring controllers (and processors) to take into account the results of any DPIAs when implementing data protection by design. A challenging issue is exactly how the data protection by design requirements may be translated into practical measures, which the Commission would tackle through laying down technical standards (Art 23(4)). However, if standards laid down by the Commission are too detailed or specific, they risk undermining the objective of technology neutrality.[163] This challenge was probably identified by LIBE and the Council, as both deleted the Commission's empowerments regarding data protection by design, including those relating to technical standards.

The Commission would introduce in Art 23(2) data protection by default as an obligation for controllers, ie the obligation to implement by default mechanisms to ensure that only those personal data are processed which are necessary for each specific purpose of the processing and that they are 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 (ie to comply with the purpose limitation principle, and data and storage minimisation). The Council would change this to 'appropriate measures' for processing personal data that are 'not excessive'. While Commission Draft Art 23(2) required controllers by default not to allow accessibility of personal data to an indefinite number of individuals, implying some kind of access control, the Council would limit this to cases where the processing purpose was not to provide public information and no human intervention was involved in making personal data thus accessible. LIBE would require controllers to 'ensure', not only implement mechanisms for ensuring, data minimisation, and further require mechanisms to ensure data subjects can control the distribution of their personal data. This obligation would not be imposed on processors. For controllers using cloud computing to process personal data, presumably measures to limit public accessibility of data would include imposing contractual access control requirements on providers, but it is unclear how they could offer mechanisms for data subjects to 'control the distribution' of their personal data, eg must data subjects be given the technical ability *directly* to delete or restrict their data or indeed to disseminate it to others as the data subject wishes, or is it sufficient if they can require the controller to do so?

The Commission Draft would introduce an accountability obligation for controllers not only to ensure but also demonstrate compliance with data protection by design and by default via adoption of internal data protection policies and implementation of appropriate measures (Rec 61). As it is unclear what data protection by design and default, in particular, would require, an obligation to demonstrate compliance with these principles could create further confusion rather than increase accountability in cloud computing (and other) contexts. The Council would allow compliance to be demonstrated through adherence to codes of conduct or certification mechanisms under Arts 38 and 39 (Art 23(2a)), discussed below.

Non-compliance with the principles of data protection by design and by default may trigger severe fines. Art 79 of the Commission Draft provides for administrative fines for controllers who do not comply. The LIBE Draft would provide for even higher fines, while the Council would impose fines both on controllers and processors for not taking technical and organisational measures implementing data protection by design and by default, based on their 'degree of responsibility' (Art 79(2a)(e)).

4.6.2 Summary and recommendations

We recommend that the Reform Proposal clarifies the concept of data protection by design, possibly including express reference to security obligations (see 4.5.2) and guidance similar to that suggested

[161] EDPS, 'Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"' (2012) <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf>.

[162] Hon and Millard (n 47).

[163] Bert-Jaap Koops and Ronald Leenes, 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data protection law' (2013) International Review of Law, Computers & Technology 3; Bert-Jaap Koops, 'Should ICT-regulation be technology-neutral?' in E J Koops and others (eds), *Starting points in ICT regulation. Deconstructing prevalent policy one-liners* (TMC Asser Press 2006) 77ff.

by the A29WP.[164] The extension of data protection by design to processors would impose significant burdens on them. Especially in cloud computing environments, controllers and even processors may not have much or any influence over the design of a system and may not be able to implement the privacy by design principle in full; they can only work within the limitations of the systems available to them, although generally controllers using IaaS or PaaS have more control than SaaS users. Due to differing degrees of control in cloud computing, and indeed other areas, we suggest that Art 23's requirements be limited to aspects within the control of the controller or processor concerned.[165] These issues again illustrate the difficulties with treating infrastructure providers as active 'processors'. We support Council Draft Art 23(2a) and recommend its expansion to cover relevant codes of conduct and seals as well as certification mechanisms.

4.7 DPIAs

4.7.1 Provisions

The Commission Draft would introduce an obligation on controllers and or processors to carry out a DPIA when the 'processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes', which the Council Draft would limit to controllers (Art 33(1)). The Commission and Council Drafts provide some examples of processing operations that present specific risks (eg processing of sensitive data or processing of personal data in large scale filing systems on children, genetic data or biometric data etc). Commission Draft Rec 74 refers to 'the use of specific new technologies' as potentially involving a high degree of specific risks for the rights and freedoms of individuals. This seems to reflect a defensive stance towards new technologies, which are not necessarily intrinsically privacy-invasive. New technologies may be no more of a threat to privacy than old ones; indeed, they may be more protective of individuals' rights and freedoms, as for example with privacy enhancing technologies. Much depends on the purpose for which a technology is used. Therefore, we suggest either deleting the reference to new technologies or referring specifically to the purpose and manner of their use. The EDPS criticised the lack of specific guidelines on how to conduct DPIAs,[166] recommending that the Commission develop templates that could be used to evaluate and manage risks in cloud computing.[167] However, cloud risk assessment guidelines already exist, notably those promulgated by ENISA.[168]

LIBE would introduce a new obligation for controllers, and where applicable processors, to carry out a risk analysis of the potential impact that the intended data processing operation may have on the rights and freedoms of data subjects in order to assess whether they are likely to present specific risks (Art 32a). This obligation, which seems to be in addition to the Art 32 DPIA obligation, would oblige all controllers (and, 'where applicable', processors) to carry out a risk analysis in order to identify the potential impact of the intended processing on data subjects' rights and freedoms, notably whether it is likely to present 'specific risks'. LIBE Draft Art 32a(2) lists processing operations that are likely to present specific risks, broader than the Commission Draft's Art 33(2) list of 'specific risks', covering for instance processing of personal data of more than 5,000 data subjects for 12 months consecutively, where presumably a personal data breach would have greater adverse impact. Under LIBE's Art 33(3)(c), when any of the specific risks listed in Art 32a(2)(a)-(h) is identified (it is unclear why Art 32a(2)(i) is omitted), the controller or processor must carry out a DPIA. Thus LIBE introduces in specific situations an obligation for controllers or processors to carry out both a risk analysis and a DPIA. If carried out in an informal and not burdensome way, a risk analysis should be useful in order to assess the potential impact of the intended data processing on the rights and freedoms of the data subjects. The added value of carrying out both a risk analysis and a DPIA in all the cases mentioned in Art 32a(2) is questionable and could result in onerous obligations for controllers and processors. In cloud environments, not all data processing operations may entail risks for the privacy of the data subjects (eg, the controller may encrypt personal data before upload to the cloud) and DPIAs should

[164] See para containing n 157.

[165] This may include choosing a provider with adequate security measures, but that is already covered by Art 26 (see 4.3).

[166] EDPS (n 161), [64].

[167] Ibid [66].

[168] Daniele Catteddu and Giles Hogben (eds), 'Cloud Computing – Benefits, risks and recommendations for information security' (*ENISA*, 2009) <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment> accessed 25 February 2014.

be limited to the situations that would actually raise specific risks for data subjects. For example the need for a DPIA when the data processing operation relates to more than 5000 data subjects (Art 32a(2)(a), which is a relatively small number, could create a heavy burden for startups that use cloud computing for their initial technology infrastructure. Moreover, the wording of Art 32a(2)(h) requiring a DPIA when the core activities of the controller or processor require regular and systematic monitoring of data subjects is very vague. Also, arguably *all* breaches would 'likely adversely' affect the privacy or legitimate interests of data subjects (Art 32a(2)(g). Therefore we suggest that Art 32a(3)(c) should be amended to limit or clarify the need for a DPIA in the situations mentioned above.

Regarding the minimum information that a DPIA should cover, the Commission and the Council Drafts require 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 protection of personal data and demonstrate compliance with the Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned (Art 33(3)). It remains unclear who the 'other persons concerned' would be, as they are clearly not the data subjects. The LIBE Draft would extend this to include, among other things, a general description of the time limits for erasure of the different categories of data, an explanation of the data protection by design and by default practices adopted, a list of intended transfers to a third country, an assessment of the context of processing (whose meaning is unclear), etc.

4.7.2 Summary and recommendations

The carrying out of a risk analysis in order to determine data processing operations that are likely to present specific risks to data subjects was already foreseen in Art 20 DPD's 'prior checking' requirement, considered the precursor to the DPIA obligation. The proposals on DPIAs need to take into account the particular characteristics of cloud computing. Cloud computing should not be considered as a technology that would *per se* entail risks to data subjects due to its great computation and storage potential. The nature, the scope, and the purposes of data processing operations should be taken into account in all cases, as well as measures that controllers and processors may take such as encryption. The Commission Draft would introduce DPIAs, while the LIBE Draft would add an obligation for controllers and processors to carry out a risk analysis. In cloud environments, DPIAs should be limited to the situations that are likely to pose specific risks to data subjects. Therefore we suggest that Art 32a(3)(c) is modified to limit or clarify the need for a DPIA in the situations highlighted above. In addition the reference to the use of specific new technologies as potentially involving a high degree of specific risks for the rights and freedoms of individuals should be removed from Rec 74 or at least amended to refer to the purpose for which and manner in which new technologies are to be used (and not their use as such).

4.8 International data transfers

4.8.1 Provisions

The DPD allows 'transfers' of 'personal data' to third countries only if there is 'adequate protection' for the data (essentially based on the receiving country's data protection laws), or 'adequate safeguards', or if a derogation applies such as the data subject's unambiguous consent. Adequate protection is deemed by certain Commission decisions, eg transfers under the US Safe Harbor scheme, and adequate safeguards may be provided through use of Commission-approved standard contractual terms often known as **model clauses**, or through DPAs authorising adoption by a group of companies of a set of rules called binding corporate rules ('**BCRs**') to allow transfers within the group.[169] Most of these procedures involve DPA approvals, often required *ex ante* ie before the transfer.

Although purportedly expanding the permitted transfer methods, the Commission Draft would restrict transfers further, which could significantly affect cloud computing. Numerous Member States

[169] W Kuan Hon and Christopher Millard, 'Data Export in Cloud Computing – How can Personal Data be Transferred outside the EEA? – the Cloud of Unknowing, part 4', updated version 'How Do Restrictions on International Data Transfers Work in Clouds?', Ch 10 in Millard (ed) (n 12).

expressed reservations here, and these provisions are still under active discussion.[170] Unfortunately, the proposed definition of 'transfers'[171] in LIBE rapporteur Albrecht's January 2013 draft report[172] did not appear in the LIBE Draft. Illustrating the uncertainties with this term, one Member State asked the Commission to clarify whether a data transfer in the cloud computing context constitutes an international transfer of data.[173] Several Member States have suggested defining 'transfer' expressly.[174] We recommend that 'transfer' be defined by reference to intention to give or allow logical access to intelligible personal data to a third party recipient[175] who is subject to the jurisdiction of a third country, rather than simply 'to a third country'. If the recipient cannot access intelligible data, due eg to encryption applied by the controller, no 'transfer' should be considered to have occurred. The concept of 'mere transit' also needs clarification.

Regulators like the UK Information Commissioner allow controllers to make their own adequacy assessment, eg that adequate protection may be achieved by strongly encrypting personal data stored on a laptop (with secure key management) before taking it outside the EU. However, as well as requiring that information be provided to data subjects about potential data locations, Commission Draft Art 34 would require prior DPA authorisation of all personal data exports, *unless* one of certain conditions (under Arts 40-43) was met for the transfer, or an Art 44 derogation applied.[176] Two Member States queried this apparent shift from the DPD, 'which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data'.[177] Indeed, seven Member States queried the feasibility of maintaining an adequacy test with reference to the massive flows of personal data in the cloud computing context.[178] Furthermore, Commission Draft Art 42 would allow transfers under 'appropriate safeguards' only where 'adduced' in a 'legally binding instrument'. This means *technological* safeguards, eg encryption, would no longer be recognised as a means to protect personal data destined for storage or other processing outside the EU. This is a step backwards, given the importance of technological measures such as encryption for data protection.[179] LIBE would further stipulate what such safeguards should 'uphold'.[180]

Absent Commission decisions approving the country of destination's 'adequacy', or 'appropriate safeguards' through a legally binding instrument (eg using Commission or DPA-approved standard data protection clauses) under Art 42, or a derogation under Art 44, prior DPA authorisation would be required for *every* personal data export by a controller or processor.[181] This seems to fly in the face of

[170] Eg Ministry of Justice, Transparency & Human Rights, Hellenic Republic, D*iscussion Paper: International Transfers in the General Data Protection Regulation* (Informal Justice and Home Affairs Ministers' Meeting, Athens 23-24 January 2014) <http://gr2014.eu/sites/default/files/DISCUSSION%20PAPERS_YPDIK_INFORMAL%20ATHENS%20DATA%20PROTECTION-9%201%2013%20final.pdf> accessed 25 February 2014.

[171] Hon and Millard (n 169).

[172] Committee on Civil Liberties, Justice and Home Affairs, European Parliament (rapporteur: Jan Philipp Albrecht), 'Draft report on the 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)' (2013) PE501.927v04-00 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-501.927%2B04%2BDOC%2BPDF%2BV0%2F%2FEN>.

[173] Council Draft fn 307.

[174] As 'communication or availability of the data to one or several recipients' - Council Draft fn 51.

[175] This ties in with Art 4(7)'s definition of 'recipient' as an entity 'to which the personal data are disclosed', as 'disclosure' connotes imparting knowledge of intelligible data. It would also be consistent with the Council of Europe's Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (2001), which refers to transfers of personal data 'to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention'.

[176] LIBE would delete Art 34(1), presumably only because it duplicates Art 42, covered below.

[177] Council Draft fn 311.

[178] Council Draft fn 307.

[179] See n 46.

[180] Rec 83. The reference to 'guarantee the existence of a data protection officer' should be qualified as such officers may not be required in all circumstances, under the Reform Proposal.

[181] Ie 'for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer'. Art 42(5), which the Council would clarify by appending wording to Art 42(1). But which DPA would be competent, given one-stop shop issues?

modern technology, business practices and social expectations, and would require regulators to be far more heavily resourced than currently if they are to have a chance of dealing with the likely volume of requests for approval. Yet LIBE's Art 42(5) would restrict data exports further by deleting the provision permitting transfers on prior DPA authorisation, which seems retrograde. The Commission has power to make adequacy decisions, taking certain factors into account (Art 41[182]); one innovation is that it could declare particular processing sectors within a third country, eg healthcare, as adequate (Art 41(1)) – not just countries or territories within them. However, LIBE would impose a sunset clause on the Commission's existing adequacy decisions under DPD Arts 25(6) or 26(4) (including Safe Harbor and model clauses) so that they would expire five years from the date when the Reform Proposal would take effect (Rec 134, Art 41(8)). In contrast, the Council would preserve their validity pending an envisaged review of existing DPD adequacy decisions, which would involve an EDPB opinion (Art 41(3a)). Both LIBE (Art 41(6a)) and the Council (Art 41(3), (5)) would require the Commission, before issuing any adequacy decision, to request an EDPB opinion, with LIBE also requiring the Commission to provide the EDPB with necessary documentation and the Council requiring the Commission to 'take the utmost account' of the opinion, both of which we agree with. Both LIBE and the Council have suggested helpful clarifications and amendments, eg a duty on the Commission to monitor the functioning of its decisions (Art 41(4a)).

As regards 'appropriate safeguards' under Rec 89 and Art 42, LIBE would stress the need for guarantees to be 'legally binding', including financial indemnification, but again it ignores technical safeguards. Commission Draft Art 42(2)(b) would empower the Commission to adopt standard data protection clauses to provide such safeguards. However, LIBE would remove this power, giving only DPAs the power to promulgate standard data protection clauses, which they can do under a proposed consistency mechanism but subject to the Commission's approval (Art 42(2)(c)). The Council would require such DPA clauses to be subject to adoption by the Commission under an examination procedure.[183] LIBE would add a new appropriate safeguard, namely 'a valid 'European Data Protection Seal' for the controller and the recipient in accordance with paragraph 1e of Art 39'.[184] We welcome this, but suggest it should cover processors as well as controllers, and query whether the recipient too must always have a seal, eg in cloud computing where the controller has encrypted and backed up the data. Similarly, the Council would allow approved codes of conduct or certification mechanisms to provide appropriate safeguards (Art 42(2)(e)), but must they still be by way of 'legally binding instruments'?[185] Some Member States have queried the use of 'appropriate safeguards' procedures for cloud computing data flows.[186]

The Commission Draft explicitly recognises BCRs as a means of providing adequacy for data transferred within a group of companies,[187] which would be helpful as not all Member States currently accept BCRs approved by other DPAs and may require repetition of procedures.[188] BCRs for processors have become a reality since the adoption of a working paper by A29WP in June 2012 setting out requirements for processor BCRs and publication of the application and regulatory approval process in January 2013. The Commission Draft also explicitly recognises BCRs for processors. However, BCRs may not be useful in cloud computing as their application to processors and sub-processors *outside* the corporate group could be problematic for services involving layers of (unrelated) providers.[189] Indeed, two Member States requested that these provisions should cover data flows in the cloud computing context, and another Member State thought more flexibility should be provided in this way.[190] LIBE would delete reference to processor groups but add 'and those external subcontractors that are covered by the scope of the binding corporate rules' (Arts 43(1)(a), 43(2)(a)). Refusing to recognise processor BCRs seems retrograde, and it is unclear how external subcontractors (which may include cloud providers or sub-providers) would be covered by BCRs. Conversely, the Council would expand BCRs to 'the group of undertakings or group of enterprises

[182] The Council would add that the Commission should also take account of participation in a suitable international data protection system (eg the APEC Privacy Framework). Council Draft Rec 81, fn 11.

[183] Art 87(2). Similarly with Commission decisions on such clauses under Art 41(3).

[184] Art 42(2)(aa). Seals are discussed at 4.10.2below.

[185] Given Art 42(1)'s reference to 'legally binding instrument'.

[186] Council Draft fn 333.

[187] Art 43. While many Member States generally welcomed Art 43 on BCRs, several Member States had reservations about various provisions – Council Draft fn 348-357.

[188] Hon and Millard (n 169).

[189] Hon and Millard (n 169).

[190] Council Draft fn 348.

engaged in a joint economic activity', which might cover cloud sub-providers.[191] The Commission Draft would preserve pre-existing DPA authorisations (including BCR authorisations), as would the Council (Art 42(5b)), but LIBE would terminate them 2 years after the Reform Proposal enters into force (Art 42(5)).

As for derogations under Art 44, a new derogation (Rec 88, Art 44(1)(h)) would permit data exports 'necessary for the purposes of the legitimate interests pursued by the controller or the processor' subject to adducing 'appropriate safeguards' to protect the data based on a risk assessment of all the circumstances – only where the transfer is not 'frequent or massive', and in light of the nature of the data, purpose and duration of the processing etc (Art 44(3)). LIBE would delete these. The Council would change the qualification to 'not large scale or frequent'[192] and add (correctly in our view) a qualification that such transfers are permissible only when those legitimate interests are not overridden by the rights and interests of data subjects. Cloud computing, and indeed Internet, transfers are likely to be frequent or massive or large scale, and so are unlikely to qualify for this derogation. We recommend that given modern realities of such data flows, the focus should be on adducing appropriate[193] risk-based safeguards and considering whether rights and interests of data subjects may override on balance, rather than on frequency or size of transfers.[194] The Commission would be empowered to specify criteria and requirements for safeguards for 'massive' etc transfers; the Council would delete this, but LIBE would instead empower the EDPB to issue guidelines, recommendations and best practices to specify criteria and requirements for data transfers based on derogations (Art 44(7)). Commission Draft Art 44(6) would require documentation of the risk assessment and safeguards, and notification of the transfer to the DPA. LIBE would delete this, whereas the Council would delete the notification requirement.[195] A controversial derogation, related to concerns about third country authorities demanding EU data subjects' personal data, is for transfers 'necessary for important grounds of public interest' (Art 44(1)(d)). Such public interest must be 'recognised in Union law or in the law of the Member State to which the controller is subject',[196] ie not a third country public interest. The Council Draft would reduce this to 'necessary for reasons of public interest', with several reservations,[197] and, interestingly, would permit Union *or Member State* law to 'designate a public interest of special importance which opposes data transfers to recipients outside' the EU even under a prior adequacy decision (Art 44(7)).

Perhaps triggered by fears regarding foreign government authorities' access to cloud data, notably US authorities under the US PATRIOT Act, LIBE would specifically ban recognition or enforcement of judgements or orders of *non*-EU courts or authorities requiring transfer of personal data, 'without prejudice to' a mutual legal assistance treaty or relevant international agreement[198] – an approach advocated by the A29WP.[199] Such requests must also be notified 'without undue delay' to the DPA, whose *prior* authorisation is required for the transfer, and the data subject must also be informed. Also, 'Any legislation which provides for extra-territorial access to personal data processed in the Union without authorisation under Union or Member State law should be considered as an indication of a lack of adequacy' and transfer to that country should be prohibited (Rec 82). When 'appropriate safeguards' have been used, LIBE would also require notification of all access by third country public authorities 'regardless of national legislation' (Rec 89), and would insist that where controllers or processors face conflicting compliance requirements, EU law must take precedence over a third country's (Rec 90). This may be problematic for any controller or processor forbidden, by a non-EU law to which it is subject, to disclose the existence of the request, and could substantially increase the

[191] However, clarification here would be helpful.
[192] Adding to Rec 88 factors to consider in assessing whether transfers are massive or frequent – 'the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis' – but inexplicably deleting the Art 44(3) factors. Three Member States thought the terms were unclear – Council Draft fn 369.
[193] Or 'suitable', to avoid confusion with 'appropriate safeguards' in Art 42 – Council Draft fn 371.
[194] Two Member States would delete the 'frequent or massive' qualification – ibid.
[195] In view of administrative burdens - Council Draft fn 375 – although one Member State would require notification *before* the transfer.
[196] Art 44(5). The processor should be specifically mentioned here too.
[197] Council Draft fn 364.
[198] Art 43a, known as the 'anti-FISA clause' after the US Foreign Intelligence Surveillance Act.
[199] Eg in A29WP (n 30).

burden on DPAs if they must assess every such request.[200] Although LIBE would task the Commission with resolving jurisdictional conflicts (Rec 90, Art 45(1)(da)), that is likely to take more time than controllers or processors may be permitted under third country laws. Furthermore, such a ban addresses the wrong issue, and if adopted may lead to a false sense of security. As the UK Information Commissioner has put it, this provision 'will not resolve what is essentially a conflict of laws. Only an international political agreement can achieve this',[201] to which we would add that international agreement is also needed on the appropriate conditions for, limitations on, and transparency and oversight regarding, governmental access to personal data generally (including that of non-citizens). Self-help in the form of data encryption would also help deter excessive mass data surveillance,[202] and (to the extent possible) cloud users could seek, and some have indeed sought, contractual protections, eg terms requiring providers to notify them of requests for their data unless prohibited by law and to give access only on legally-binding court orders (not on mere request).[203]

Another difficult issue is onward transfers to another third country of personal data previously transferred in compliance with the Reform Proposal. Commission Draft Art 40 simply states, without more, that the rules on transfers to third countries apply to onward transfers. It may be problematic, both in theory and practice, to apply EU data protection rules restricting data exports to personal data *already* transferred to a third country. BCRs must specify 'requirements for onward transfers to organisations' not bound by the BCR, but this only repeats an existing requirement.[204] Clarification as to how restrictions on onward transfers should operate in practice is much needed. Finally, a new LIBE Art 22(3a) states that 'the controller shall have the right to transmit personal data inside the Union within the group of undertakings the controller is part of, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as well as the interests of the data subjects are safeguarded by internal data protection provisions or equivalent codes of conduct as referred to in Article 38'. As one of the key aims of the DPD (and Reform Proposal) was to enable free flow of personal data *within* the EU, this seems inexplicable and unnecessary. However, if desired, a provision could be added confirming that data flows within the EU should be permitted freely.

4.8.2 Summary and recommendations

The Reform Proposal's provisions on transfers generally would restrict use of cloud computing further, rather than encouraging it. Consideration should be given to abolishing the data export restriction and instead ensuring appropriate rules regarding access to intelligible personal data and data security,[205] as well as transparency and accountability (and international agreement sought on jurisdictional conflicts). If the restriction is to be retained, a definition of 'transfer' is urgently needed. We recommend that this be by reference to intention to give or allow logical access to intelligible personal data to a third party recipient who is subject to the jurisdiction of a third country. The positions regarding 'mere transit' and onward transfers also need clarification. The Commission as well as national DPAs should be empowered to make adequacy decisions, eg adopting standard clauses, after consultation with and taking full account of the EDPB's opinion. Given the reality of huge daily volumes of Internet transfers, prior authorisations by DPAs are not practicable and should be required only in selective appropriate cases rather than for routine transfers. Sunset periods for adequacy decisions, if too short, may jeopardise international trade and require unnecessary resources in handling renewals. Requiring recognition of BCRs for processors is positive, if retained, but

[200] See eg Google's Transparency Reports, showing the huge, and increasing, volume of requests received by Google from government authorities worldwide. Google Inc, 'Requests for user information' (*Google Transparency Report*)' <http://www.google.com/transparencyreport/userdatarequests/> accessed 25 February 2014 - over 25,000 in 2012, when Google complied with only 65% of requests.

[201] Information Commissioner's Office (UK), 'ICO views on the European Parliament LIBE Committee's approach to the draft General Data Protection Regulation and draft Directive on data protection in criminal justice and law enforcement' (*ICO*, 19 December 2013), 4 <http://ico.org.uk/news/blog/2013/~/media/documents/library/Data_Protection/Research_and_reports/ico-views-european-parliament-libe-committee-19122013.pdf> accessed 25 February 2014.

[202] Eg Snowden (n 179).

[203] Hon, Millard and Walden (n 70) Ch 4.

[204] A29WP, 'Working Document Setting up a framework for the structure of Binding Corporate Rules' (2008) WP154, [12] <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf>.

[205] See 4.5.

clarification is needed regarding exactly how external sub-contractors of controllers could be considered adequately covered by controller BCRs. Any ‘legitimate interests’ derogation should recognise modern realities of ‘frequent and massive’ data flows, and be permitted based not on size or frequency but on risk-appropriate safeguards and a balancing against data subjects’ rights and interests, with more guidance on what would be appropriate. Allowing transfers under a European Data Protection Seal, certification or code of conduct is also positive, but again more guidance is needed on the conditions/consequences. Technological safeguards, eg encryption, can provide effective protection, often more than contractual rights/liabilities, and their role should be given appropriate legal recognition, eg by allowing them to be taken into account when assessing adequacy of protection, rather than only permitting safeguards under ‘legally binding instruments’. Conflicts of laws must be taken into account beyond simply prohibiting controllers and processors who may be subject to laws of multiple jurisdictions from complying with non-EU laws, or making transfers under third country court orders etc subject to DPA approval; international agreement should be sought to resolve these issues, as well as to circumscribe appropriately and provide adequate safeguards regarding access to personal data by law enforcement or intelligence authorities or agencies. Finally, the permissibility of intra-EU transfers should be put beyond doubt.

4.9 Data breach notification

4.9.1 Provisions

Art 13a of the Framework Directive[206] requires the competent national authorities to be notified of breach of security and loss of integrity having a significant impact on the operation of networks. However, the DPD does not establish such an obligation relating to breaches of personal data, although some Member States have introduced data breach notification laws such as Germany’s section 42a, Federal Data Protection Act (Bundesdatenschutzgesetz). The Commission Draft would introduce, for the first time EU-wide, the concept of ‘personal data breach’ and a mandatory scheme to notify data breaches both to DPAs (Art 31) and data subjects (Art 32). The Commission Draft argues that personal data breaches ‘may result in substantial economic loss and social harm, including identity fraud, to the individual concerned’ (Rec 67). It defines personal data breach as ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed’ (Art 4(9)), targeting the confidentiality and integrity (but not availability) attributes of data security. The LIBE Draft would remove the reference to ‘a breach of security’. Thus, LIBE does not see personal data breaches as an end result of security breaches, but rather focuses on the outcome itself. The exact impact of such a modification of the definition of personal data breach is unclear and it depends on how the Commission understood ‘breach of security’. If a breach of security would cover only technical security measures, namely covering IT security, then the definition would be narrow. If it would actually include organisational security measures, then the Commission and the LIBE definition would actually be the same in effect, as for instance a ‘personal data breach’ would include unauthorised disclosure by employees who were authorised to access the data concerned, but misused their access rights. In this respect the definition of personal data breach should be clarified with regard to the types of breaches it is intended to cover, as this will ensure legal certainty with regard to the actual scope of application of the obligation to notify the breaches. However, the actual value of the notification, especially to data subjects, deserves special consideration (see below 5.9.1.2).

4.9.1.1 Notification to the DPA

The Commission Draft would introduce an obligation on controllers to notify the national DPA when a personal data breach has occurred (Art 31(1)). The Council would limit this to personal data breaches that are likely to ‘severely’ affect rights and freedoms of data subjects. We agree in principle that

[206] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L108/33, as modified by European Parliament and the Council of the European Union, Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services [2009] OJ L337/37.

notification of personal data breaches to the DPAs may not be necessary when the rights and freedoms of data subjects are not likely to be affected. However, it is unclear how ‘severe’ a breach must be (cf ‘material’), and in what way it must affect data subjects. We recommend that guidelines by the EDPB, as suggested by LIBE (discussed below), should include examples of situations likely to ‘severely’ affect the rights and freedoms of data subjects, e.g payment details. The Council would introduce an exception from this notification obligation in cases when communication of the breach to the data subject is not required because the controller has implemented appropriate technological protection measures, such as encryption or the use of pseudonymous data, or when the controller has taken subsequent measures to ensure that the rights and freedoms of the data subject are no longer likely to be severely affected (Art 31(1a)). It seems that, for the exception to apply, both those criteria must be satisfied, ie appropriate measures and subsequent measures, not just one of them, but this should be clarified. Although the notification obligation is addressed only towards controllers, ‘the processor’ involved (presumably only those affected by the breach, as one controller could use several processors) must inform controllers ‘immediately after the establishment of the data breach’ (Art 31(2)).

With regard to the time limit for notification to the DPA, the Commission Draft would require this to happen ‘without undue delay and, where feasible, within 24 hours’ after the controller becomes aware of the breach. Any notification after the 24 hours must be justified. The Commission Draft stated that to determine whether notification has taken place without undue delay, it should be ascertained ‘whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject’ (Rec 68). LIBE would require notification only ‘without undue delay’, removing reference to any specific timeframe, while the Council would extend it to 72 hours, where feasible. As for the content of the notification, the Commission Draft details the minimum required information, including categories and number of data subjects concerned (which the Council would require only where possible and appropriate), and recommends measures to mitigate the possible adverse effects of the breach, as well as its consequences (Art 31(3)). LIBE would allow the information to be provided ‘in phases’ if necessary.

The controller must provide the DPA with sufficient documentation, describing the facts surrounding the breach, its effects and any actions take to remedy it. Such documentation must enable the DPA to verify the controller’s compliance with the breach notification requirement. This is a transparency mechanism to demonstrate the accountability of controllers in cases of personal data breaches. The Commission and the Council (with some Member State objections) would empower the Commission under Art 31(6) to prescribe the standard format of notifications, their procedures and the form and the modalities of documentation required. LIBE would instead empower the EDPB to issue (non-binding, but clearly persuasive) guidelines, recommendations and best practices, not only for establishing a breach and determining ‘undue delay’, but for ‘particular circumstances in which a controller and a processor are required to notify the personal data breach’, which we support.

LIBE Draft Art 31(4a) would oblige DPAs to maintain a public register of the ‘types’ of breaches notified. If the register identifies the controllers involved, this could result in publicly ‘naming and shaming’ them, even when they have taken all appropriate technical and organisational measures to protect their data. The types of information to be included in such a public registry, where it seems all personal data breaches would be included irrespective of potential responsibility of the controllers (or even the processor they have chosen), should be clarified, as well as the level of detail to be included, in order to avoid providing information to such a detail that security weaknesses can be easily spotted, which may result in further breaches.

4.9.1.2 Notification to the data subject

After notifying the DPA, the controller must notify personal data breaches to data subjects, when ‘likely to adversely affect the protection of the personal data or privacy of the data subject’ (Art 32(1)). Under Commission Draft Rec 67 a breach should be considered to have such adverse effect where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. LIBE would require notification of the data subject also when the breach is likely to adversely affect the data subject’s rights or ‘legitimate interests’, which is very broad and unclear.

Conversely, as with notification to DPAs, the Council would require communication of breaches to data subjects only when likely to 'severely' affect data subjects' rights and freedoms. LIBE Draft Art 53(1)(a) would empower DPAs to order controllers to communicate personal data breaches to the data subjects.

The Commission Draft would require controllers to communicate personal data breaches to data subjects without undue delay, with no reference to a specific timeframe (see previous sub-section for criteria on determining 'undue delay'). Less minimum information is required to be given to data subjects than to DPAs. Such communication shall describe the nature of the personal data breach, the identity and contact details of the DPA or another contact point, and recommend measures to mitigate the possible adverse effects of the breach (Art 32(2)). The LIBE Draft would also require inclusion of information about data subjects' rights, including redress, and communications must be comprehensive and use clear and plain language (although query 'comprehensive' cf 'comprehensible' – it is difficult to be both comprehensive and clear, and surely data subjects do not need to know full technical details).

The Commission Draft would not require communication of the breach to data subjects when the controller demonstrates to the DPA's satisfaction that they have implemented, and applied to the data concerned by the breach, appropriate technological protection measures that rendered the data unintelligible to unauthorised persons (Art 32(3)). Thus, the Commission wished to incentivise the industry to implement encryption measures to protect personal data due to the increasing number of data breaches in Europe.[207] However, this apparent acknowledgement of the use of modern cryptography technologies, and of the security of strongly encrypted data, was not extended further in the Commission Draft, although the UK ICO considers that 'where encrypted data is lost but the decryption key remains safe, there will not have been a "personal data breach"'.[208] The Council helpfully would mention explicitly encryption and use of pseudonymous data as examples of technological measures rendering data unintelligible. It would also introduce further exceptions from the obligation of controllers to communicate a personal data breach to data subjects, when they have taken subsequent measures to ensure that data subjects' rights and freedoms are 'no longer likely to be severely affected', or when the notification would adversely affect a substantial public interest (not however stated to be that of the EU or Member State). Moreover, when notification to data subjects would involve disproportionate effort, in particular due to the number of 'cases involved', the Council would permit controllers to make a public communication or a similar measure instead (Art 32(3)).

4.9.2 Summary and recommendations

Notifications of personal data breaches could increase transparency within a cloud ecosystem. However, such notifications are part of the broader issue of allocating responsibilities between the multiple actors holding a role in the cloud chain and, especially, specifying who is the cloud actor acting as a controller. The definition of personal data breach should be clarified with regard to the types of breaches it is intended to cover, especially given the LIBE proposed amendment, ie whether it covers only technical security measures, or also organisational ones. We suggest that the LIBE amendment requiring creation of a public register of personal data breaches should specify what information must be included in the register, and to what level of detail. Controllers who use cloud computing often depend on the processor's security and breach detection measures (although not always, eg the controller's own employees, authorised to access cloud data, may disclose data for unauthorised purposes). In terms of timing, we support 'without undue delay' rather than specifying hard time limits. It is important to clarify the threshold for notifications: a balance is needed between 'severely affects' and simply 'affects'. Rather than imposing direct notification obligations on cloud

[207] Eleni Kosta and Colette Cuijpers, 'The draft Data Protection Regulation and the development of data processing applications', in M Hansen et al (eds), *Proceedings of the IFIP Summer School on Privacy and Identity Management 2013*, IFIP AICT 421 (Springer 2014) (forthcoming).

[208] Information Commissioner's Office (UK), 'Proposed new EU General Data Protection Regulation: Article - by - article analysis paper' (*ICO*, 12 February 2013) 42 <http://ico.org.uk/news/~/media/documents/library/Data_Protection/Research_and_reports/ico_proposed_dp_regulation_analysis_paper_20130212_pdf.ashx> accessed 25 February 2014. As explained at 4.1, regulators would treat encrypted personal data as personal data even in the hands of a mere storage provider without the key, and would not recognise (for the purposes of the requirement to delete data that have served their purpose) that deleting the decryption key for strongly-encrypted data may be as effective as deleting the actual data.

providers under Art 30(2), who may not always be aware that personal data are processed using their infrastructure, only controllers should be responsible (or E-Commerce Directive-type exemptions extended to processors of personal data, as previously discussed). To enable controllers to comply with their obligations, they may well impose contractual obligations on their processors regarding security breach detection and notification. If they cannot do so, under many cloud providers' non-negotiable standard terms of service, it may be that controllers would be unable to both use cloud computing and comply with breach notification provisions, which may lead to avoidance of cloud computing or to non-compliance on the part of controllers. Another possibility is that cloud services would be offered containing breach notification requirements and other contract terms required by the Reform Proposal, but at higher prices.

4.10 Codes of conduct and certification

Codes of conduct and certification are particularly important means for increasing transparency and accountability in the cloud, given that people are 'concerned about which cloud providers they can trust'.[209] They are both voluntary mechanisms and will be, therefore, discussed together below.

4.10.1 Codes of conduct

The Commission Draft would task the Commission, DPAs and Member States with encouraging the industry to draft codes of conduct aiming at contributing to the proper application of the Regulation (Art 38(1)). The Council would add the EDPB to these bodies, while LIBE would add codes of conduct drawn up by DPAs. The Commission Draft would allow any bodies representing categories of controllers to be involved in drafting codes of conduct or proposing amendments, while LIBE and the Council would extend this possibility to processor representatives, which we support particularly in relation to cloud providers. Under the Commission Draft, codes of conduct must take into account specific features of various processing sectors, particularly regarding, for instance, fair and transparent data processing, 'the information of the public and of data subjects', transfer of data to third countries or international organisations and mechanisms for monitoring and ensuring adherents' compliance with the code. These could be relevant to cloud computing. It has been argued that presumably 'compliance with a code of conduct would also satisfy the legal requirements of the Proposed Regulation, but this should be made more explicit in the text',[210] ie the legal consequences of adherence to codes of conduct need to be clarified (see 3.3 and below). LIBE would require codes of conduct to take into account consumer rights, while the Council would specifically allow codes to cover, among other things, the legitimate interests of controllers, use of pseudonymous data and principles of data protection by design and by default (Art 38(1a)). The Council also proposes that codes of conduct should take into account specific needs of 'micro, small and medium-sized enterprises'. LIBE sees codes of conduct as a means to facilitate industry compliance with the Regulation (Rec 76), as does the Council, which in several areas would provide that adherence to codes should suffice to demonstrate compliance. The Council would, correctly, require a code of conduct to include mechanisms for monitoring and ensuring compliance by controllers and processors which adopt it, establishing a new accountability mechanism and creating, therefore, an additional safeguard for compliance (Art 38(1b)). Finally, the Council Draft would add a new Art 38a on the monitoring of compliance with codes of conduct by DPA-accredited bodies, which would increase the credibility of codes of conduct within the broader context both of the market and the society.

4.10.2 Data protection certification, seals and marks

The DPD did not include any mechanisms to demonstrate compliance with data protection rules. However, the Reform Proposal pays special attention to use of data protection certification mechanisms, seals and marks that would contribute to the demonstration of compliance of controllers and processors and function as accountability mechanisms. The Commission Draft would entrust the Commission and Member States with encouraging, especially at European level, the establishment of

[209] Neelie Kroes, 'EU Data protection reform and Cloud Computing' (Data protection reform and Cloud Computing "Fuelling the European Economy" event, Brussels, 30 January 2012) SPEECH/12/40 <http://europa.eu/rapid/press-release_SPEECH-12-40_en.htm> accessed 25 February 2014.

[210] Christopher Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', (2012) 11 Privacy & Security Law Report 6, 3.

mechanisms allowing data subjects to assess in a quick and easy way the level of data protection provided by controllers and processors. Such mechanisms can involve data protection certifications as well as data protection seals and marks. The certification mechanisms to be put in place shall 'contribute to the proper application' of the Regulation, taking into account specific features of various sectors and different data processing operations (Art 39(1)), which the Council would amend to refer to the purpose of demonstrating compliance. The Council would add the EDPB to the bodies that should encourage establishment of certification mechanisms, and provide specifically that a certification 'does not reduce the responsibility of the controller or the processor for compliance' (Art 39(2)), which seems at odds with the aim of incentivising controllers and processors to obtain certifications (see 3.3), and is not stipulated in relation to codes or seals. The Council Draft would emphasise that certification mechanisms, seals and marks are to be used as accountability mechanisms to demonstrate compliance of controllers and processors. LIBE would require DPA certifications to be affordable and available for a reasonable fee and via a transparent and not unduly burdensome process, harmonised within the EU (Art 39(1b) and (1c)). As currently most cloud providers are not based in the EU and are not necessarily concerned with complying with European data protection legislation, the adoption of data protection certification mechanisms could be a valuable tool for cloud users, who might be more comfortable entrusting their personal data to cloud service providers that are compliant with the EU rules. LIBE would allocate a significant role to DPAs for certification processes, as well as for accreditation of third party auditors (Art 39(1d)). The Council would further introduce a separate Art 39a elaborating on the role of certification bodies and procedures for accreditation by DPAs. We support these provisions, but criteria for accreditation and accreditation details, as well as certification criteria and details, should be made public, and fees for accreditation should be reasonable.

The LIBE Draft would introduce also a standardised data protection mark, named the 'European Data Protection Seal', which would be granted to controllers and processors by DPAs (Art 39(1e)). A European Data Protection Seal should be established at a European level 'to create trust among data subjects, legal certainty for controllers, and at the same time export European data protection standards by allowing non-European companies to more easily enter European markets by being certified' (Rec 77) (and see also 3.3 regarding the potential value of seals to shield controllers or processors from administrative sanctions for non-negligent and unintentional breaches, which concept could be extended to codes and certifications; indeed the concepts of seals and certifications could perhaps be combined). A public electronic record of all valid and invalid certificates issued in Member States would be established by the EDPB (Art 39(1h)).

4.10.3 Summary and recommendations

We agree that processor representatives should be permitted to be involved in drafting of codes of conduct. Cloud providers will usually be processors, for instance. Both the A29WP and the EDPS welcomed the introduction of certification schemes for cloud computing. The A29WP acknowledges that 'independent verification or certification by a reputable third party can be a credible means for cloud providers to demonstrate their compliance with their obligations', and that standards and certifications are central to establishment of a 'trustworthy relationship between cloud providers, controllers and data subjects'.[211] While the EDPS acknowledged the importance of certification mechanisms he pointed out that, 'especially in the context of cloud computing, more specific guidance is required to clarify which mechanisms should be put in place to ensure verification of the effectiveness of data protection measures in practice. Unless this happens, these verification exercises risk measuring compliance only on 'paper' but not in 'reality'.'[212] The use of data protection standardisation mechanisms could be very valuable for EU customers of cloud services, since most major cloud providers are based outside the EU. Several Standards Developing Organisations (SDOs) have recently started to study cloud computing in relation to the development of information privacy protection standards.[213] To foster cloud computing in the EU, the ETSI's Cloud Standards

[211] WP196, 22.
[212] EDPS (n 161) [71].
[212] Kuner (n 210).
[213] Stéphane Guilloteau and Venkatesen Mauree, 'Privacy in cloud computing, ITU-T Technology Watch Report', (*ITU,* March 2012) 14-16 <http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf> accessed on 25 February 2014.

Coordination initiative (CSS) was established upon the request of the Commission focusing among other things on security and privacy as well as interoperability and data portability. Explicit reference in the Reform Proposal to data protection certification mechanisms should encourage such initiatives. However, we support LIBE's proposal that certifications should be affordable and available via a process that is transparent and not unduly burdensome, and this should apply to accreditations also. The European Data Protection Seal may have value in shielding controllers and processors for non-negligent and unintentional breaches, and this approach should be extend to certifications and codes. We recommend merging the concepts of certifications and seals and their requirements, for simplicity. Finally, as previously mentioned, the consequences of obtaining certifications or seals need to be spelled out more clearly.

4.11 Right to erasure

4.11.1 Provisions

The Commission Draft would introduce a new right to be forgotten and to erasure, which raised a fierce debate regarding the meaning of 'forgetting' and the consequences that would entail for controllers, in view of the difficulty of ensuring erasure of personal data from all possible locations once 'made public' on the Internet, particularly where third parties have republished the data online. The European Union Networks and Information Security Agency (ENISA) expressed reservations about the practicability of this right, pointing out technical limitations in terms of the means to enforce or support the right in information systems, and the need for clearer definitions and legal clarification.[214]

The Commission Draft would extend and detail the right to erasure, already established under Art 12(b) DPD. The Commission Draft would entitle data subjects to 'the erasure of personal data relating to them and the abstention from further dissemination of such data', especially personal data made available by the data subjects while they were a child, when the data are no longer necessary for the purposes for which they were processed; when the data subjects withdraw their consent, the consent period has expired or there is no other legal ground to legitimise data processing; when the data subject objects to the processing; or when the processing is not compliant with the Regulation for any other reason (Art 17(1)). LIBE and the Council would replace the last ground with unlawful processing, which is broader than non-compliance with the Regulation. LIBE would add as a ground for data erasure the final and absolute decision of an EU court or regulatory authority that the data must be erased. The Council Draft would oblige the controller to erase the data 'without undue delay', while also requiring erasure to comply with a legal obligation to which the controller is subject (which could include a contractual obligation or order of a non-EU court).

Under Commission Draft Art 17(2) a controller who made the data public must take *all reasonable steps*, including technical measures, to inform third parties about the request to erase any links to, or copies of that personal data. Moreover, a controller who has made personal data public would be obliged to inform third parties about the data subject's request to erase any links to, or copies or replications of that personal data (Rec 54). Whether 'all reasonable steps' will result in all third parties being informed of the erasure request, and whether or not the parties informed will respect the request, cannot be guaranteed. The LIBE Draft deleted references to the right to be 'forgotten' and combined the rights in Commission Draft Arts 17(1) and (2), creating a right for data subjects not only to obtain erasure of their data, but also to obtain from third parties the erasure of any links to, or copy or replication of that data. Where a controller has made personal data public without a justification under Art 6(1) (on lawfulness of processing), it must take all 'reasonable steps, including technical measures', to have data erased including by third parties. Further clarification is needed on how that could be achieved in practice in an online environment. A particular issue in cloud is that some providers take automatic backups of data, so where the controller may be obliged to delete personal data under the right to erasure, it may not be able to ensure copies are deleted from all backups, unless it so stipulates in its contract with the provider.

[214] Peter Druschel, Michael Backes and Rodica Tirtea, 'The right to be forgotten – between expectations and practice' (*ENISA*, 2011) <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport> accessed 25 February 2014.

The Council would add Art 17(2a) providing that when controllers have made personal data public and are obliged to erase them, they should take into account the cost of implementation and available technology, in taking reasonable steps, including technical measures, to inform controllers about a data subject's request for erasure. The Council Draft requires only controllers to be informed and not other third parties, unlike the Commission Draft. Three Member States have suggested referring to 'known' controllers (or third parties), limiting to an extent the obligation of the controller that made the data public. We support the proposal to clarify that the obligation should be extended to 'known' controllers, so as not to disproportionately burden controllers, and suggest stipulating explicitly that the erasure should be to a degree appropriate to the risks taking into account the cost of implementation and available technology.[215] Such clarifications would benefit cloud computing by creating a clearer framework for cloud providers.

The Commission Draft Art 17(3) would allow retention of personal data notwithstanding an 'erasure' request, in certain limited circumstances, eg for the exercise of freedom of expression, 'for reasons of public interest in the area of public health', etc. The Council would introduce further exceptions, namely, where processing is necessary for 'purpose of social protection' (Art 17(3)(ca)) and when necessary for 'the establishment, exercise or defence of legal claims' (Art 17(3)(g)). A specific accountability requirement is that the controller must 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' (Art 17(7)), which seems to tie in with Art 5(e) on data retention. LIBE would move this to Art 17(8a) but the Council would delete it. Art 17(8) requires oddly that 'Where the erasure is carried out, the controller shall not otherwise process such personal data' - suggesting that even after data 'erasure' a controller would be capable of processing the 'erased' data. Another interpretation could well be that whenever an erasure request is complied with, the controller must simply erase the data and not do anything else with the data. Clarification of this issue would be helpful.

The Commission Draft does not define 'erasure'. It would allow the 'restriction' of personal data, instead of erasure (which seems to suggest a 'hold'), where the data subject contests data accuracy and the controller needs time to verify this; where data have to be maintained for purposes of proof; when the data subject asks for restriction of use instead of erasure in cases of unlawful processing; and when data subjects request transmission of data to another automated system exercising their right to data portability (Art 17(4)) (although it is odd that data are not required to be erased after such transmission). What such a 'restriction' means is not defined or described, save that it appears to involve storing such data but not processing them except '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' (Art 17(5)), in which event the data subject must be informed before the processing (Art 17(6) – although 'lifting the restriction' should be clarified by reference to Art 17(5), if that is the intention; it could be taken to refer to processing other than that specified in Art 17(5)). LIBE would require the controller to restrict the data 'in such a way that it is not subject to the normal data access and processing operations and cannot be changed anymore'. The Council would split out the right to restriction of processing to a separate Art 17a. It is difficult to understand though why the possibility to restrict data is limited to these specific situations proposed in the Regulation, and why for example it could not be introduced in cloud computing environments as an alternative to erasure.

4.11.2 Summary and recommendations

Time-conditioned licenses carried by so-called 'sticky technologies' have been named among the tools for implementing the right to be forgotten.[216] ENISA reports, though, that, regardless of the intentions behind the proposed right, enforcement by 'a purely technical and comprehensive solution' is generally impossible in the open Internet and '[a]n interdisciplinary approach is needed, with an important role assigned to search engines and sharing services 'to filter references to forgotten information.''[217] Given the possible replication of data in the cloud, which assists integrity and availability, it is important to define clearly what is meant by 'erasure' and 'restriction', and to what degree – eg, what is appropriate to the nature and sensitivity of the data, etc.

[215] See paragraph containing n 51.

[216] Eg Bert-Jaap Koops, 'Forgetting footprints, shunning shadows: A critical analysis of the 'right to be forgotten' in big data practice' (2011) 8(3) SCRIPTed 229.

[217] Druschel, Backes and Tirtea (n 214) 2.

4.12 Data portability

4.12.1 Provisions

The right to data portability is a new right that the Commission Draft would introduce, characterised by some as a competition rather than a data protection law issue. It would enable data subjects to transfer their data between electronic processing systems without being prevented from doing so by the controller, and further improve access of individuals to their personal data. Commission Draft Art 18(1) would entitle data subjects to obtain from the controller a copy of their data in “an electronic and structured format which is commonly used and allows for further use by the data subject”. This right would be exercisable regardless of the legal basis of processing. This right does not enable the data subjects to ‘take their data and leave’, given that it allows them simply to get a copy of the data for their own use, unless the right to erasure was extended accordingly. The Commission would be able in this case as well to specify formats and technical standards through the adoption of implementing acts (Art 18(3)). Art 18(2) would introduce a specific right to data portability, a separate right entitling data subjects to transmit their personal data from an automated processing system (such as a social networking service) into another one in an electronic format which is commonly used. However, unlike the Art 18(1) right, this right would only apply where the processing of personal data is based on data subject consent or on a contract. LIBE would delete Commission Draft Art 18 and treat the right to data portability as part of the right to access and to *obtain* data (Article 15(2a)). It has been suggested that the right to data portability should be accompanied with a duty for controllers to provide for interoperability.[218] LIBE would add that the copy of the personal data to be given to the data subject must be in an ‘interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn’. The Council Draft would restate the right as a right of data subjects to ‘withdraw’ their personal data in such a form that would allow transmitting them into another automated processing system provided by an information society service without hindrance from the controller (Art 18(2)), which seems narrower than LIBE’s ‘interoperable’ or ‘commonly used’ formats, but it is unclear whether ‘withdraw’ requires erasure after transmission, and this should be clarified.[219] Moreover, the explicit reference to information society services actually limits the right to data portability to cases relating to information society services.[220] Both the Council and LIBE would delete the general right in Commission Draft Art 18(1) and restrict the data portability right to situations where the data subject has ‘provided’ the personal data and further, in the Council’s case, only where the processing is based on consent or contract. Clarification is needed regarding when data subjects ‘provide’ their data, eg is this meant to exclude situations where data are automatically collected from devices or usage rather than actively given by data subjects, such as cookie information and location data? In a cloud webmail service, are emails ‘provided’ by the data subject only when sent by, but not to, the data subject? Is the proposed restriction by reference to data ‘provided’ feasible? Furthermore, under Council Draft 18(2) the right to portability would apply only where processing ‘is carried on in an automated processing system provided by an information society service’, so this right may apply to SaaS services such as social networking but not necessarily IaaS storage. Finally, Council Draft Art 18(2a) would stipulate that the right to data portability ‘shall be without prejudice to intellectual property rights’, a missing parameter in both other Drafts, raising the important issue of such rights in relation to cloud data.[221]

4.12.2 Summary and recommendations

The right to data portability aims to further strengthen data subjects’ control over their personal data and their right of access (Rec 55). As far as cloud computing is concerned, the right to data portability increases the accountability obligations of controllers, who have to ensure personal data are in an

[218] Gerrit Hornung, ‘A general data protection regulation for Europe? Light and shade in the Commission’s draft of 25 January 2012’ (2012) 9(1) SCRIPTed 74.

[219] Similarly some Member States have queried the meaning of ‘automated processing system’ – Council Draft fn 164.

[220] Ie ‘any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services’. Art 1(2), Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, [1998] OJ L204/37 as amended.

[221] Chris Reed and Alan Cunningham, ‘Ownership of Information in Clouds’, Ch 6 in Millard (ed) (n 12).

interoperable or at least transferable format (we prefer LIBE's formulation regarding 'commonly used'), allowing users to transfer their data to another platform that offers a similar service. Thus, controllers may wish to choose cloud providers that allow data to be retrieved in such formats, perhaps including contractual provisions to that effect. The right to data portability aims at minimising customer 'lock-in' situations. The two paragraphs of Commission Draft Art 18 read together reveal how limited is the scope of control that the right offers, especially given the breadth of situations when processing of data is not based on consent or contract.[222] The practical cases when this expression of the right to data portability can be applied seem rather limited. If adopted in the form proposed by the Commission or the Council, the right to data portability will not have significant application in cloud computing, although under the LIBE Draft the right would be broader. Also, it is not clear what 'provided by the data subject' should mean. If interpreted as 'actively given by the data subject', Art 18(2) guarantees will be of limited relevance for cloud computing and indeed Internet environments where data are not necessarily provided directly by the data subject. The right to data portability goes hand in hand with the right to erasure, triggering within the cloud environment concerns on their practical application. Although the importance of the right to data portability for individual cloud customers has been explicitly acknowledged,[223] the EDPS points out that 'in order to implement this right, it is important that, once the data have been transferred, no trace is left in the original system', while 'in technical terms, it should become possible to verify the secure erasure of data'[224].

5 Conclusions

The definition of 'personal data' triggers application of the EU data protection regime. If the test is set so broadly that most information is 'personal data', the obligations applicable need to be more carefully calibrated. Introducing the concept of pseudonymous data is one way, with fewer obligations applying to such data, but its definition needs care, and the obligations that are to be adapted for pseudonymous data should be considered carefully also. We support the aim of encouraging anonymisation or pseudonymisation of personal data, but it should be made clear that the procedure of anonymisation or pseudonymisation is permitted.

In terms of both controller and processor liability, policy decisions need to be taken on which obligations should be 'strict liability' regardless of fault, for the protection of data subjects, and which obligations should be risk-based, requiring only the taking of measures appropriate to the individual situation, or reasonable measures to industry standards and the like. Proposals for codes of conduct, certifications and seals are welcome as accountability mechanisms, but incentives are needed to encourage cloud actors to invest time and money in adopting them, in particular clear liability consequences where codes etc are adopted, such as defences for breach of specific obligations, not just in relation to administrative but also judicial sanctions. If it is thought too radical to rule that providers of technology infrastructure should not even be 'processors', defences along the lines of those under the E-Commerce Directive for intermediaries should be available to processors in relation to personal data, so that knowledge and control of personal data (including access to intelligible personal data) are pre-requisites to cloud provider liability.

Given these issues, rather than impose joint liability on processors and co-controllers, a more fault-based allocation of liability is recommended, and consideration given to specifying clearly which obligations should be imposed on processors, also taking the availability of insurance into account. The status of data centres and hardware/software providers as well as EU subsidiaries of third country actors needs to be clarified. To avoid discouraging non-EU controllers and providers from using EU data centres and EU cloud providers or sub-providers, the concepts of 'establishment', 'context of activities' and 'offering' need to be clarified, and the intended extra-territorial scope of EU data protection legislation carefully defined.

We welcome the updating of security requirements in line with general concepts of confidentiality, integrity and availability, but specific reference should be made to encryption and backups as example measures, to help raise awareness. Data protection by design and default need to be clarified as

[215] Colette Cuijpers, Nadezhda Purtova and Eleni Kosta, 'Data Protection Reform and the Internet: the draft Data Protection Regulation', in A Savin and J Traskowski, *Research Handbook on EU Internet Law* (Edward Elgar 2014) (forthcoming) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2373683>.

[223] EDPS (n 161), [113].

[224] EDPS (n 161), [117].

regards their requirements and scope, and again should take account of infrastructure providers not necessarily knowing the nature of data processed using their infrastructure, and controllers and processors not having total control over all infrastructure used. We support requiring data protection impact assessments, but only when warranted by the risks involved, whereas the Reform Proposal would require assessments in a very broad range of situations. Also, new technologies should not be treated as risky per se – risks depend on the purpose for which and manner in which they are to be used and the type and sensitivity of the data concerned.

Proposals on international transfers of data would be more restrictive than currently, and threaten to hold back cloud computing. Consideration should be given to abolishing the data export restriction and instead ensuring appropriate rules regarding access to intelligble personal data and data security, as well as transparency and accountability (and international agreement sought on jurisdictional conflicts and rules restricting government access to personal data). If the restriction is to be retained, 'transfer' should be defined by reference to intention to give or allow logical access to intelligible personal data to a third party recipient who is subject to the jurisdiction of a third country. Given the reality of huge daily volumes of Internet transfers, prior authorisations by DPAs are not practicable and should be required only in selective appropriate cases rather than for routine transfers. Similarly, any 'legitimate interests' derogation should be based not on size or frequency but on risk-appropriate safeguards and a balancing against data subjects' rights and interests.

Clarification is needed regarding the types of data breaches to be notified, thresholds and the detailed contents of any public register, but we recommend deletion of 'hard' time limits. Processor representatives should be entitled to give input regarding codes of conduct, but more guidance is needed regarding certifications, codes and seals, and the provisions on certifications and seals could be merged. As regards the right to erasure, given the possible replication of data in the cloud, which assists integrity and availability, it is important to define clearly what is meant by 'erasure' and 'restriction', and to what degree – eg, what is appropriate to the nature and sensitivity of the data, etc. The right to data portability is very limited in scope, and its limits could be reconsidered, including its relationship with the right to erasure.

In summary, the Reform Proposal would modify the accountability relationships between data protection actors, compared with the current regime of the DPD. The Reform Proposal would widen the ambit of who is accountable (processors established in the EU, controllers offering into the EU), expand what they will be accountable for (wider and new obligations), and change who they would be accountable to and how (regulatory authorities and data subject). This White Paper has elaborated on these issues, provided an analysis of the relevant provisions of the Reform Proposal that are likely to have an impact on accountability for personal data in the cloud, and recommended some suggested amendments that it is considered would provide for cloud accountability in a clearer, more balanced and technologically-neutral way.

6 Appendix: Background to the EU data protection reform process

6.1 Context and Commission proposals

Recognising that EU data protection laws needed updating in light of extensive technological, social and commercial developments since 1995, the European Commission launched a public consultation and engaged with stakeholders on the EU data protection framework in May 2009. Following consideration of responses received, in January 2012 the Commission issued draft reform proposals in the form of a draft General Data Protection Regulation (**Commission Draft**) together with a draft Directive on processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (including police and judicial cooperation) (**Draft Directive**). Cloud computing was specifically cited as one of the technological developments driving the need to modernise data protection laws.[225]

A Regulation was proposed to replace the current Data Protection Directive, rather than a Directive (or even maximum harmonisation Directive), with the aim of eliminating the current fragmentation and legal uncertainty, costs and burdens arising from 27 (since increased to 28) different national data protection laws for businesses operating in Europe's single market.[226] This White Paper only discusses the draft general Data Protection Regulation, and *not* the Draft Directive on the processing of personal data for policing and criminal justice purposes.

The three main policy objectives behind the reform proposals were:[227]

1. To enhance the internal market dimension of data protection (harmonisation, clarification and consistency across Member States, and reducing red tape).

2. To increase the effectiveness of the fundamental right to data protection (individuals' control over their personal data and trust of the digital environment, continued protection including when their data are processed abroad, and reinforcing the **accountability** of those who process personal data).

3. To establish a comprehensive EU data protection framework and enhance the coherence and consistency of EU data protection rules, including in the field of police cooperation and judicial cooperation in criminal matters.

6.2 Parliament

Within Parliament, the proposals were referred to several standing committees of MEPs for their opinions, with each committee appointing a 'rapporteur' to produce a draft report or opinion on the proposals. These committees were ITRE (industry), rapporteur Seán Kelly; IMCO (internal market and consumer protection), rapporteur Lara Comi, and LIBE (civil liberties), rapporteur Jan-Philipp Albrecht. LIBE is the main Parliamentary committee assigned responsibility for scrutinising these proposals. JURI (legal), rapporteur Marielle Gallo, and EMPL (employment), rapporteur Nadja Hirsch, also

[225] Eg Commission, 'Data protection reform: Frequently asked questions' (*Commission*, 25 January 2012) MEMO/12/41 <http://europa.eu/rapid/press-release_MEMO-12-41_en.htm> and Commission, 'Safeguarding fundamental rights – Adapting EU data protection to the digital age to clear citizens' doubts about the cloud' (*Commission*, 27 January 2012) <http://europa.eu/rapid/press-release_ETW-12-2701_en.htm#Topic1> both accessed 25 February 2014.

[226] 'I have chosen a Regulation because this is the only way to achieve real harmonisation and consistency of the rules on data protection. As experience since 1995 has taught us, we would not have achieved this level of harmonisation with a Directive. Instead, as we all know, today we have a patchwork of rules which did not offer sufficient protection to individuals, and which did not provide a uniform and reliable regulatory environment for businesses.' Viviane Reding, 'Strong and independent data protection authorities: the bedrock of the EU's data protection reform' (Spring Conference of European Data Protection Authorities, Luxembourg, 3 May 2012) SPEECH/12/316 <http://europa.eu/rapid/press-release_SPEECH-12-316_en.htm> accessed 25 February 2014. However, while a Regulation may seem preferable for harmonisation purposes, if any provisions of the Regulation are insufficiently clear there may still be fragmentation, as different Member States may interpret ambiguous provisions of a Regulation differently. Furthermore, in certain areas the Reform Proposal gives Member States scope to enact different national laws. Accordingly, a Regulation will not necessarily guarantee consistency in data protection laws or their application across the EU.

[227] Commission Staff Working Paper (n 23), 43.

provided opinions. (The Economic and Monetary Affairs Committee (ECON) decided not to give an opinion.)[228]

A record-breaking number of amendments were proposed. ITRE voted on over 900 amendments to the draft, while IMCO voted on over 400 (and approved over 200) amendments; the draft LIBE report contained over 3000 proposed amendments. After several postponements, in October 2013 LIBE voted to approve[229] its own draft report,[230] accepting all the compromise amendments proposed by Albrecht. LIBE also authorised Albrecht to negotiate with the Council and Commission on the Reform Proposal in the 'trilogue' that would then follow, aiming to align the different institutional views on the EU data protection reform proposals. Parliament as a whole (ie in 'plenary session') will debate and vote on the draft report, in Parliament's first reading on the proposals in around April 2014.[231]

However, the position is complicated by the 22-25 May 2014 EU elections.[232] If the Reform Proposal is not agreed between all three EU institutions by the time of the last plenary session of Parliament before these elections (14-17 April 2014[233]), which seems likely given disagreements within the Council (covered below), then Parliament's unfinished business will lapse.[234] After the next Parliamentary term starts (the earliest session being 1-3 July 2014), the Conference of Presidents of the Parliament may decide, on reasoned requests from Parliamentary committees and other institutions, to resume consideration of any lapsed business. If the Parliament decides to resume work on the Reform Proposal, the LIBE report will remain valid, as will Albrecht's mandate (if he is re-elected).

6.3 Commission

A new Commission President will be chosen in July 2014. New candidates for the College of Commissioners (28, one from each Member State) will be considered between then and 31 October 2014, when the current Commission's term of office expires,[235] to serve the standard five-year term.[236]

The Commission may alter its legislative proposals at any time before the Council has acted.[237] It remains to be seen what action the new Commissioner responsible for data protection will take on the Reform Proposal. The DPD itself was originally proposed in 1990 but, after much controversy, the Commission presented an amended proposal in 1992, which after further amendments was eventually adopted in 1995.

[228] See European Parliament Legislative Observatory Procedure File, <http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011(COD)> accessed 25 February 2014. A rapporteur's draft opinion may contain a draft legislative resolution and proposed amendments to the Commission's legislative text. Amendments may be proposed by the rapporteur and/or committee members, who may debate the issues and produce compromise amendments. Each committee discusses and votes on its own rapporteur's draft opinion, accepting or rejecting each of the suggested amendments.

[229] Committee on Civil Liberties, Justice and Home Affairs, European Parliament, 'Civil Liberties MEPs pave the way for stronger data protection in the EU' (*Europarl*, 21 October 2013) <http://www.europarl.europa.eu/news/en/news-room/content/20131021IPR22706/html/Civil-Liberties-MEPs-pave-the-way-for-stronger-data-protection-in-the-EU> accessed 25 February 2014.

[230] N 4.

[231] Or perhaps 11 Mar 2014 according to the procedure file (n 228).

[232] Council, 'Next European elections will take place from 22 to 25 May 2014' (*Consilium*, 14 June 2013) <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/genaff/137466.pdf>.

[233] European Parliament, 'European Parliament approves its session calendar for 2014' (*Europarl*, 12 June 2013) <http://www.europarl.europa.eu/news/en/news-room/content/20130610IPR11413/html/European-Parliament-approves-its-session-calendar-for-2014>.

[234] Rule 214, Rules of Procedure of the European Parliament <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+RULES-EP+20140203+RULE-214+DOC+XML+V0//EN&language=EN&navigationBar=YES>.

[235] Commission, 'About the European Commission' (*Commission*) <http://ec.europa.eu/about/index_en.htm> accessed 25 February 2014.

[236] Consolidated Version of the Treaty on European Union, OJ [2012] C326/13, Art 17(3).

[237] Consolidated Version of the Treaty on the Functioning of the European Union, OJ [2012] C326/47, Art 293(2).

6.4 Council

The Council has been considering the Commission Draft in parallel with Parliament. The subgroup of the Council dealing with these proposals is the Working Party on Data Protection or DAPIX (Data Protection and Information Exchange), chaired by the (6-month rotating) Council Presidency. Consideration of the proposals began under the Danish Presidency, and continued under the Cyprus, Irish and Lithuanian Presidencies. Greece holds the Presidency from January-June 2014.[238]

In January 2014 the Council released its first full public version of the draft Regulation (**Council Draft**), with proposed amendments that sought to take into account discussions in DAPIX under the Lithuanian Presidency. This represents the latest draft position on the Council front, but it is not the agreed text, and still includes numerous reservations on the part of Member States and/or the Commission – in particular, regarding the 'one-stop shop' principle, which has become an unexpected bone of contention, with the Council's legal service raising queries in December 2013 as to its compatibility with data subjects' fundamental right to an effective remedy.[239]

In Oct 2013 the Council had issued an aspirational statement to the effect that 'The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015'.[240] However, in December 2013 in the 3279th Council Meeting (Justice and Home Affairs) the Lithuanian Justice Minister stated, 'We prefer a strong agreement to a fast one, and must work to ensure a proper balance between business interests and fundamental rights of citizens.'[241] Rather than committing to ensure the Council Draft is finalised within the Council, the Hellenic Presidency has simply stated, 'In the field of Data Protection, the Greek Presidency has set as a main priority the systematic continuation of discussions on the legislative package of data protection. Taking under consideration the works of the European Parliament, the Presidency will seek progress on discussions aimed towards a political approach.'[242] Therefore it seems that, while wishing to make progress, implicitly Greece may be acknowledging that agreeing the Council Draft may not be possible by mid-2014, although Commissioner Reding is more positive about the timing.[243]

As mentioned previously, if Parliament and Council do not agree on a common legislative text, which now seems likely, negotiations on a compromise text will be necessary, and the matter may proceed to the Conciliation Committee under a new Parliament and new Commission, or amended reform proposals may even be made by the new Commission.

[238] Thereafter, the Council Presidency will rotate as follows, until 2017: Italy July-December 2014; Latvia January-June 2015; Luxembourg July-December 2015; Netherlands January-June 2016; Slovakia July-December 2016. Council Decision of 1 January 2007 determining the order in which the office of President of the Council shall be held [2007] OJ L1/11.

[239] Council, '3279th Council meeting Justice and Home Affairs 5-6 December 2013' 17342/13, 12 <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/139938.pdf>.

[240] European Council, 'European Council 24/25 October 2013 Conclusions' EUCO 169/13, 5 <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf#5>.

[241] Council (n 239).

[242] Hellenic Republic, 'Programme of the Hellenic Presidency of the Council of the European Union 1 January-30 June 2014', 27 <http://gr2014.eu/sites/default/files/PROGRAMME%28EN%2928012014.pdf> accessed 25 February 2014.

[243] Commission (n 18).