://Data Protection: the Future of Privacy

Rebecca Wong, Senior Lecturer in Law, Nottingham Law School[1]

Contents

INTRODUCTION

The Art. 29 Working Party (hereinafter "Art. 29 WP) is an influential body comprised of representatives from the Member State Data Protection Authorities[2] established under the Data Protection Directive 95/46/EC, has recently issued an opinion with the Working Party on Police and Justice. This is quite significant, since the opinion sets out some of the issues that will need to be addressed in the lead up to the revision of the Data Protection Directive 95/46/EC.[3] This comes at the a time, when there have been discussions on the current application of the European Data Protection Directive to the internet,[4] (such as social networking) and the recent European Commission's

1 Views expressed in the article are entirely the author's and does not represent the organisation. She can be reached at r.wong@ntu.ac.uk.

2 Kuner, C. *European Data Protection Law,* 2nd ed., p. 9

3 At the time of writing, the revision of the Data Protection Directive 95/46/EC has been postponed until November 2010. See Hunton and Williams Privacy Law Blog: *European Commission postpones revision of the Data Protection Directive* available at http://www.huntonprivacyblog.com/2010/08/articles/european-union-1/european-commission-postpones-revision-of-the-general-data-protection-directive/, dated 3rd August 2010.

4 See UK ICO. RAND: *Review of the European Data Protection* Directive available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf, dated May 2009 (examines the strengths and weaknesses of the European

consultation on the legal framework for the fundamental right to protection of personal data. Not least, there have been a number of cases brought before the European Court of Justice dealing with the partial implementation of the Data Protection Directive 95/46/EC.[5]

The aim of this paper is to consider in detail the issues set out by the Art. 29 WP and the likely challenges in revising the Data Protection Directive 95/46/EC.

ART. 29 WP OPINION ON THE FUTURE OF PRIVACY

The Art. 29 WP's opinion on the *Future of privacy*[6] is prescient since it deals with the very issues that are likely to be considered in the discussions surrounding the revision of the Data Protection Directive 95/46/EC.[7] This is a result of the recent consultation by the European Commission on the legal framework for the fundamental right to protection of personal data. The Art. 29 WP takes the view that the main principles of data protection are still valid despite new technologies and globalisation. In their view, "the level of data protection in the EU can benefit from a better application of the existing data protection principles in practice." Their primary focus has been on the:

- Clarification on the application of some key rules and principles of data protection
- Innovating the [data protection] framework by introducing additional principles (such as "privacy by design" and "accountability")
- Strengthening the effectiveness of the system by modernising arrangements in Directive 95/46/EC
- Including the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters.

Space does not permit a thorough analysis of all the issues considered in the Art. 29 WP Opinion, so the author will therefore focus on the salient points that deserve attention.

1: Framework of the Data Protection Directive 95/46/EC

In brief, the DPD was introduced under Art. 95 with the dual aim (under Art. 1 of the DPD) for EU Member States to ensure the free flow of personal data from one Member State to another, whilst at the same time, safeguarding the high level of protection of fundamental rights of individuals. This has been the subject of much discussion whether the DPD adopts a minimalist or maximalist approach

Data Protection Directive 95/46/EC); Art. 29 Working Party. *Press release regarding the review of the Data Protection Regulatory Framework* available at http://ec.europa.eu/justice/policies/privacy/news/docs/pr_15_07_10_en.pdf, dated 15 July 2010.

5 See C-518/07 *European Commission v Germany*, OJ C 37, 9.2.2008. available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

6 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, 01 December 2009, WP 168 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf, adopted on 1 December 2009.

7 See PRIVIREAL, Data Protection Directive 95/46/EC at http://www.privireal.org

to protection of personal data,[8] but will not be discussed here, as these issues have been addressed elsewhere.

The DPD is further complemented by Directive 2002/58/EC on Privacy and Electronic and Communications (DPEC) to the processing of personal data in the *electronic communications sector*[9] covering personal data processed by "publicly available" communications services.

The Art. 29 WP identified that there were shortcomings in the current framework particularly for the third pillar of the EU. More specifically, the lack of linkage of the data protection framework to the internal market. It should be remembered that the DPD was introduced under Art. 95 EC, which was the legal basis for adopting legal measures for internal market. The Art. 29 WP exemplified this by considering this in the light of Art. 8 of the Charter of Fundamental Rights of the EU. It should be added that data protection as a subject is now covered within the ambit of EU Freedom of Justice and Security, so there is some ambiguity whether DPD would fall within the category of internal market and whether it does matter that it falls under the remit of Freedom of Justice and Security section.[10]

There were other issues raised by the Art. 29 WP, which include the former division between the pillars that does not reflect the reality of data protection where personal data was used in cross pillar situations as exemplified by the PNR and Data Retention judgments of the ECJ.

In view of these shortcomings, the Art. 29 WP recommended a reflection on a "comprehensive and consistent data protection framework" to cover all areas of EU competence. It also notes the Lisbon Treaty, which is significant, since this will deal with the differences or divergences that exist under the current framework to provide a "seamless, consistent and effective protection of all individuals." It further reinforced the view that the safeguards and principles under the DPD should apply to data processing in all sectors and that the DPD should serve as a benchmark for the comprehensive framework.

Certain concepts under the DPD would therefore, need to be revisited for further clarification including consent (between opt-in and opt-out consent) and transparency (pre-condition to fair processing).

The proposals for a comprehensive framework should be welcomed, but the question arises is how these concerns can be easily achieved within the current timeframe (for revision of the DPD) and the extent to which Member States can be given the discretion (that they presently have with certain provisions such as Art. 9 of the DPD to exempt the processing of personal data on grounds of artistic,

---

8 See Thomas Hoeren. "The new German Data Protection Act and its compatibility with the European Data Protection Directive" (2009) *Computer Law and Security Report*, 25(4) 318-324 and PRIVIREAL, European Data Protection Directive 95/46/EC at http://www.privireal.org/content/dp/directivecommentary.php.

9 Recital 10 of the DPEC states that 'in the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, *which are not specifically covered by the provisions of this Directive*, including the obligations on the controller and the rights of individuals. Directive 95/46/EC *applies to non-public communications services.'* (emphasis added).

10 See European Commission: Justice, Freedom and Security at http://ec.europa.eu/justice/doc_centre/privacy/law/index_en.htm, dated 21 September 2010.

literary and journalistic purposes) to diverge or differ from the framework. Whether it would be possible for Member States to adopt a maximum or minimalist application of the DPD is not yet clear.[11] The Art. 29 WP did, however, express the view that there was room for flexibility and differences between the sectors and the Member States within the scope of the general protection, provided they fit within the notion of a comprehensive framework and comply with the main [data protection] principles.[12] To give an example, one Member State has already adopted legislation by using the existing exemptions under the DPD and their national data protection laws to amend their laws to adopt a misuse-orientated approach towards the processing of personal data as applied online (misuse rather than the processing model under the current data protection framework).[13] So far, no Member State (at least to the author's knowledge) has followed this model, but it is a clear example of how Member States can use the existing exemptions to diverge from the DPD where this is legally possible to adapt to their current scenario.

2: Current and present legal framework

The Art. 29 WP raised several points in relation to the current framework. The Art. 29 WP acknowledged that data protection was a fundamental right protected under Art. 8 of the Charter of Fundamental Rights of the EU and is a relevant point, since this was not necessarily recognised by other parts of the world.

The application of the DPD under Art. 4 is also an issue of relevance, since the Art. 29 WP was of the view that the Directive could apply to data processed outside the EU. However, Art. 4 of the DPD was complex and not sufficiently clear for multinational establishments. Furthermore, there were instances where the DPD was not applicable to non-EU established data controllers such as online websites. It is anticipated that an opinion is currently being drafted by the Art. 29 WP, so one awaits to see whether this will lead to further clarification in the application of data protection rules.

A few preliminary observations to be made on the application at this stage:

- The application of the DPD or national data protection laws to organisations/individuals, who "use" equipment within the EU would qualify as processing of personal data under Art. 4(1)(c).
- The need to identify where the "data controller(s)" was established for data protection rules to apply.
- Its application to social networking websites (if any) and whether SNS could opt-out of the data protection rules, through contractual terms set out on their website and whether this is legal under EU or national data protection rules.

3: Increasing Standards of the Madrid Resolution

The Madrid Resolution was adopted by the International Conference of Data Protection and Privacy Commissioners on 6 November 2009 with the aim of establishing a global standard for the protection

11 See Germany as an example. Cf with the UK's approach to Data Protection.

12 See Art. 29 WP Opinion, *The future of privacy*, op. cit. n. 5 p. 8

13 See P. Seipel, Sweden In: *Nordic data protection laws* (Copenhagen: DJOF, 2001), p. 123.

of personal data and privacy through legislation in the five continents. The Art. 29 WP urged the Commission to adopt "initiatives towards the further development of international global standards regarding the protection of personal data with a view to promote an international framework for data protection". Whilst the Madrid Resolution is the first step, it should be recognised that there are *cultural and national differences* in the understanding of privacy and the extent to which personal data should be protected and counterbalanced against factors such as national security, public health etc, which are already recognised under the current EU Data Protection framework.[14] Further education for organisations and individuals based outside the EU and recognition by relevant non-EU private sector organisations that process personal information (such as human resources; customer database etc) would go a long way.

4: Adequacy decisions

This is based on Art. 25 of the DPD which prohibits the transfer of personal information to non-EU countries without satisfying the adequacy standards laid down under Art. 25 and 26. To date, only a handful of countries including Switzerland, Canada, Isle of Man, Argentina and Guernsey have received recognition for the transfer of personal data from EU Member States.[15]

The Art. 29 WP has recommended the redesign of the adequacy process by defining the criteria for the legal status of "adequacy" more precisely and streamlining the procedures for the analysis of the legal regimes of third countries on the adequate level of protection.

A few notes of observation on this front is that it has been over 10 years since the Data Protection Directive 95/46/EC was adopted, yet third countries that do not satisfy the level of adequacy, would require more administrative burdens on the part of the organisation to safeguard privacy rights when dealing with the transfer of personal data from an EU country to a non-EU country. To the author's knowledge, there are at least two or three countries that have begun modelling their privacy laws to the EU (such as Hong Kong) but have yet to achieve the "adequacy status".

5: Privacy by Design Principle

The Art. 29 WP recognises the challenges facing data protection in the digital era, with Web 2.0 services and cloud computing blurring the lines between data controllers, data processors and data subjects. Thus, it has recommended that to strengthen the rights for individuals' privacy and data protection, the principle of "privacy by design" should be introduced under the new framework and as the need arises, for regulations to specific technological contexts. The privacy by design principle is not new, since the European Commission has always expressed the view that organisations should adopt privacy enhancing technologies. However, for an explicit provision on this would, according to the Art. 29 WP, bind technology designers and producers and data controllers when using ICT technologies, such that "privacy by default" would become the norm and not the exception. It can be argued that this is gradually (though slowly) happening with internet browsers set to ask for consent

[14] See E. Barendt (ed.) *Privacy*: *International library of essays in law and legal theory*, Vol. I (Aldershot: Ashgate/Dartmouth, 2000) on the concept of privacy; cf. D. Solove, *Understanding Privacy*, (Cambridge, Mass: Harvard University Press, 2009).

[15] See Commission decision on adequacy of the protection of personal data in third countries at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm, last accessed August 2010.

before cookies are installed onto the computer user's hard drive or the internet search engines such as Ixquick to delete any browsing data after 24 hours. Perhaps, a question is whether ubiquitous technology such as mobile phones which records the GPS location of individuals could be easily masked or behavioural ad programs embedded onto a website (likened to spyware which is prohibited under DPEC) and creating an individual's profile by monitoring the user's internet activities could be removed or easily made clear for users. The Art. 29 WP has identified that biometric identifiers, video surveillance were among the examples how privacy by design could contribute to a better data protection. These are some of the issues that arise and no doubt, there will be more technology issues that emerge which will pose a challenge for the existing data protection framework.

6: Data subjects rights

Empower the Data Subject

One of the issues highlighted was the need to "empower the data subject". The Art. 29 WP was of the view that the potential of the DPD (as implemented in the national data protection laws) was not fully used. Therefore, they recommended mechanisms for redress should be improved such that data subjects could easily bring a legal action for breach of their data protection rights. The possibility of class action procedures was suggested[16] within the Data Protection Directive 95/46/EC. This is an interesting development as the current provisions as implemented in the UK Data Protection Act 1998 are centred on individual rights rather than a class action for infringement of privacy. An apt example is Privacy International, which had contemplated of bringing a class action against the UK government for data security breaches.[17] Secondly, the Art. 29 WP also suggested that data controllers should provide for complaints procedures to resolve any disputes arising between the data subject and the data controller. This is not new and Data Protection Authorities such as UK ICO have been making themselves known through media channels to educate individuals about who to complain for (alleged) breaches of data protection.

Transparency

The Art. 29 WP emphasised the need for transparency in the collection of personal data prior to processing in the context of profiling, data mining. It suggested that individuals should be informed to improve transparency and notified in the event of a privacy breach including a privacy breach notification into the new legal framework. Data security breaches have been introduced in the Citizens Directive 2009/136/EC.[18] This is relevant with stories emerging of behavioural programs that collect individual's profile of their surfing habits and giving data subjects the right to know that information is collected about them through surreptitious techniques are necessary to protect an individual's privacy.

---

16 See para. 61 of the Art. 29 WP Opinion, *op. cit.* n. 5.

17 Privacy International to pursue data breach legal action against UK government at http://pi.gn.apc.org/article.shtml?cmd[347]=x-347-558703.

18 OJ L337/11, 18.12.2009 available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF

Consent

The Art. 29 WP suggested that the new legal framework should specifically require consent of individuals and recognised the limitations of giving a freely informed consent. Explicit consent (opt-in) for all processing will need to be differentiated from opt-out consent. However, in scenarios where the processing of personal data will be conditional upon giving consent such as a employer - employee contract or use of certain programs online, it is arguable that the need to obtain express consent is futile under those circumstances. Therefore, the question is whether consent given can be revocable or withdrawn or consent given for one purpose will not be used for another purpose with the right of the data subject to express the conditions under which his/her consent is given.

Harmonisation

The Art. 29 WP noted that there were differences in the implementation of the Data Protection Directive 95/46/EC by Member States including liability provisions and the possibility to claim immaterial damages.[19] Furthermore, there have been differences in the interpretation of the DPD. Further harmonisation was recommended through legislation to remedy this. A few preliminary observations on this point – the interpretation of certain concepts have not been uniformly applied by national courts such as "personal data"; application of exemptions under Art. 3.2 and Art. 9 of the Data Protection Directive are some examples which have been the subject of interpretation by the European Court of Justice.[20]

Data subjects on the internet

It is interesting to find that the Art. 29 WP was of the view that DPD was not applicable to individuals who post their data for "purely personal" purposes or "in the course of a household activity", but also notes that there was a significant lack of safeguards for individuals who voluntary post personal data in the context of social networking, cloud computing etc. The Art. 29 WP has recommended that the role of the data subject on the internet should be clarified. This is significant, since this will discuss the application of the framework to new technologies and the extent to which data subjects can be protected in the event of misuse of their personal information through the use of social networking etc.

7: Data controller's responsibility

The Data Protection Directive places responsibilities on data controllers to comply with the DPD (or national data protection laws) and the Art. 29 WP is currently in the process of drafting an opinion on the concept of data controller and processor. The Art. 29 WP suggests that privacy should be embedded into information processing technologies and systems. According to Art. 29 WP, data

[19] Art. 29 WP Opinion, *op. cit.* n. 5, p. 17.

[20] See C-101/01 *Lindqvist* [2004] 1 C.M.L.R. 20; C-465/00 *Rechnungshof v Österreichischer Rundfunk and Others* [2003] ECR I-4989 and C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and another* [2010] All ER (EC) 213.

controllers should be proactive in at least the following: adopting internal policies and process to implement the requirements of the DPD; put in place mechanisms executing the internal policies and processes; draft compliance reports and carry out audits; carry out privacy impact assessments; assign responsibility for data protection to designated persons. Furthermore, it suggested an accountability principle to be introduced under the new framework making data controllers more accountable for their actions and simplify the notification processes by national Data Protection Authorities. The role of data controllers has been considered quite in-depth by the Art. 29 WP, particularly how the current process could be improved. It does not recommend, however, revising the terminology used in the Data Protection framework for data controller and data subject relationship in the context of Web 2.0 technologies or cloud computing, but rather, to continue using the "data controller – data subject" dichotomy and enhancing their responsibilities, which appears by some to be outmoded in Web 2.0 technologies. Furthermore, it is arguable whether the measures to enhance the data controller's responsibilities have not been achieved by the larger companies, such as Microsoft whereas the smaller (SME) companies need to more training, education and awareness of their knowledge of the data protection framework. It remains to be seen how these measures will be applied by organisations.

8. Data Protection Authorities

The Art. 29 WP recognised that there were big differences in the position of the DPAs in the 27 Member States due to the history, case law, culture and the internal organisation of the Member States. Thus, it has recommended for a clearer role for DPAs. It also criticised the lack of precision of the DPD, which has been poorly implemented in some jurisdictions. It therefore suggested a stronger supervision by DPAs and the following issues should be addressed:

- The need for a fully and independent DPAs (Art. 28.1 of the DPD)
- Enforcement role of the DPAs to be stronger to enable DPAs to impose financial sanctions on data controllers and processors (Art. 28 of the DPD)
- Advisory role of the DPAs to become an essential part to improve (data protection) legislation
- DPAs should to be able to decide on their own agendas when setting priorities such as handling complaints
- A transparent role of the DPAs in the way they operate and the priorities they set. (Art. 28.5 of the DPD).

9. Art. 29 Working Party

The role of the Art. 29 WP (Art. 30 of the DPD) was also considered with several points raised:

- Art. 29 WP's effective contribution to the uniform implementation of EU law and the uniform application of national law.
- Art. 29 WP's effectiveness vis-à-vis the EU institutions such as the Commission

It recognised that there was no need for further legislative changes in the uniformed application of national law implementing the DPD, which, according to the view of the Art. 29 WP, could be achieved within the present legal framework.

There were other issues in relation to the field of police and law enforcement which (given the scope of this paper) will not be considered here.

Concluding Remarks

With impending proposals to revise the Data Protection Framework, which was long overdue and is likely to take place in Autumn 2010, the Art. 29 Paper on the *Future of Privacy* reinforces the relevance and present shortcomings of the DPD. It is one step in the right direction in underlining the global role the DPD plays on the one hand in the protection of fundamental rights including privacy and on the other hand, the free flow of personal data. The DPD is over 10 years and revising the Directive is the beginning. Recognising how the DPD can be applied effectively to Web 2.0, cloud computing and identity management systems are also necessary.

Furthermore, steps to harmonise and streamline guidance from the Art. 29 WP and the DPA to deal with the coherency of the framework including interpretation of different concepts and/or principles (such as Art. 3.2 of the DPD) so that the Data Protection framework is not applied rigidly and that there is scope for discretion or manoeuvre by Member States and flexibility for DPAs to apply the DPD effectively. It will be watched with much anticipation to see how far the DPD will be revised and whether it can address the shortcomings outlined in the European Commission's public consultation and the Art. 29 WP future of privacy. Much work is still needed and the time is ripe to reconsider the future of privacy!