Summary Report of EURIM Data Protection Group meeting, Thursday 22nd March 2012, 1030-1230, Symantec Offices, 88 Wood Street, London

Chair: Sue Daley (Symantec); Rapporteur: Dave Wright (EURIM)
N.B. the report should be read in association with the accompanying slide presentation

SUMMARY OF MAIN POINTS

1. The Data Protection Group will focus on the scrutiny of selected proposals in the draft Regulation (as set out in Communication COM (2012) 9 final) that sets out a general EU legislative framework for personal data protection, rather than the draft Directive, which is concerned with law enforcement around the processing of personal data.

2. There is a need to update data protection law, to fix obvious problems and help make a reality of the single market as an attractive place in which to locate and do business. Most of the concerns expressed by the Group relate to ambiguities and lack of clarity and consistency in definitions, including of personal data, leading to different interpretations with the risk that these can only be resolved in the courts. Lack of clarity also means the cost of compliance cannot be known with any certainty. This could not only get in the way of the further development of a Digital Single Market but could increase the incentive to organisations which wish to sell across national borders to base the operations involved outside the reach of the directives.

3. An early action will be to distil and synthesise key concerns from members' responses to the UK Ministry of Justice call for evidence on the likely impact of the EC's proposals on organisations that process personal data and benefits to individuals through strengthened rights.

4. The Group will explore opportunities for further joint work with the European Internet Foundation (with which EURIM has a Memorandum of Understanding) and others, in order to outreach and build alliances, collate evidence and opinion, and maximise engagement with interested parties, including MEPs.

5. The EU Parliament has only just announced its rapporteurs for the relevant committees, and we are only at the beginning of what is expected to be a long debate. The Group meeting is therefore timely for identifying members' initial key concerns with the proposed Regulation and making representations, where appropriate, jointly with the EIF.

6. Recent announcements from the EC may not accord with other interpretations, e.g. where cloud computing is involved. There was concern that where clarity is lacking, the cost of regulatory confusion may encourage cloud service providers to locate their servers outside the EU. It was suggested that it is perhaps doubtful that any company making services available to EU citizens from the US or Asia would be caught by EU law, as the draft regulation suggests.

7. Conflicting or simply differing interpretations make giving advice difficult but a common understanding of what is defined is necessary in order to assess the impact on organisations.

8. Another major concern is the assumption that the issues of identity governance will be handled by the Commission, because this is an area of similar confusion.

9. Key actions are to produce a draft confirming the core issues identified by the Group, and following these up with EIF members with regard to their priorities, timetable and the alignment of interests.

1 Introduction

1.1 Sue Daley opened the meeting, and explained that the reason for this meeting was traceable back to the joint EURIM - European Internet Foundation (www.eifonline.org) meeting on 23rd January chaired by Malcolm Harbour MEP, on driving the Digital Single Market (DSM). A major need was for joined-up scrutiny of legislative and regulatory proposals coming from the EU, to ensure clarity and the removal of conflicts and barriers to economic growth.

1.2 A major objective at that meeting was to look at jointly producing agreed recommendations on policy priorities, from both UK and European perspectives. One of the key issues identified for joined-up scrutiny was the proposed reform by the EC of EU data protection regulations - a 'hot topic' in Brussels.

1.3 The main purpose of this meeting is to have an initial discussion of the proposals to identify issues of concern to members.

1.4 SD invited those present to introduce themselves.

2. Presentation on Data Protection – Sue Daley

2.1 New legislative proposals for data protection were published by the European Commission on 25 January 2012, developed from earlier working documents (Slides 1-5). The proposals consist of a draft Regulation setting out a general EU legislative framework for personal data protection and a draft Directive around law enforcement on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

The draft Regulation will repeal and replace the 1995 Data Protection Directive, which is implemented into UK law by the Data Protection Act 1998. The draft Directive will repeal and replace the existing Data Protection Framework Decision, which was negotiated in 2008 (Slide 6).

2.2 The UK Ministry of Justice issued a call for evidence on 7 February 2012, which ended after a relatively short period on 6 March 2012. The call invited comments on the likely impact of the EC's proposals on organisations processing personal data, as well as the likely benefits to individuals through strengthened rights.

2.3 It was suggested that this Group should focus on the draft Regulation, since this was most relevant to member companies and the UK economy generally. Of the 91 Articles contained in the proposed Regulation, a selection of 12 was considered to be most relevant to the Group membership (Slide 7). This includes changes to the definition of personal data, explicit consent, and data portability. Some of the proposals had been welcomed, such as harmonisation of applicable law across all EU Member States, but others had raised much debate.

2.4 A main aim of the meeting was to identify key areas of concern to EURIM members, and to decide how we might invite feedback and input on the likely impact of the proposals in the UK. We should therefore discuss the scope and terms of reference for the Group's work, how this might link with the EIF, and the potential opportunities for joint meetings, work and briefings with the EIF in Brussels (Slide 8).

3. Discussion - Key areas of concern for EURIM members in the EC proposals

3.1 Many interpretations of aspects of the proposals are available that do not match, with some poor definitions, some verging on unintelligible including 'personal data' and 'storage', and others inconsistent (i.e. different definitions used in different sections). This makes giving advice very difficult. Trying to get a common understanding of what is defined is important for assessing the impact on organisations. There is particular concern by some at the assumption that issues of identity governance would be handled by the Commission, because this is an area of similar confusion, and raises fears that the Commission may be empowered to consult and just declare an answer.

3.2 There was some discussion over whether some of the ambiguities were deliberate, or whether inconsistencies had accumulated over time that could be traced to issues that were of particular concern to a specific party. In attempting to get a detailed analysis of an issue, given the confusion in the proposal, a workable approach might be to begin with a statement of how an issue is interpreted at

present, which could then be put as a question or a basis for discussion. This might reveal what was intended.

3.3 Some discussion was held on the comments of Commissioner Viviane Reding who was quoted as saying that certain ambiguities are necessary, the feeling being that these comments were probably in recognition of the fact that the only way that any single piece of legislation could be acceptable across the board is to allow for different views. Some problems do not have obvious solutions, and this will perpetuate current difficulties with interpretations. The ICO has a detailed paper on this.

3.4 This will be a long game and we are only at the beginning of the debate; the EU Parliament has only just announced its rapporteurs for the relevant committees. We should be able to learn more from the MoJ call for evidence as the information is evaluated and a response formulated. This meeting is therefore timely for identifying members' key concerns and making representations, and where appropriate, jointly with the EIF.

3.5 It was suggested that we should ask the EU if it is content that the ambiguities present are sufficiently fundamental or necessary to run the risk that organisations which find the consequences (including regulatory and legal uncertainty) expensive and impractical, may well keep or relocate their customer service or transaction processing operations (and the associated call centres and databases) outside the EU single market. Such prioritisation may be helpful in forcing clarity on the debate. Preserving 'necessary' ambiguities actually infers that these are more important than a single market.

3.6 Ambiguities tend to lead to court cases, and the European Court of Justice would then act as legislator – which we should try to avoid. SMEs in particular want clarity and certainty. While some of the proposals are welcome, some of the new areas of legislation – e.g. the right to be forgotten, privacy by design, heavy sanctions – will take time to understand.

3.7 The short time period allowed for responses to the MoJ's call for evidence meant that an accurate estimate of cost implications of the proposals has not been possible. But an accurate assessment does need to be done.

3.8 At least one response to the MoJ did mention questions on the cost of compliance; this issue is extremely important because the proposal suggests that there are administrative burdens that should be lifted. One initial assessment is that there will be a substantial cost to compliance, e.g. for privacy by design. However, it was suggested that privacy by design should be considered in the same way as technology or end-user requirements and as a process that should be part of designing a system – it should not be particularly onerous for new systems. That raised concerns over the effect on existing systems and the impact that the proposals could have on the technology neutrality of the current legal framework.

3.9 Principles are not really the issue – the problem is that the regulation lacks clarity, and therefore the cost of compliance cannot be known with any certainty, and will delay an organisation's decision-making. It is especially difficult for SMEs which often lack the skills necessary to come to terms with the proposals. It was pointed out that the type of organisation that the EC is trying to target is where a business relies on collecting and using data but has not taken privacy into account. Other organisations then become targets by default. However, this offers an opportunity to look at standards and what is permissible from the SME perspective.

3.10 Mandating privacy by design by some kind of manual (with rules, processes and standards) might be counterproductive from a regulator's point of view. The recommendation on Privacy by Design is seen as good in concept and could be useful for ensuring data protection and privacy issues are dealt with as part of the process of developing systems, and not as an add on at the end of a project. But there were concerns that to mandate technologically specific terms and conditions could impact the technology neutrality of the legal framework and this would not be welcomed. Without clarity or definitions, or even an understanding of the changes necessary from the existing position and any guidance on how to achieve this, it was seen as a recipe for confusion.

3.11 It was suggested that setting targets would be a better approach than detailed mandation, which is likely to lead to conflicts between data controllers, bureaucratic confusion and court cases, rather than realise the stated vision for the citizen. Overall the point was made that data protection should be held as an enabler of the Digital Single Market, rather than a barrier.

3.12 Explicit consent is another concern, particularly for Internet-based businesses which might find obtaining this from users to be practically impossible because of the number of user-responses needed, which could stifle innovation. This is especially true for large businesses where there is an inability to get consent in an unequal relationship between the data controller and the data subject. This imposes a massive administrative cost burden when interpreting how personal data is handled, and for staff training. Having a clear distinction of where responsibility and liability lie facilitates compliance, and is a good enabler of business. There is a need to demonstrate compliance, though onerous in some respects, but we need to avoid lack of clarity and the legal and contractual wrangling over the liability and responsibility issues that would then ensue.

3.13 Compliance in practice is about meeting standards and implementing data protection, information security, regulatory standards etc., but a data processor cannot say 'this is the solution' unless there is clear information and guidance, including on who is responsible for what.

3.14 Recent announcements from the EC may not accord with other interpretations, e.g. where cloud computing is involved. This raises a kaleidoscope of issues, and where clarity is lacking, the cost of regulatory confusion could encourage cloud service providers to locate their servers outside the EU. It was doubtful that any company making services available to EU citizens from the US or Asia would be caught by EU law, as the draft regulation suggests. It appears to give false assurances to citizens by suggesting that policing is possible where in fact it may not be enforceable in practice. Two proposals are involved here – the extension of EU law outside the EU and the role of DPAs.

3.15 This Group can highlight such problems, and propose recommendations to introduce clarity, consistency and workability. Cloud computing is a key enabler to the Digital Single Market, so we should be looking for opportunities and whatever enables the cloud to grow in Europe, rather than erecting barriers. This may involve new and innovative business models.

3.16 Once data is secure and access is appropriately restricted, the location of data processing and other operations is incidental. We therefore need to move from a Eurocentric to a global view. The proposal to extend EU law beyond Europe may deter organisations from moving operations abroad – because they would still be caught. However, it does make a big difference depending on the kind of data – most suppliers do not hold any personal data, though this depends on the actual definition of personal data, which according to some interpretations could be wider than currently held.

3.18 A key issue for discussion was the revised definition of personal data. It was discussed that the new definition could mean that once you accept a definition that includes taking your online search records as part of your footprint, for example to authenticate that transactions really do originate from you, your footprint may be considered as personal data. These changing and vague definitions raise a whole raft of issues including at the political level.

3.19 The issue was raised of software that can be purchased which can be used in a way that breaches the DPA; however, this is a problem for the purchaser/user, not the software designer. The Internet Advertising Bureau had claimed at a recent meeting that the proposed definition of personal data, combined with the requirements for explicit consent, would undermine a whole industry.

3.20 It was suggested that if all information is personal data, including an online identifier like a cookie or IP address, the rules of explicit consent will apply. This raises questions of the legality of identifying e.g. spammers – and although exemptions exist in the case of law enforcement, national security etc., this is not stated in the proposal. Does an exemption for law enforcement include civil actions? There is also an issue about the difference between consent and choice.

3.21 Concern was expressed about the ability of organisations to move data handling operations around the globe according to costs; the proposal to extend EU law and mandate privacy by design may give enhanced rights and protection to the individual. However, more clarity is needed on the issues of consent and profiling, with a balance between the interests of the consumer and business,

so that businesses can continue to innovate and offer personalised services to their customers. The choice of consent regime is important.

3.22 A useful approach would be to evaluate the effect of the proposed measures on advancing the Digital Single Market. This would mean evaluating ***each*** of the proposals against how these would, or would not, advance the Single Market.

3.23 Discussion then focused on the work this Group could be doing, including how we should outreach and engage with others. Notwithstanding the compliance-cost to business, how we regulate data handling is the key to enabling and driving the Digital Single Market and making the EU a good place to do business. Any EURIM paper or message should therefore not emphasise the negative points, but focus on recommending how the regulation of data protection can best serve both the interests of business and the consumer, and also act as an enabler and driver of the Digital Single Market.

3.24 The background to many of the issues was more complex than stated, e.g. in the field of mobile technology. Might identifying the circumstances which led to the drafting of regulations to address specific problems be a useful exercise? For example, some devices were designed to gather as much data as possible, but these were extreme cases and the rules proposed to address these are not necessary for the majority of situations.

3.25 The political process will begin soon, and what we have here is probably the best we will get, given the Parliamentary process which may not be particularly favourable to business objections. The Digital Single Market is not just a UK phenomenon. We need a supportive approach in combination if possible with the EIF, treating it as a political campaign, and pointing out that legal uncertainty is potentially damaging and that the proposals could benefit from clarification in key areas. We need to find allies beyond Brussels to build further momentum, though we need to limit the number of issues we address so as to maximise impact.

3.26 If we can produce a piece of work that promotes jobs and growth, possibly distilling information from members' submissions to the MoJ call for evidence, we can reach an EU audience. It is understood that the MoJ plans to publish responses in June for those who were happy for their submissions to be made public. We could combine essential information on key topics with the discussion at this meeting in an agreed short draft which could form the basis of discussion at the next Group meeting, referencing other documents/organisations as appropriate. Dave Wright undertook to contact Ollie Simpson at the MoJ regarding availability of submissions on its website.

3.27 We should also approach the EIF for an understanding of their thinking on the issues, and their plans. The EU Parliament is a key target audience for the EIF, and should be for us if we want to influence thinking in Brussels. The EU Parliament has just announced the leaders of key committees, which have yet to start work. We therefore are likely to have some time to develop our thoughts, concerns and recommendations.

3.28 It was suggested that EURIM could work with Intellect on joint exercises for the technology sector; however this needed to be explored further with Intellect. It is also an EIF objective to have better co-operation with groups representing financial services, and a meeting in co-operation with UK Payments is being planned on payment issues.

3.29 There was general agreement that there is a need to update data protection law, but also to approach the new Regulation in a positive spirit and use this opportunity to fix some obvious problems - e.g. what 'identified' means - and to make sure the new Regulation delivers the best benefits to citizens and businesses. An initial analysis by the ICO of the Regulation by the ICO can be found at http://www.ico.gov.uk/news/~/media/documents/library/Data_Protection/Research_and_reports/ico_initial_analysis_of_revised_eu_dp_legislative_proposals.ashx

4 Terms of Reference

4.1 The discussion had shown that EURIM members could make a positive contribution to the debate on the regulatory environment around data protection, in particular in association with the EIF and potentially others. In setting the Terms of Reference, there are 2 core elements of activity:

- confirming the core issues identified by the Group at this meeting, in association with responses to the MoJ call for evidence, as the basis for the next meeting and identifying the target audience for, and the timing of, our output(s). SD would produce a draft on this;

- following up with the EIF on their priorities and timetable, and determining how we can align with them. This might beneficially involve organising a joint messaging event in Brussels, to which MEPs are invited. SD confirmed that she would be happy to drive this supported by the EURIM team. SD also agreed to discuss further the possibility of an association with Intellect on data protection issues going forward.

4.2 It was suggested that we contribute input on citizens' rights, in particular on the right to be forgotten, access and the degree of user control. Malcolm Harbour MEP has this as an agenda item; he would like to see industry input after consultation with citizen and consumer advocacy groups like Citizens Advice. This should avoid open confrontation when the issues are discussed in Brussels. However, prior to consultation with other groups, we need to decide what is the EURIM core message that we want to deliver before reaching out to these groups.

4.3 Members who had submitted responses to the MoJ were invited to send copies to DW for collation and the team would then work on these to produce a draft synthesis; in the meantime if members became aware of new developments they should email SD, copy to DW.

5 Date of Next Meeting

5.1 The date of the next meeting would be planned for 2-3 weeks after Easter.