COUNCIL OF THE EUROPEAN UNION

Brussels, 6 March 2013

7106/13

Interinstitutional File: 2012/0011 (COD)

LIMITE

DATAPROTECT 29
JAI 183
MI 171
DRS 43
DAPIX 50
FREMP 25
COMIX 142
CODEC 477

NOTE

from:	UK Delegation
to:	Council
No. Cion prop.:	5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219
Subject:	The Proposed General Data Protection Regulation and the Impact of Small and Medium-Sized Companies

Delegations find attached a letter by Chris Grayling, Lord Chancellor and Secretary of State for Justice of the United Kingdom to Vice-President Reding of the Commission on the above topic.

I am writing further to our meeting on 13 February 2013 and, in particular, our discussion on the proposed General Data Protection Regulation.

You will recall that we discussed the cost impact that the proposed Regulation would have on Small and Medium-sized Enterprises. As a result of our conversation, you invited me to send you suggestions on specific articles where the Regulation should not apply to small businesses that do not operate cross-border, and therefore would not gain any benefit from harmonised rules. I am pleased to enclose a short paper which identifies areas where costs could be reduced for UK SMEs in that context. I will also be sharing this paper with other Member State delegations for their information.

By way of background, I would like to remind you that our Impact Analysis, which we published in November 2012, concluded that the Regulation in its current form would have a net cost to the UK SME sector of £80-£290 million (€100-£340 million) per annum (see Annex B of the UK's main Impact Assessment). We have been informed by many stakeholders that the UK impact assessment provides a credible evaluation of the cost of this Regulation.

Although Data Protection Officers were excluded from administrative burden calculations in the Commission's Impact Assessment, the designation of a DPO would be a cost burden that many SMEs would need to bear. That is why we have included all compliance costs in our calculations and also why we need to continue to work on the risk-based approach that the UK has supported. The attached paper highlights where we think costs on SMEs can be reduced. These areas include; data protection officers, subject access requests (right of access for the data subject), data protection impact assessments, documentation, notification of data breaches and administrative sanctions. All these areas need further consideration in order to minimise the cost burdens on SMEs.

In my view, any imposition of increased red tape on businesses will result in extra cost burdens for SMEs in particular and I am concerned that the proposed Regulation will obstruct rather than promote growth in the economy. The Commission has argued that the Regulation will help build individuals' trust in emerging businesses, particularly online, which in turn will be a key driver for business growth. However, we have already shown that we can encourage growth the digital economy. Indeed, it is no accident that the UK is a leading digital economy with a higher proportion of GDP (8.3%) in this sector than Europe and the G-20[1]. It is important therefore that the UK and the EU as a whole can preserve growth rates in this area but I am concerned that the Regulation could put this at risk as our Impact Assessment has set out.

On a separate point, recent discussions in the Council on the need for flexibility for member states have resulted from the choice of a Regulation for the new data protection framework. However, with the Directive for the criminal justice sphere coming in alongside the Regulation, many controllers will need to conduct an analysis of which instrument applies where. We may therefore end up with a fragmented system and a lack of interoperability between the two instruments which could lead to confusion at domestic level, particularly amongst citizens who will be less certain about how the law would apply to them in particular contexts. Changing to a Directive would instead deal with the fragmentation and complexity that a Regulation will cause as it would give Member States sufficient flexibility to implement rules that reflect their own traditions and practice, whilst also allowing for a coherent domestic legal framework as is the case under the current Directive.

I hope you find the attached paper on SMEs useful and my officials would be happy to engage in further discussion with Commission officials on the points raised. In the meantime, I look forward to continued constructive discussions on this very important dossier.

[1] Analysis by the Boston Consulting Group (2012).

Draft General Data Protection Regulation: Costs to Small Business

The UK Impact Assessment estimated that the draft Regulation could cost UK SMEs between £80 million and £290 million per annum (€100-€340 million)[1]. This paper identifies areas where these costs could be reduced for SMEs that do not operate outside of the UK.

UK Impact Assessment analysis

Table 1 gives the costs and benefits to UK SMEs monetised in the UK Impact Assessment[2]. It shows that the most costly parts of the Regulation are to the 42,000 UK SMEs that are not exempt from the requirement to employ a Data Protection Officer, or whose processing operations are such they will be required to carry out Data Protection Impact Assessments (DPIAs). If these articles could be more clearly defined and where applicable the SME exemption widened, this could significantly reduce the cost to business.

1 An exchange rate of £1 = €1.16 has been used through the paper.
2 UK Impact Assessment on the draft regulation (Annex B).

Table 1: Annual monetised costs and benefits to small business; £millions, 2013-13 earnings terms

	Small Businesses		
	Low	**Central (best)**	**High**
Benefits			
Reduction in data breaches	£30	£50	£70
No Notification	£10	£10	£10
Total Benefit	**£40 (€50)**	**£60 (€70)**	**£80 (€90)**
Costs			
Notifying breaches	£20	£40	£50
SAR Requests	£10	£20	£30
DPIAs	£50	£60	£70
DPOs	£30	£110	£180
Demonstrating Compliance	£10	£10	£30
Total Cost	**£130 (€150)**	**£240 (€280)**	**£370 (€430)**
Net Benefit	**-£80 (€100)**	**-£180 (€210)**	**-£290 (€340)**

Note: figures have been rounded to the nearest £10million / €10 million.

There are a number of other costs to small businesses which it has not been possible to monetise, but which are described in the Impact Assessment. These include the cost of administrative sanctions, the cost of consent being made explicit and the cost of providing detailed information to the data subject.

It should be noted that one of the benefits of the Regulation cited by the European Commission is a reduction in legal fragmentation. This reduces the cost of doing business for organisations that have to comply with the data law of multiple member states. However, a reduction in legal fragmentation is less likely to benefit small organisations because they are far less likely to process data in more than one Member State. For example, 17% of large retailers have a retail outlet or subsidiary in at least four other member states, compared with 3% of organisations employing between 10-49 people. Small organisations are therefore less likely to benefit from harmonisation.

Reducing the burden to SMEs

The following areas of the Regulation have been identified as areas where the cost to small businesses that do no operate cross-border could be reduced.

1. Documentation, DPIAs and DPOs (articles 28, 33 and 35)

The UK Impact Assessment identified 42,000 UK SME and micro businesses that would be not be covered by the SME exemptions in the current Regulation. To reduce the cost to SMEs that do not operate cross-border, the Regulation should make it clear that the requirement to employ a DPO, carry out a DPIA (unless a high risk is identified) and maintain documentation of all processing is non-mandatory for SMEs in the following business sectors that are captured by the current drafting:

- Market research and polling organisations
- Employment agencies
- The healthcare profession
- The financial sector (including pensions and insurance)
- Businesses providing security and investigation services

The UK would also support an overall reduction in the amount of documentation that must be held. The requirement to maintain documentation of all processing activities has been identified as a particular burden that should be removed from the Regulation. We consider that the Irish Presidency has made a good start in this area by proposing the deletion of some documentation requirements. However, under the Commission's proposal, data controllers would be required to document all processing operations irrespective of the nature of the processing or the volume of personal data processed. We consider that data controllers should have a greater degree of flexibility in determining the measures they adopt in order to ensure compliance with the proposed Regulation but guidance from supervisory authorities may also be helpful in setting out documentation requirements.

The existence of compulsory data protection impact assessments is potentially extremely burdensome for micro and SMEs whose processing is such that they will be required to carry these out (£50m-£70m (€60-€80m) per year in the UK). We consider that there are a range of options open to controllers in mitigating risk and DPIAs are one of these options. Where it is appropriate to conduct a data protection impact assessment however, this should make reference to the risks identified and the appropriate compliance mechanisms that the controller has or will put in place.

The UK believes that the obligation to designate a Data Protection Officer (DPO) should not be mandatory and there are a range of options for controllers to ensure compliance with the proposed Regulation. We also do not think that the tasks of the DPO should be set out in the Regulation. Under the Regulation as drafted, a Data Protection Officer could cost SMEs anywhere between £30-£180m (€30-€210m) per year in the UK, depending upon whether 4 hours of legal work is sufficient to fulfil the requirements of the Regulation. We therefore consider that guidance for data controllers may be more helpful in this context.

2. Notification of data protection breaches (article 31)

In the UK, 11% of small organisations have at least one personal data security breach a year[1]. The UK Impact Assessment estimated that the cost of reporting a breach to small businesses would be between £1,100 and £3,000 (€1,300 - €3,500). Making the reporting of data security breaches non-mandatory for SMEs that do not operate cross-border would lower the cost to business of this article. There should be a greater emphasis on assessing risk of harm from the breach and mitigating it rather being subject to prescriptive reporting requirements.

The UK would also favour an overall reduction in the burden of this article for organisations that are still required to notify. In response to the UK's Call for Evidence, a number of businesses stated that it took more than 24 hours to investigate a breach and collate the necessary information to give to the Commissioner; one organisation representing retailers estimated that it can take several days or weeks to conclude the preliminary investigation. The UK is therefore advocating that the requirement to notify "within 24 hours" be changed to "without undue delay" and that the level of prescription on the information that the Commissioner must be provided with, be reduced.

[1] PWC (2012), 'Information security breaches survey: technical report'.

3. Right of access for the data subject: Subject Access Request (SAR) Fee (article 12)

Removing the £10 fee for a SAR is anticipated to lead to a rise in requests of between 25% and 40%. The cost of these requests to UK SMEs is estimated at between £10 million and 30 million per annum (€10 - €40 million). Retaining the £10 fee for SARs would therefore lighten the burden to SMEs not operating across the border.

4. Administrative Sanctions (article 79)

The Federation of Small Business has identified the fines in the Regulation as significant sums of money to a small business that could force some of them to close[1]. In addition, the high fines are expected to lead to data controllers spending more than is necessary on data protection at the expense of other areas. Reducing the sanctions in the Regulation to SMEs that do not operate cross border would therefore ease the burden of the Regulation.

5. Other administrative burdens (articles 7, 11, 14, 15 and 34)

The prescriptive nature of the Regulation means that micro and small businesses will need to seek legal advice to ensure they are compliant. In a discussion with small UK technology companies, the companies all stated that they would need to employ external consultants to be assured of full compliance. The widespread reliance on delegated and implementing acts in the Regulation also creates greater legal uncertainty which would make it more difficult for SMEs in particular to plan their business. Guidance from supervisory authorities or industry certificates and codes of conduct can help alleviate these burdens, for example tailoring measures to the sectors or industries concerned whilst being more responsive to future technical developments.

[1] Federation of Small Business response to the UK Call for Evidence.

The following articles have been identified as areas that are particularly burdensome to SMEs and where easing the level of prescription would lower the cost of the Regulation to small businesses not operating cross-border:

- **Information to the data subject and rights of access for the data subject (articles 14 and 15):** narrowing the scope of these articles would reduce the burden on business. It is not possible for data controllers to specify how long the data will be stored and so this should be removed for all controllers. The delegated acts allowing the Commission to specify criteria should also be dropped.

- **Prior 'authorisation and consultation' for processing (article 34):** the requirement to consult the supervisory authority before the processing of personal data in specific circumstances is an unnecessary burden on business which the UK would like to be removed the Regulation, particularly for SMEs not processing outside of the UK.

- **Explicit consent (article 4):** the higher threshold for consent will be costly to business and the UK would support an easing of this standard, particularly for SMEs.

- **Transparent information and communication (article 11):** This article will have costs to controllers due to the requirement to ensure that transparent policies are in place. In particular the requirement to adapt the format to the data subject is likely to be particularly burdensome for small controllers and the UK would like to see this removed, particularly for SMEs.