Proposed EU data protection Regulation

What do people think?

June 2012

www.allencovery.com
Introduction

Significant changes to data protection legislation in the EU are approaching. On 25 January, the Commission released proposed draft amendments to the European data protection framework. The draft amendments take the form of a Regulation which will replace the current Directive (95/46/EC) and will be directly applicable in all member states without the need for national implementing legislation. Alongside this will be a Directive which sets out rules, among other things, on protecting personal data processed to prevent, investigate or prosecute criminal offences.

Adoption of the legislation is expected in 2013, and whilst the proposed Regulation will take some time to become law (two years after adoption), we expect that organisations will start to move towards compliance in advance.

If the proposed Regulation remains materially intact through the legislative process, the impact on organisations both within and outside the EU will be substantial. Fines that can be issued by supervisory authorities will be increased dramatically (proposed to be set at up to 2% of annual worldwide turnover) and companies will need to adapt their processes to deal with concepts such as the right to be forgotten and mandatory breach notification. Data protection compliance will certainly be higher on organisations’ agendas.

We carried out a survey to find out what our clients and other contacts think about the proposed changes to the law and the impact of these changes on their organisation. In the survey we focussed on the proposed Regulation. This note presents the statistical findings of our survey and includes interesting comments made by respondents to the survey, other clients of Allen & Overy, the Commission, various regulators and associations and some thoughts from us.
Overview of the results

KEY

BBA means the AFME/BBA response letter to the MoJ consultation dated 6 March 2012
CBI means the CBI response to the MoJ consultation dated February 2012 “Data Protection in the EU: The case for a re-think”
Client indicates a point of view provided by a client of A&O who did not respond to the A&O survey
Dutch DPA means the Dutch Data Protection Authority
EDPS means the European Data Protection Supervisor (Peter Hustinx) in his Opinion on the data protection reform package dated 7 March 2012
ICO means a quote taken from the ICO’s initial analysis of the European Commission’s proposals for a revised data protection legislative framework dated 27 February 2012
Italian DPA means quotes from Mr. Francesco Pizzetti of the Italian DPA (translated by A&O)
Respondent means a respondent to the Allen & Overy survey carried out between February and April 2012
Slovak DPA means Úrad na ochranu osobných údajov SR
Spanish DPA means comments made by the Director of the Spanish Data Protection Authority (AEPD) (translated by A&O)
Respondents warmly welcomed the removal of the requirement for data controllers to notify (ie register) with their supervisory authority, with half of respondents choosing this as the most welcome change. Also very popular was the formal recognition of BCRs in the proposed Regulation, and, to a slightly lesser extent, the changes to privacy by design and accountability (ie taking responsibility for demonstrating compliance through various internal measures).

Looking at changes that are of particular concern Respondents chose the right to be forgotten as the main issue, with a majority admitting that they were particularly concerned with this change. Also of particular concern were the data breach notification requirement and the issue of explicit consent. It is interesting that the increase in potential fines only came fourth in this survey. Also, the introduction of measures to promote accountability were of less concern.

Which three changes do you welcome the most?

- Increased fines
- Other
- Obligation to have a data protection officer (250+ employees etc)
- Right to be forgotten
- Data breach notification
- Consent to be explicit
- More direct obligations on data processors
- Accountability
- Privacy by design
- Recognition of BCRs
- Removal of notification requirement

Which three changes are of particular concern to you?

- Recognition of BCRs
- Other
- Privacy by design
- Accountability
- Obligation to have a data protection officer (250+ employees etc)
- More direct obligations on data processors
- Expanded territorial reach
- Increased fines
- Consent to be explicit
- Data breach notification
- Right to be forgotten
In general do you think the proposed Regulation is an improvement compared to the current legislative framework?

The Regulation has four main aims:

- a focus on harmonisation;
- the provision of greater rights to the data subject;
- cutting red tape; and
- addressing the challenges of the 21st century.

**YES** 47%

**NO** 25%

**DON’T KNOW** 28%

Do you think that the EC has listened to your concerns?

Viviane Reding, Vice-President of the EC in charge of Justice, Fundamental Rights and Citizenship has a vision of a single set of European rules on data protection, and one data protection authority for one company: a one-stop-shop.

Some Respondents felt that the proposed Regulation appears to be focussed on issues that arise in relation to social networking providers, but imposes the resulting requirements on everyone.

**YES** 15%

**NO** 30%

**DON’T KNOW** 55%

“In this legislative initiative represents an important step towards strengthening the protection of personal data of individuals in the territory of the European Union.” (Spanish DPA)

“At worst we fear that the proposed changes may put European businesses at a competitive disadvantage.” (CEII)

“Our members welcome the aims of the [Regulation] to improve legal certainty through harmonisation, to reduce the administrative burden on companies and providing effective rights to individuals. However, they doubt that these aims have been achieved” (BBA)

“The proposed draft is quite detailed, but at this moment the international context is very important and such detailed legislation may constitute an obstacle to the conclusion of international treaties regarding the protection of personal data” (Italian DPA)

“One key request was a single regulator. Have they achieved this? Some observers have commented that the reality may be that a company has a number of “main establishments” depending on their different business lines.” (Jane Finlayson-Brown, Allen & Overy)

“The Commission’s proposals are a positive contribution towards updating EU data protection law. We do not doubt that this is necessary.” (ICO)

“The one-stop-shop regime does not sit well with our corporate structure as we have a network of subsidiaries, each exercising a great deal of independence.” (Client)

“It appears that the EC has listened to the concerns laid before them, and opted for the highest compliance bar irrespective of the impact on cost, technology and consumer experience.” (Respondent)
The reform of the EU rules goes in parallel with the modernisation of data protection rules adopted in other international organisations... This means that the reform of EU rules comes at a crucial point in time and opens a window of great opportunities. If these opportunities are used well, this will reinforce the legal frameworks in the EU and achieve more global privacy at the same time. (EDPS)

The proposed Regulation is a huge step forward for data protection in the EU. (EDPS)

“High costs of compliance and legal ambiguity will stifle innovation and deter investment” (CBI)

“The draft Regulation includes a number of draconian requirements for businesses that will be difficult to implement for many” (Jane Finlayson-Brown, Allen & Overy)

Do you think that the proposed Regulation is fit for the 21st century?

Yes 37%
No 42%
Don't know 21%

One Respondent felt that despite presenting itself as fit for the 21st century, the proposed Regulation largely fails to grasp the nature of international data flows. Another stated that it is still lagging behind technological innovations.

Do you feel that the EC understands the challenges faced by business?

Yes 21%
No 63%
Don't know 16%

Some Respondents felt that the EC is failing to understand the challenges global businesses face today. One stated that the focus on protecting the data subject has failed to consider the potential negative impact on business.
Do you think the requirement for consent to be explicit is manageable within your business?

**YES** 53%

**NO** 35%

**DON’T KNOW** 12%

Do you think a right to be forgotten is workable?

**YES** 37%

**NO** 48%

**DON’T KNOW** 15%

**EXPLICIT CONSENT**

As well as requiring that a data subject’s consent to processing of its personal data is freely given, specific and informed, the Regulation requires that consent be explicit, shown either by a statement or by a clear affirmative action, which signifies agreement to the processing; the burden of proof is on the data controller. Respondents pointed out that this will inadvertently create increased burden on data subjects, but some welcomed the certainty.

**RIGHT TO BE FORGOTTEN**

Individuals can require the erasure of personal data relating to them and the abstention from further dissemination of such data, by the data controller in certain situations, eg they withdraw consent and no other legal ground for processing applies.

Where data has been made public, the controller shall take all reasonable steps to inform third parties to erase links to, or copies of, the data, and where the controller authorised the publication, it remains responsible. While attractive to users of social networks, it will be difficult and costly to implement.

“**We welcome the ‘high standard’ of consent provided for here.**” (ICO)

“No. Where we operate retail stores and therefore gain consent on a face to face basis, it is far more tricky to get explicit consent.” (Respondent)

“**Already today, certain EU member states (such as Belgium) require, in most cases, that consent be explicit to be valid. So in these member states, the requirement for consent to be explicit is not revolutionary.**” (Tom De Cordier, Allen & Overy)

“The right to be forgotten as currently drafted may give data subjects unrealistic expectations and cause disappointment and uncertainty when companies explain they have legitimate grounds for continuing to process the personal data.” (Charlotte Mullarkey, Allen & Overy)

“Players in Luxembourg are not welcoming the return of explicit consent in the draft Regulation.” (Cyril Pierre-Beausse, Allen & Overy)

“Players in Luxembourg are not welcoming the return of explicit consent in the draft Regulation.” (Cyril Pierre-Beausse, Allen & Overy)

“**Explicitly recognising the right to be forgotten is something we have been advocating and trying to realise steadily in recent years.**” (Spanish DPA)

“On many online platforms site administrators cannot realistically exercise full control of how posted data may be used or reproduced by third parties.” (E5)

© Allen & Overy LLP 2012
Will compliance with the accountability requirements and privacy by design mean big changes for the way you currently set your processes?

ACCOUNTABILITY AND PRIVACY BY DESIGN

The Regulation places onerous accountability obligations on data controllers, eg by requiring them to (i) maintain documentation of all processing activities (which shall be made available on request to their supervisory authority) with minor exceptions for certain small organisations, (ii) conduct a data protection impact assessment for more risky processing, eg using new, large-scale filing systems, and (iii) implement data protection by design and by default, eg data minimisation.

Do you think international transfers will be easier to carry out under the new regime?

INTERNATIONAL TRANSFERS

This is essentially the same toolkit. However, in certain member states (eg Spain and Poland) the process has been improved by the removal of the need for authorisation for model clauses. The legitimate interests concept has been introduced as a new derogation, applicable to transfers which are not frequent or massive—in some countries, this represents a useful broadening of the derogations; in others, this is more restrictive, eg the UK.
Are you more likely to implement BCRs as a result of the legislation?

Many Respondents welcomed the formal recognition of BCRs as a means for complying with data protection rules when carrying out international data transfers within organisations. One Respondent commented that the requirement for BCRs to cover every member of the group is ‘a somewhat unexpected sting in the tail’. We do not think that this was intentional and therefore anticipate that it may change.

Would you consider BCRs for processors?

BCRs are formally recognised by the Regulation, both for controllers and processors.

© Allen & Overy LLP 2012
Do you think your approach to data protection compliance will change as a result of the increases in the potential fines (which may now be up to 2% of annual worldwide turnover)?

- **YES** 71%
- **NO** 24%
- **DON’T KNOW** 5%

"The new sanctions regime appears to be disproportionately rigid. They could be based on turnover generated by parts of our business that do not process personal data. Further, the method of fining would concentrate reputational damage on those entities with the largest turnover, rather than those that have committed the more severe breaches." (Client)

"The potential amount of fines combined with increased obligations on controllers is clearly designed to create a paradigm shift and change businesses’ current, often relaxed, approach to privacy.” (Cyril Pierre-Beausse, Allen & Overy)

"The Working Party … welcomes the fact that the proposals harmonise the powers and competences of supervisory authorities to more effectively ensure and where necessary enforce compliance, both individually and in cooperation with each other, for example, by being able to impose significant fines.” (Working Party)

**SANCTIONS**

The Regulation establishes a tiered approach to penalties for breach which enables DPAs to impose fines of up to 2% of annual worldwide turnover. This represents a dramatic change which seems to be designed to attract the attention of board-level executives.

However, one Respondent commented that it would have little impact as they endeavour to comply regardless of the sanctions.

"the working party … welcomes the fact that the proposals harmonise the powers and competences of supervisory authorities to more effectively ensure and where necessary enforce compliance, both individually and in cooperation with each other, for example, by being able to impose significant fines.”

(Working Party)
The notification regime will be largely abolished and data controllers operating in a number of EU countries should be supervised by only one authority – will you make significant savings as a result?

Yes 18%
No 53%
Don’t know 29%

Will the costs that your company/organisation will incur as a result of the new obligations under the proposed Regulation significantly outweigh the savings as a result of the abolition of the notification regime and the streamlining of supervision to one DPA?

Yes 40%
No 27%
Don’t know 33%

“Our members are most concerned the Commission has stated that the reduction in the administrative burden from having one single law will generate cost savings of €2.3 billion (£1.9 billion), when members are clear that overall costs of compliance will increase and dwarf such savings from notifications.” (EBA)

“Members welcome many of the proposals, such as the abolition of the general notification requirement.” (EBA)

“While general notification obligations would be abolished, we expect that DPAs will be looking for alternative means of raising revenue.”

(Charlotte Mullearkey, Allen & Overy)

“Businesses with cross-border operations in particular have welcomed the Commission’s intentions to reduce elements of administrative burden by attempting to simplify companies’ relationships with … DPAs.” (CBI)

“It seems unlikely that non-EU based organisations, having no other connection with the EU than offering goods or services (including passive sales) will have the one-stop-shop available to them since they will not be able to point to a main establishment and even more unfair, such companies may well be subject to the whims of all 27 supervisory authorities. This may produce an anti-competitive effect, discouraging firms from offering goods and services in EU, reducing choices for both consumers and businesses.” (Client)

“Individuals and undertakings will not gain any advantage by selecting the most accommodating country in order to process personal data… The same law will be applicable in the entire European territory and the discretion of single national authorities will decrease.” (Italian DPA)

© Allen & Overy LLP 2012
Certain obligations under the new proposed Regulation will apply directly to data processors - will this have any impact on your organisation?

"The changes are certain to impact on the terms of many types of service agreements (eg cloud services, outsourcing and similar).”
(Nigel Parker, Allen & Overy)

“We may have to employ a small army of people to develop and maintain internal documentation for client data processing operations, to complete data privacy impact assessments and to review all our client contracts.”
(Client)

”The changes are certain to impact on the terms of many types of service agreements (eg cloud services, outsourcing and similar).”
(Nigel Parker, Allen & Overy)

“Role of Data Processors

Data processors have many direct obligations under the Regulation, eg assisting with impact assessments, implementing technical and organisational measures, maintaining documentation on processing activities and informing the controller immediately if there is a data breach.

Data processors also need the controller’s prior permission to appoint a sub-processor.

<table>
<thead>
<tr>
<th></th>
<th>YES</th>
<th>NO</th>
<th>DON’T KNOW</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>52%</td>
<td>26%</td>
<td>22%</td>
</tr>
</tbody>
</table>
Do you think a Regulation is the most appropriate legislative instrument to achieve the EC’s desire for increased harmonisation?

One Respondent felt that the price of consistency is too high. Another suggested that while a Regulation is appropriate it goes too far. A simpler Regulation addressing fewer issues would have been more appropriate and more likely to succeed. The Slovak DPA consider the proposal for a Regulation to be rather ambitious.

**YES** 66%  
**NO** 25%  
**DON’T KNOW** 9%

Would you prefer an increased standard of data protection which is harmonised, as opposed to a lesser standard which is not harmonised?

One Respondent noted that, from a US perspective, the biggest challenge has been ensuring compliance with all the different EU country implementations of the Directive. Many DPAs including the Dutch DPA have reacted positively to harmonising privacy regulations, creating an equal playing field for all member states.

**YES** 73%  
**NO** 16%  
**DON’T KNOW** 11%

"The EDPS is particularly pleased to see that the instrument of a regulation is proposed for the general rules on data protection. The proposed Regulation would be directly applicable in the Member States and would do away with many complexities and inconsistencies stemming from the different implementing laws of the Member States currently in place." (EDPS)

"Yes, the Regulation is the right way forward – we need uniform data privacy rules to allow European business to be efficient and competitive." (Respondent)

"Overwhelmingly, people do want a consistent standard, even if it is a high standard, but the problem with the Regulation as it currently stands is that it is far too onerous." (Jane Finlayson-Brown, Allen & Overy)

"There is a risk that the implementation of rules that may be perceived as onerous or disproportionate could actually lead to more variable standards of compliance by reluctant data controllers. For data protection to be effective in practice data controllers must be able to see a clear link between the measures they are required to take and the protection of privacy." (ICO)

"A more prescriptive approach will not necessarily bring about better data protection. In any case, complete harmonisation is probably an unachievable goal." (ICO)
Conclusion

The results of our survey and comments made by interested parties across the European Union, and beyond, show a wide range of views on the proposed Regulation. While their views often conflict, there are some general themes emerging.

Most welcome the intention and the use of a Regulation. However, the main concerns centre around excessive administrative burden, where the required activities may have little bearing on whether an organisation is adequately protecting the personal data it processes.

While some issues with the draft may be easily fixed (such as applying thresholds to data breach notification requirements), others promise to be more complex. It would appear that we are stuck with the cross-border transfer regime for now, and can only hope that some of the many concerns raised about the model may be addressed.

If you have any comments on this publication, we would be delighted to hear from you.
Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP’s affiliated undertakings. Allen & Overy maintains a database of business contact details in order to develop and improve its services to its clients. The information is not traded with any external bodies or organisations. If any of your details are incorrect or you no longer wish to receive publications from Allen & Overy, please contact corporatepublications@allenovery.com.

Global Presence

Allen & Overy is an international legal practice with approximately 5,000 people, including some 512 partners, working in 40 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

- Abu Dhabi
- Amsterdam
- Antwerp
- Athens (representative office)
- Bangkok
- Beijing
- Belfast
- Bratislava
- Brussels
- Bucharest (associated office)
- Budapest
- Casablanca
- Doha
- Dubai
- Düsseldorf
- Frankfurt
- Hamburg
- Hong Kong
- Istanbul
- Jakarta (associated office)
- London
- Luxembourg
- Madrid
- Mannheim
- Milan
- Moscow
- Munich
- New York
- Paris
- Perth
- Prague
- Riyadh (associated office)
- Rome
- São Paulo
- Shanghai
- Singapore
- Sydney
- Tokyo
- Warsaw
- Washington, D.C.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP’s affiliated undertakings. Allen & Overy maintains a database of business contact details in order to develop and improve its services to its clients. The information is not traded with any external bodies or organisations. If any of your details are incorrect or you no longer wish to receive publications from Allen & Overy, please contact corporatepublications@allenovery.com.

© Allen & Overy LLP 2012