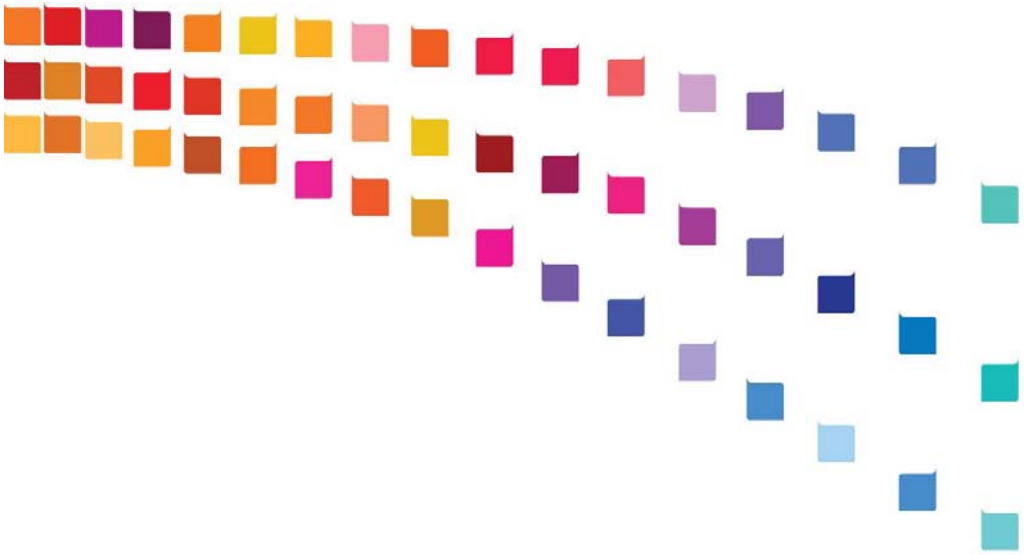
DMA response to Ministry of Justice call for evidence on proposals for EU Regulation com(2012)11 on data protection



DMA response to Ministry of Justice call for evidence on proposals for EU Regulation com(2012)11 on data protection

The DMA welcomes this opportunity to respond to the Ministry of Justice's Call for Evidence.

The DMA has consulted its membership and the following comments reflect their views on the likely impact that the draft Regulation would have upon their businesses were it to be implemented in its present form. Whilst it is not straightforward to give definitive costings for the Regulation's provisions, we have tried to show, by examples provided by some of our members, something of its practical impact upon data-driven direct marketing.

General

The DMA agrees that the current Directive needs to be reviewed and updated to take account of the significant technological developments and the increasing complexity of information systems and networks since the 1995 Directive was enacted. A comprehensive and uniformly enforced data protection regime across the European Union would certainly be beneficial to business (although this may be wishful thinking, given the varying cultural attitudes towards compliance and enforcement in the different Member States of the EU.)

We appreciate that there is merit in the streamlining of processes and we welcome the removal of unnecessary bureaucratic burdens such as notification requirements and that some organisations will only need to deal with a single national data protection authority in the home country of their main establishment. The simplification of Binding Corporate Rules for intra-firm transfer of data beyond European Economic Area (EEA) borders is also welcome. However, we note that the other rules on transfer of data outside the EEA have been made more prescriptive than the current regime in the UK – for example, the Information Commissioner's Office (ICO) will be required to pre-approve some transfers.

We fully support the Commission's aim to increase consumer trust and confidence as this can only be a positive development for business and consumer alike. Greater transparency will mean those organisations or individuals not complying with the rules can be more easily identified. We are concerned that the ICO will now have to take action against organisations for non-compliance with procedural points, rather than taking enforcement action on a risk-based approach.

It is important to maintain a balance between the need to protect individuals' rights and freedoms with the need to ensure a free flow of personal information within the Single Market and the legitimate commercial interests of business. As much as the DMA welcomes the general aim of the Commission to enhance privacy, reduce bureaucracy, and simplify data compliance, we do not have confidence that their proposal will deliver these outcomes. Overall, we believe that the Regulation would increase, rather than alleviate the regulatory burden on business and would have significant resource implications in terms of time, money, staffing and lost sales. Restrictions on online business models reliant on processing user data and high compliance costs could stifle innovation and deter investment. It is hard to see just how the European Commission's estimate that its proposals will save European business 2.3 billion euros has been calculated and we would welcome further information on this.

The DMA is seriously concerned that those small and medium-sized businesses, which make a vitally important contribution to economic recovery in the UK and other EU countries, will find some of the requirements of the proposed Regulation overly bureaucratic, restrictive and costly and potentially a significant deterrent to business start-ups or development. Anything that threatens innovation and the freedom to market goods and services in the current economic climate must be challenged.

There are also broader concerns about the far-reaching powers that would, under the proposed Regulation, be transferred from national governments and DPAs to the European Commission, which raise constitutional/political issues on subsidiarity which we do not address here. In particular, we are concerned about the power given to the European Commission under the Regulation to issue delegated legislation. We understand that these will not be ready when the Regulation is passed and this will create considerable legal uncertainty for organisations in relation to key parts of the legislative framework.

Specific provisions in the proposed Regulation

Opt-in / opt-out and obtaining explicit consent

The current proposal demands that organisations would have to obtain explicit consent from consumers by 'clear statement or affirmative action' to use their data for marketing purposes unless they were relying on the 'balance of interests' justification. While organisations would not necessarily have to get consumers to tick an opt-in box, they would not be able to take for granted that consumers consent to receiving marketing information - even if they have had previous interaction with them and were existing customers of the organisation.

There is doubt surrounding the issue of what would constitute 'fair processing' when considering the 'balance of interests' between the organisation and the consumer. The worst case scenario is that organisations that fail to prove they have properly obtained consent from individuals to contact them with direct marketing messages would have to scrap their contact databases completely. These would be costly to replace. There is also the question of what would happen to 'legacy data' validly collected under the current legal framework.

We would also welcome clarification as to the relationship between the Regulation and the Privacy and Electronic Communications Directive, which contains specific rules for electronic marketing communications. .

Definition of personal data and consequences for profiling

The new Regulation could class IP addresses as personal data. IP addresses are allocated to an individual device and often such devices might be shared in households, offices and other organisations, such as libraries. Furthermore, individuals connect via multiple devices (pc, laptop, mobile phone, tablet) and a particular IP address does not specifically reveal individual behaviour but merely the behaviour of a device.

This extension of the definition of personal data would result in web analytics no longer being available to organisations without the express consent of individuals and therefore limit commercial development. Even though analysis is concerned with the online activities of anonymised batches of IP addresses, the information itself could be considered personal data and hence off limits to those who did not provide consent. This has serious ramifications for digital marketers as they would then struggle to chart the journey consumers take from communication to action, or to analyse their behaviour online. Profiling is a legitimate business activity which benefits consumers, giving them more targeted and relevant marketing communications and this proposal would jeopardise that benefit.

Classifying IP addresses as personal data would also overlap with the Privacy and Electronic Communications Directive. Doing so would damage user experience of websites: their preferences might not be stored, which would deny visitors a personalised experience with the inconvenience of having to upload their details with every repeat transaction. These two effects would inflict incalculable damage on sales.

The right to be forgotten

The new Regulation proposing to give individuals the right to request organisations to delete any personal information that is held on them has been designed with social media networks in mind. This requirement would certainly stifle innovation for social media platforms, but the consequences of the right to be forgotten reach beyond that.

Organisations that hold an individual's data and pass them to third parties would not only have to delete their information but would also have to ensure that the third party does the same. This is clearly impractical. For data list brokers, this obviously has enormous and problematic implications and all organisations would also face increased data processing costs.

We welcome clarification from the Commission that the right to be forgotten would not prevent the use of an individual's data to be held for suppression purposes in direct marketing. However, this needs to be made clear specifically in the text of the Regulation.

Subject access request

Currently, organisations can charge a fee of £10 when supplying individuals with a copy of all of the information held on that individual, to meet a subject access request. Under the new Regulation, organisations would have to supply this information free of charge. The £10 fee does not cover the cost of collating and supplying the information but does, at least, act as a small check to discourage frivolous or vexatious requests. We are concerned that this may lead to an increase in subject access requests being used for other purposes, such as for early discovery at a pre-litigation stage in legal proceedings. (This point was identified in the Ministry of Justice's Call for Evidence on the Data Protection Act 1998 in 2010.)

The administrative burden this places on organisations is huge. In 2009, the Ministry of Justice estimated that UK businesses spend £50 million a year in fulfilling subject access requests through additional manpower costs.

A positive note, however, is that we welcome the proposed provision that a subject access right can be met by providing information to the data subject electronically, if that information is held electronically and the data subject agrees to this.

Data breach notifications

There are no requirements under the current Data Protection Directive to notify the authorities of serious data breaches but the new Regulation would radically change this. Every organisation that holds personal data would have to notify the ICO and the individuals concerned within 24 hours of any instances of data breaches. Although the current draft is particularly vague on the detail of how this would work, it is difficult to see how the ICO would cope practically with the weight of breach notifications which may, in any case, be of a minor nature. It is not always possible to identify breaches within 24 hours, or to assess the extent or likely detriment of a security lapse. If every data breach has to be reported, regardless of its nature or importance, there is a strong possibility of "notification fatigue" setting in – there is evidence of this effect in the USA where most states have this obligation. There is then a risk that consumers may ignore the notification of a serious breach, where they need to take action in order to prevent identify theft.

We would like to see a threshold level for data breach notification in the Regulation as there is in the Privacy and Electronic Communications Directive and the same wording to be employed.

International transfers of personal information to countries outside the EEA

While the rules on transferring personal information to countries outside the EEA may have been made more business-friendly, problems could arise with their application beyond the European Union. The law would apply to any organisation in the world processing information about European citizens, but in a digital world an organisation would not necessarily be aware that they were dealing with a European citizen until they had completed an online registration process. This requirement simply doesn't reflect the reality of 21st century global data transfer practices, and needs to be rethought if it is to be workable.

Marketing to children

This is an area where a prescriptive "one size fits all" approach may not work. We would prefer to see a risk-based flexible framework here, as recommended in the ICO's Personal Information Online Code of Practice.

Other compliance obligations

We have concerns about the proposal that organisations would have to keep full records of their data processing activities and supply them to the ICO on request, rather than as a matter of course under current rules. This does raise questions as to how the ICO will be adequately funded to carry out its work effectively.

The additional bureaucratic requirements will certainly create extra administrative costs, particularly for smaller organisations. Implementing the right to be forgotten, explicit consent for data processing and appointment of data protection officer will all create additional administrative costs. The requirement for organisations with 250 or more staff to have a designated independent data protection officer takes no account of the nature of the organisation's business and how much, or little, data is handled by them.

Sanctions regime

The proposal to levy potential fines of up to 2% of an organisation's global turnover is disproportionate and inappropriate in this context, and could lead to organisations removing their operations offshore, or restructuring into different parts to avoid larger penalties.

Conclusion

The DMA looks forward to working closely with the Ministry of Justice as the negotiations on the draft Regulation proceed in Brussels.

The DMA has commissioned research into the economic impact of the Draft Regulation and into consumer attitudes to privacy. We will send a copy of this research to the MoJ when available (likely to be late April 2012).

For further information, please contact:

Caroline Roberts, Director of Public Affairs: tel. 020 7291 3346, email caroline.roberts@dma.org.uk
James Milligan, DMA Solicitor: tel. 020 7291 3347, email james.milligan@dma.org.uk

Appendix – Case studies

The examples below have been provided by some of our member organisations to illustrate their estimate of the impact on their business of the Regulation in its present draft.

1. Global marketing services provider

- The proposed Regulation will add significant additional administrative costs especially around the right to be forgotten, explicit consent for data processing and the appointment and training of a Data Protection Officer. Increased responsibility and accountability of data processors will also place additional administrative costs, plus increased insurance costs against potential fines and penalties.
- There is a cost implication in the review and assessments of all legacy systems which collect personal data to make sure of compliance with the new requirements, e.g.Privacy by Design
- It is difficult to quantify the potential additional costs but in staffing and training costs alone, the company would expect this to be in the region of £50,000 to £ 75,000 per year.

2. Data services provider to the retail sector

- New data portability and right to be forgotten clauses could require one off new system development at a cost of £100,000
- Cost of up to £5 million pounds for each year of legacy data (up to a maximum of 7 years) that could not be used if Draft Regulation had retrospective impact on data which had already been collected.

3. Membership organisation with charitable status

- General rule requiring explicit consent for marketing would make fundraising via marketing almost impossible.
- Increase in call time with regard to information needed to be provided to donor on phone – estimate of additional 10 seconds – means an annual full time requirement of 1.8 agents. Also additional 10 seconds average handling time to back office processes gives an annual requirement of 1.3 full time agents. Total of 3.1 full time agents or additional costs of £90,000 means a requirement of an additional 1800 individual memberships to cover this.
- Several of our charity members have said that their ability to fundraise via marketing would be made more difficult. There is also a problem over how much information consumers can take in at a time and at least one charity thought that the extra time it will take to provide the necessary information on privacy could well put donors off the whole process.

4. Financial Services Organisation

- Cost of reformulating databases to take account of changes - £ 100 -500k
- General rule requiring opt-in consent for marketing may lead to inability to market to existing customer database – loss of revenue estimated at around £6 million
- Cost per lead from data list brokers could increase by double
- Cost or responding to a Subject Access Request would be an additional £ 30-50 per request based on system set –up costs and incremental staffing and administrative costs due to changes in procedure in draft Regulation.
- Consent requirements would create additional administration, and possible difficulties, for accounts held in joint names.

5. Bureau Cleaning services (organisation which cleans lists for other direct marketing organisations against preference services files and other suppression files, such as names of recently deceased persons and those who have recently moved house).

- General rule requiring opt-in consent for marketing could lead to a 50% drop in data being sent to it for processing.

6. List broking company

- Changes introduced in draft Regulation could lead to a 50% drop in turnover which would mean closure of business with loss of 26 full time jobs

7. B2B Telemarketing and Digital Marketing Company

- Digital side – adding a consent form to all website downloads – 1 day's development work at £400 per day.
- Adding opt-in telemarketing button to CRM system: 1 day development work at £560
- Cost of staff training £7,600 per annum
- Cost of updating CRM system with clear statement of affirmative action - require call recording cost £1000's.

8. Global data company

- Introduction of explicit requirements for consent - loss of revenue in excess of £1m
- Review, assessment and updating legacy data to comply with new requirements – cost in excess of £500,000
- New data security and breach notification requirements - cost between £100–500,000.
- System developments to take account of the right to be forgotten, data portability, removal of fee for subject access requests, privacy by design – one off cost in excess of £500,000.

9. List broking and list owning businesses

Business	Current turnover £ 000	Current revenue £ 000	Current profit £ 000	Impact of opt-in on turnover £ 000 *	Impact of opt-in on revenue £ 000 *	Impact of opt-in on profit £ 000 *
Large broker	3,500	1000	100	350	100	10
Small broker	1000	300	30	100	30	3
Total Broking sector	120,000	36,000	3,600	12,000	3,600	360
Large list owner	25,000	20,000	4,000	2,500	2,000	400
Small list owner	2,500	2,000	400	250	200	40
Total List Owners	600,000	480,000	96,000	60,000	48,000	9,600

* Assuming impact of opt-in would lose 80% of names, representing 90% of turnover

In these circumstances, list-broking would no longer be a viable business model and third party list ownership would become a high risk business option.

There are approximately 100 organisations directly involved in the UK in list-broking and list-owning sectors: between 600 and 1000 jobs would be at risk.

Additionally, the cost of customer acquisition would increase for all brands significantly.

The Direct Marketing Association (UK) Limited (DMA) is the national trade association for the UK direct marketing industry, with over 900 corporate members and positioned in the top 5% of UK trade associations by income. The total value of direct marketing to the UK economy is estimated to be £72.5 billion. This comprises three separate figures; £43.3 billion on expenditure on direct marketing media and activities, £16.7 billion on employment and £12.5 billion on overheads resulting from employment.

The DMA represents both advertisers, who market their products using direct marketing techniques (such as financial services; media owners; retail; charities; sport, travel & leisure; publishers; political parties) and specialist suppliers of direct marketing services to those advertisers (for example, list brokers/owners/managers; data bureaux; email and mobile marketers; online and web marketers; dm agencies; mailing houses; outsourced contact centres).

Please visit our website www.dma.org.uk for further information about us.