SpeechlyBircham

December 2011

Draft Regulation on the Protection of Individuals with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation)

Briefing

On the 29th November 2011 the European Commission published an updated version of its draft Regulation intended to produce a harmonised Data Protection Framework for the EU which amongst other things will repeal the Data Protection Directive 95/46/EC.

Whilst the intention of the Regulation is "to build a stronger and more coherent Data Protection Framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities", the Regulation in its current draft form imposes significant changes to the way in which businesses comply with Data Protection laws and regulations in the EU.

The European Commission considers that a Regulation "will be the most appropriate legal instrument to define the framework for the protection of personal data in the EU since the direct applicability of the Regulation will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functionality of the internal market".

Whilst the key principles of the Data Protection Directive and the majority of the definitions therein remain the same there are significant changes to some definitions, clarification over some of the principles (in particular consent), reinforcement of the current solutions for data transfers and most importantly the addition of new obligations for both data controller and data processor in terms of the role of the Data Protection Officer, mandatory reporting of data breaches, dramatic increases to enforcement powers and fines and specific obligations in relation to the personal data of children.

We understand from our sources that the draft Regulation will be announced on 25th January 2102 and will come into force 2 years after publication.

If the Regulation is published in the same form as the current draft of which we are in possession then businesses that either have entities in Europe processing personal data, or use equipment in the EU for processing personal data, or are not in the EU but where the processing activities are directed to EU data subjects or served to monitor their behaviour, then significant compliance actions will need to be made.

As the Regulation applies to both data controllers and data processors and dramatically extends the enforcement powers of the regulators and the fines for non-compliance (5% of worldwide

Speechly Bircham LLP 6 New Street Square London EC4A 3LX
Tel +44 (0)20 7427 6400 Fax +44 (0)20 7427 6600 DX 54 Chancery Lane email information@speechlys.com web www.speechlys.com

revenue for negligent or reckless breach) businesses will need to prepare for investment in EU data protection compliance.

The current draft Regulation runs to 116 pages, but our summary of the key provisions are as follows:

- The Regulation will be binding on all member states from the date that it comes into force. That date will be 20th day following the date of publication of the Regulation in the official journal of the European Union and the application of the Regulation will be 2 years from the aforementioned date. Our understanding is that an announcement of the final Regulation may take place in the Spring of 2012 which means that we can expect the Regulation to enter into force in the second half of 2012 giving a 2 year period for businesses to get into compliance by 2014.

- The Regulation applies to both data controllers and data processors who have either legal entities in the EU, or process personal data of EU data subjects irrespective as to the location of the controller or processor, but the Regulation does not apply where the processing is by an individual purely for personal or household activities.

- Most of the current definitions of data subject personal data and the like remain the same except that sensitive personal data now includes genetic and biometric information and consent is defined as “any freely given specific, informed and specific indication of” the data subjects signification for the purposes of processing and “personal data breach” is now defined in respect of breach of security for which new obligations arise.

- The data protection principles broadly remain the same although it should be noted that consent and the mechanisms for gaining consent are provided in detail in Article 7. Article 7 amongst other things states that consent cannot be automatically implied in respect of the processing of employees data, nor in respect of the processing of the data of a child where the child is under the age of 18 and parental consent has not been given.

- Fair processing statements or privacy notices will have to be in plain and intelligible language and drafted with certain data subjects in mind “in particular for any information addressed specifically to a child”.

- In a privacy statement or privacy notice Article 12 indicates that there needs to be specific information given to a data subject in respect of the nature and purposes of the processing of their data and of their rights and there are detailed requirements in relation to profiling and the collection of data via social network services.

- Whilst subject access requests are still permitted in addition there is now in Article 15. In addition Article 15 provides the “right to be forgotten” and to have personal data erased. This new right in conjunction with the right of data portability in Article 16 will require businesses to implement stricter controls over the management of data bases particularly where they are outsourced.

- Article 16 and 17 provide new rights to object to profiling and obligations in respect of companies that use profiling technologies.

- There are redefinitions of the obligations for the data controller, joint data controllers and the data processor and the data processor now has a direct liability for compliance which does not exist in the current regime.

- Whilst the concept of registration or notification with a data protection authority is likely to remain in place there is now, under Article 25, a new obligation for the controller and processor to maintain an internal register of compliance and to make this available on request to the Data Protection Authority concerned by virtue of its new powers.

- There are enhanced requirements for data security and specifically in Article 28 there is a mandatory breach notification procedure for all but small enterprises.

- There are new details in relation to Privacy Impact Assessments and specific prior authorisations and prior consultations before data processing or data transfers may be permitted and in relation to data transfers there is considerably more detail on binding corporate rules as a solution to transborder data flows or transborder data transfers.

- For the first time the role of the data protection officer is introduced for all but small businesses and this will require businesses to put in place not only contracts for the engagement of the Data Protection Officer, but also training and powers for the Data Protection Officer in terms of an ability to be independent for the purposes of compliance. We think it likely that the Data Protection Officer will be the person responsible for maintaining internal compliance registers and being the interface between the business and the regulators.

- Whilst there are other specific issues, the last one that we wanted to mention is that in relation to the new powers of enforcement for the Data Protection Authorities who will have an independent duty to monitor, audit, provide guidance, hear complaints, conduct investigations, opine on compliance issues and publish permission or licences for international data transfers. Furthermore in respect of breaches of the Regulation there are a whole new range of penalties and sanctions with fines for minor breaches of 1% of a businesses annual worldwide turnover rising to 5% of annual worldwide turnover in the case of intentional or negligent breach of the Regulation.

Whilst there is no guarantee that the documentation we currently hold will be the final published Regulation we anticipate that at this stage few significant changes or additions will be made and therefore we are starting the process of considering the full range of compliance, policies, practices and procedures that will be necessary for small, medium and large enterprises whether operating in a single member state or operating globally.

Contact

If you have any queries or require any further information, please do not hesitate to contact:

Robert Bond
Partner at Speechly Bircham LLP
+44 (0)20 7427 6660
Robert.Bond@speechlys.com