

EU Releases Proposal for New Data Protection Laws

4 More London Riverside
London SE1 2AU

T/ +44 20 7379 0000
F/ +44 20 7379 6854

info@lg-legal.com
www.lg-legal.com



26th January 2012

The European Commission has this week released its proposal for a new data protection framework, signalling the most significant global legislative development affecting the collection, use and protection of personal information of the past 15 years. The Commission's proposals are aimed at updating and modernising the existing laws, which are seen as inadequate given the ways in which technology allows personal data to be used, transferred and stored.

The proposed laws will require all businesses collecting personal data in the EU to make changes to the way they collect and process that data, although there should be a period of at least 2 years until the laws take effect.

Legal changes

The main changes introduced by the new regime will be as follows. These notes are for general information only and are not intended to provide legal advice.

A Single Regulation for the EU -

Introducing the revised laws by way of a regulation means that a single set of rules will be implemented across the EU. This should save businesses money, as the notification requirements for companies in each country in which data is collected and processed will be abolished.

Application to companies based outside of the EU - EU rules will apply if personal data is handled abroad by companies that are active in the EU market and offer services to EU citizens. This means that social media companies

such as Facebook will have to ensure they are aligned with the new EU laws.

Stronger rights – The Commission has introduced the controversial 'right to be forgotten'. Individuals will have the right to have their personal data erased and no longer processed. Although there are some exceptions to this rule, this could create particular difficulties for personal data stored in the cloud, or via social media networks. For example, the law will require that a data controller who has made personal data public is to take all reasonable steps to ensure the erasure of data by third parties who may also be processing data. The Commission also wants to give people as much control as possible over their data, particularly in relation to profiling activities.

Controller's responsibilities – Data controllers will face very specific responsibilities ranging from the adoption of policies and principles such as privacy by design and privacy by default to the training of staff and the appointment of data protection officers. This will be one of the most noticeable differences with the existing regime, as putting in place a comprehensive data protection compliance programme will become a legal obligation under the statute.

Need for explicit consent - Consent should be given explicitly by any appropriate method enabling a 'freely given specific and informed indication of the data subject's wishes', either by a statement or by a clear affirmative action. This will ensure that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an internet website or by any other statement or

Want to know more?

Please contact:



Peter Brudenall
Partner

T/ +442077596823
E/ Peter.Brudenall@lg-legal.com

Peter is a specialist in technology, outsourcing and data protection law. He has over 15 years' experience in advising companies on the procurement of technology, the outsourcing of services (both IT and business process outsourcing), contract disputes, software licensing and development, and data protection and information security issues. He also advises companies on intellectual property, research and development agreements and distribution agreements.

conduct which clearly indicates the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore *not* constitute consent.

Data Processing Impact Assessments -

Companies will be required to carry out privacy impact assessments before processing any data that is likely to present specific risks to individuals, and to be transparent as to what data they hold and how it is used. If such an assessment suggests that processing may be particularly risky (for example, by using new technologies) then the regulator would need to be informed.

Security – Both the data controller and the data processor (ie service provider) will need to have in place measures to protect personal data from a data breach – meaning that the data processor will for the first time have direct regulatory responsibility for security.

Data Portability - Companies must make data easier to be transferred from one service provider to another by making consumer information readily available to individuals.

Data breach notification – As is already the case for providers of communications services, an obligation to notify security breaches to data protection authorities will now apply to all controllers. If feasible, notifications are to be made within 24 hours after having become aware of the breach. Again, this will represent a significant departure from current practices. However, if the breached data has been encrypted or appropriate technological protection measures have been applied to the data to render the data unintelligible, there is no requirement to notify the data subject (although notification must still be given to the supervisory authority).

International data transfers – The Regulation suggests that binding corporate rules should become the norm for data transfers within international companies going forward. Binding corporate rules are data protection policies applying to a group of companies wishing to transfer personal data into and out of the EU.

Role of data protection authorities – The data protection authority of the Member State where the main establishment of a data processing organisation is based will be responsible for supervising that organisation across the whole of the EU.

Enforcement powers – national data protection authorities will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules. This can lead to penalties of up to €1 million or up to 2% of the global annual turnover of a company.

Data Protection Officers – For any company with more than 250 employees, a data protection officer would be appointed to ensure that the Regulation's rules are being enforced appropriately.

Practical Implications

Privacy policies and consent forms -

The importance of deploying the right privacy policies and consent forms will become increasingly important under the new Regulation and existing policies may no longer be adequate.


Encryption - Companies should examine what data needs to be encrypted to mitigate the effect of a data breach, as the loss of unencrypted data could lead to the increased costs of providing notification to individual data subjects.

Subject access and other rights – Having suitable procedures to comply with subject access and other individuals' rights will be the key to getting this aspect of compliance right.

Data Processors and Service Providers

– Data Controllers may need to review their contracts with service providers, to ensure that responsibilities are clearly set out and are consistent with the proposed law. Service providers who process personal data for their customers may, however, wish to look to these laws as an opportunity to demonstrate higher levels of security than their peers, but should in any event be certain that processes are in place to ensure compliance. Encouragement will be given to associations to develop 'codes of conduct' as well as certification mechanisms, data protection seals and the like in order to allow individuals to quickly assess the level of data protection and data security offered by particular organisations, and service providers should start thinking now about how these could be developed.

Accountability framework – Under the new regime, evidencing compliance will be critical. This means adopting easy to find and understand internal compliance policies and implementing a sensible line of responsibility. Whilst it is still early to know what privacy by design and privacy by default will amount to, the practice of



carrying out privacy impact assessments should already be embedded into product design activities where such products involve accessing or using customer data.

Insurance – Examine insurance policies covering data breach and cyber liability – traditional insurance products are unlikely to provide the scope of coverage required by the proposed Regulation, and specific products may need to be obtained.

The Commission's proposals will now be passed on to the European Parliament and EU Member States meeting in the Council of Ministers for discussion. They will take effect two years after they have been adopted.