



New EU Data Protection Regulation Announced

The official proposal for an EU Regulation on Data Protection was released in Brussels on Wednesday 25 January 2012 (the “Regulation”). The Regulation, which will replace the existing EU data protection regime, will have a significant impact on almost every business either established in the EU or that has EU customers. The proposed Regulation will now be discussed in detail over the next few months as it goes through the European legislative process and is set to be adopted in 2014. The main implications of the proposed Regulation are summarised below.

- **Greater Enforcement** – fines can be imposed of up to **2% of the annual worldwide turnover** of a business for failure to comply with the proposed Regulation. In addition, supervisory authorities will be able to impose a temporary or definitive ban on processing personal data, enter premises and suspend data flows to a recipient in a third country or to an international organisation.
- **Class Actions** – any organisation which aims to protect the data protection rights of individuals, such as consumer organisations, can make complaints to supervisory authorities and bring class actions on behalf of individuals for non-compliance, even without the consent of those affected.
- **Application to Non European Businesses** – the proposed Regulation will apply to businesses established in the EU and importantly to non-European businesses that process personal data of individuals residing in the EU where the processing activities are related to offering goods or services to such individuals or the monitoring of their behaviour.
- **Accountability** – businesses will be required to adopt policies and implement measures to demonstrate compliance with the requirements in the proposed Regulation. This will include keeping a detailed record of all forms of data processing and carrying out data protection impact assessments. This will lead to significant compliance costs for affected businesses. Privacy by design measures must also be implemented to ensure, for example, that data is not collected or retained beyond the minimum necessary.
- **Data Protection Impact Assessments** – the proposed Regulation introduces a new requirement for impact assessments to be conducted where the processing is likely to present specific risks, such as the processing of health data. As part of the assessment the views of the individuals whose data are being processed need to be obtained.
- **Data Protection Notifications** – while the requirement in some EU Member States for data controllers to notify their Data Protection Authority in respect of their data processing activities will be abolished, businesses will be required to consult the relevant supervisory authority prior to the processing of personal data where a data protection impact assessment is required. Where the supervisory authority considers that the assessment

This **Sidley update** has been prepared by Sidley Austin LLP for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.

Attorney Advertising - For purposes of compliance with New York State Bar rules, our headquarters are Sidley Austin LLP, 787 Seventh Avenue, New York, NY 10019, 212.839.5300 and One South Dearborn, Chicago, IL 60603, 312.853.7000.

Prior results do not guarantee a similar outcome.

insufficiently identifies or mitigates risks it can prohibit the intended processing. Where a data controller or processor is established in more than one EU Member State then the competent authority is where the controller or processor has its main establishment.

- **Information Security** – the proposed Regulation requires data controllers and processors to implement appropriate technical and organisational security measures after having carried out an evaluation of data privacy risks. Moreover, data security breaches will have to be notified to the relevant supervisory authority without undue delay and “where feasible” no later than 24 hours after having become aware of it. The proposed Regulation specifies that when the breach notification is not made within 24 hours a reasoned justification must be provided to the relevant supervisory authority. The breach will have to be communicated to the individual without undue delay when the breach is likely to adversely affect the protection of the personal data or the privacy of the individual.
- **Consent** – the proposed Regulation places the legal burden on the data controller to prove that the individual has given consent and gives an individual a right to withdraw their consent at any time. The Regulation also significantly restricts reliance on consent “where there is a significant imbalance between the position of the data subject and the controller.”
- **Data Protection Officers** – businesses with over 250 employees will be required to appoint a data protection officer who will have to have “expert knowledge” of data protection law and practices. The appointment which must be for a term of at least two years should be notified to the relevant supervisory authority and the public. The proposed Regulation also provides that businesses may appoint a single data protection officer for a corporate group.
- **Increased Rights of Individuals** – businesses must have transparent and easily accessible data protection policies and provide information using clear and plain language. An individual also has a right to correct his or her personal data and, importantly for social media, a right to data portability (*i.e.* to transfer his or her personal data to another provider) and will have a right to be forgotten (*i.e.* to have his or her personal data erased) which will be complex to apply in practice.
- **Transfer of Personal Data from the EU** – the proposed Regulation maintains the restriction under the current Data Protection Directive of transferring personal data to countries outside the EU that are not considered to provide an adequate level of protection including the United States. The Regulation provides that one of the main solutions to permit such international transfers is the adoption of Binding Corporate Rules, which are a set of data protection rules adopted by an international corporate group that meet EU requirements and must be approved by a lead supervisory authority. Significantly, the proposal confirms that that specific sectors of a country could be deemed adequate – perhaps paving the way for recognition of the United States health, communications and financial sectors.

The proposed Regulation will certainly be subject to lengthy discussion and revision by the Council of Ministers and the European Parliament before it is finally adopted and becomes law. However, it is clear that whatever the final form of the Regulation it will have a significant impact on businesses worldwide, increase compliance costs and enforcement actions and will therefore require a new approach to data protection.

If you have any questions regarding this update, please contact:

London

John Casanova
jcasanova@sidley.com
+44 20 7360 3739

William Long
wlong@sidley.com
+44 20 7360 2061

Washington, D.C.

Ed McNicholas
emcnicholas@sidley.com
+1 (202) 736 8010

Alan Raul
araul@sidley.com
+1 (202) 736 8477

The Privacy, Data Security & Information Law Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers. Sidley provides services in the following areas:

- Privacy and Internet Litigation and Regulatory Advice
- Data Breach, Incident Response, and Cybersecurity Advice
- Global Data Protection and Information Security
- Information Governance Assessments and Compliance Programs
- International Data Transfer Solutions, Outsourcing and Cross-Border Issues
- Cyberlaw, E-Commerce, Social Media, Cloud Computing and Internet Issues
- EU, China and Japan Compliance Counseling
- Gramm-Leach-Bliley and Financial Privacy
- HIPAA and Healthcare Privacy
- Communications Law and Data Protection
- Workplace Privacy and Employee Monitoring
- Unfair Competition, Advertising and Consumer Protection
- Website Policies Online Trademarks and Domain Name Protection
- Records Retention, Electronic Discovery, Government Access and National Security

To receive future copies of this and other Sidley updates via email, please sign up at www.sidley.com/subscribe

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

www.sidley.com

Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm's offices other than Chicago, New York, Los Angeles, San Francisco, Palo Alto, Dallas, London, Hong Kong, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin (NY) LLP, a Delaware limited liability partnership (New York); Sidley Austin (CA) LLP, a Delaware limited liability partnership (Los Angeles, San Francisco, Palo Alto); Sidley Austin (TX) LLP, a Delaware limited liability partnership (Dallas); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley, or the firm.

SIDLEY AUSTIN LLP
SIDLEY