GLOBAL BANKING & FINANCE REVIEW
GlobalBankingAndFinance.com

# SIGNIFICANT IMPACT OF NEW EU DATA PROTECTION REGULATION ON FINANCIAL SERVICES

April 18, 2014 Top Stories 0 Comments

William Long, Partner at Sidley Austin LLP

Over two years ago, in January 2012, the European Parliament published a proposal for an EU Regulation on Data Protection (the "**Regulation**") to replace the current European Data Protection Directive. Whilst the Regulation raises significant issues for all industries, the financial services sector has been particularly concerned given the billions of financial records and transitions handled yearly. Due to its potential impact, the proposed Regulation has been one of the most lobbied pieces of European legislation in European Union history. According to reports, the European Parliament's Civil Liberties Committee, which has been negotiating the Regulation, has received over 4,000 amendments.

On 12 March 2014, the European Parliament voted in a plenary session to fully endorse the proposed Regulation. In order for the proposed Regulation to become law, it must now be adopted by the EU Council of Ministers and the European Commission which is expected to happen sometime in 2015. EU Member States will then have a short period to implement the Regulation, which is expected to be around twelve months, before it becomes law.

Financial services companies should start considering now the significant impact of the Regulation on their business and assessing the changes that should be made to ensure compliance once the Regulation is adopted. The main elements of the proposed Regulation that will have a significant impact on financial services are summarised below:

- ***Significant Fines and Greater Enforcement***: non compliance with the Regulation could lead to fines of up to 5% of annual worldwide turnover or €100 million whichever is the *greater*. Individuals and any association, acting in the public interest, will also have the ability to bring claims for non compliance.

William Long

- ***Broad Territorial Scope***: the proposed Regulation will not only apply to businesses established in the EU, but also to businesses outside the EU that offer goods or services to European customers and process their personal data. This means that financial services companies established in the US or other non-EU countries, but have data on European customers, such as through offering services through a financial services website, will have to comply with requirements under the proposed Regulation.

- ***Security***: under the proposed Regulation financial services companies and their vendors will need to implement appropriate technical and organisational security measures. Security policies will also have to contain a number of elements including, for example, a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness. Importantly, there will also be a mandatory requirement to report security breaches to Data Protection Authorities without undue delay and to customers where the breach may adversely affect them. Financial services firms should therefore start reviewing their existing security policies and procedures and consider amending them to ensure compliance with the new requirements under the proposed Regulation.

- ***Accountability***: under the Regulation businesses will be required to adopt all reasonable steps to implement compliance procedures and policies that respect the choices of individuals. Such procedures and policies will need to be reviewed every two years. Businesses will also have to implement privacy into the design of products and services throughout the lifecycle of processing from collection of data to its deletion. In addition, businesses will need to keep detailed documentation of data being processed and carry out a privacy impact assessment where processing involves more than 5,000 individuals, with the assessment being reviewed every two years. Financial services companies should consider doing a gap analysis between their current data protection programme and what is required under the Regulation.

- ***Standardised Information Policies:*** under the proposed Regulation, certain standardised data protection information will have to be provided to individuals in the form of symbols or icons. Individuals will also have to be informed about how their personal data will be processed and their rights of access to data, rectification and erasure of data and of the right to object to profiling. Financial services businesses should start to consider whether current customer documents, policies and procedures will need to be amended to deal with the new requirements under the Regulation.

- ***Data Protection Officers***: financial services companies with personal data on more than 5,000 individuals in any 12 period or that processes sensitive data, such as health data, will be required to appoint an independent data protection officer who should have extensive knowledge of data protection and have a direct reporting to executive management. This requirement will mean that many financial services companies will have to appoint data protection officers and in practice build a privacy office.

- ***Profiling:*** every individual will have a general right to object to profiling and to be informed of this right in a "highly visible manner". The proposed Regulation also provides that profiling which significantly affects the interests of an individual can only be carried out under limited circumstances such as with the individual's consent, and should not be automated but involves human assessment. Profiling is important to many financial services companies and so the new requirements on profiling should be carefully analysed and procedures designed to deal with these new requirements.

- ***International Data Transfers***: the current prohibition on transfers of personal data from the European Economic Area continues under the proposed Regulation. Of the possible data transfer solutions to allow for international transfers, emphasis is given in the Regulation to Binding Corporate Rules ("BCRs"). BCRs require businesses to implement a global privacy policy following EU standards which once approved by EU Data Protection Authorities allows for international transfers of data. Importantly, the latest amendments to the Regulation re-introduce a provision requiring that any requests for access to personal data by foreign authorities or courts outside the EU must be authorised by a relevant EU Data Protection Authority. If enacted this will have a significant impact on financial services companies involved in cross-border litigation, investigations or regulatory reporting obligations.