Finding an alternative 'safe harbor' for US financial organisations

Could US financial privacy rules be used by organisations as an alternative route for the safe transfer of data from the EU to the US? **Dr Jan-Peter Ohrtmann** examines whether the Gramm-Leach-Bliley Act meets data protection requirements set out in European and German law.

In November 1999, the US "Financial Services Modernisation Act" (also known as Gramm-Leach-Bliley (GLB) after its legislative sponsors), was enacted. With this Act, the US legislator, especially the US Department of Commerce, intended, among other matters, to ease the transmission of personal data between the EU/European Economic Area (EEA) and the US.

GLB required further regulations regarding the protection and disclosure of consumer financial information with respect to financial institutions not covered by the regulations of other federal or state agencies. On May 23rd 2003, these privacy provisions - the 'Safeguards Rule' issued by the US Federal Trade Commission (FTC) - became effective.

This article considers whether the implementation of GLB meets the requirements of EU and German data protection law regarding the transfer of personal data to countries outside the EEA, referred to as "third countries" by the European Commission.

EU-US DATA TRANSFERS - THE LEGAL FRAMEWORK

Under EU law the transfer of personal data to countries outside the EU/EEA is generally only permitted with the consent of the data subject (within the circumstances specified in Article 26) or if the destination countries provide an 'adequate' level of protection for personal data. The transfer to other third countries is prohibited. This is stipulated in Article 25 of the EU Data Protection Directive, a provision that has been implemented into German law by Section 4(b) paragraph 2, 3 of the German Federal Data Protection Act (BDSG).

So far, US law has not been regarded as providing an adequate standard of protection. The FTC issued the so-called "Safe Harbor" rules in 2000 which can be adopted by certain types of organisations (but not financial institutions) on a voluntary basis and permit a continuous transfer of personal data from the EU/EEA to the US. However, only around 300 US companies and other organisations have signed up to Safe Harbor. Consequently the transfer of data to the US still faces major obstacles.

> it is unlikely that a German data protection authority will assume that GLB provides an adequate level of protection in the financial sector.

THE PROVISIONS OF GLB

GLB applies to institutions in the financial sector. However, it limits a financial institution's transfer of personal data to third parties only with regard to unaffiliated third parties. The data that is protected is personal, non-public financial information of 'consumers' and 'customers'. In this context 'non-public financial information' means information that a financial institution has a reasonable basis to believe is lawfully available to the general public from one of the following three sources: official records, widely distributed media and public disclosures required by law.

As a general rule, financial institutions may not disclose consumers' non-public financial information to unaffiliated third parties. This applies unless the consumer has been notified prior to the disclosure and has not opted-out. In addition, customers must receive initial, annual and corrective notices of the institutions' privacy policies. And finally, financial institutions may not disclose customers' account numbers to unaffiliated parties for marketing via the telephone, post or e-mail.

However, this rule is rendered ineffective by numerous exemptions. These exemptions apply, for example, to the institutions' risk and claims management or fraud prevention, to security or confidentiality of consumers' records and to resolving consumer disputes or enquiries. Additionally, among others, the financial institutions may disclose the information to persons holding a legal or financial interest relating to the consumer or acting in a fiduciary capacity and to consumer credit reporting agencies. GLB does now prevent the resale of credit header information (basic information identifying the individual to which the credit report relates) by consumer reporting agencies to direct marketers and provides for privacy policies for the more than 100,000 businesses to which GLB applies.

PENDING POSITION OF THE EUROPEAN COMMISSION

By implementing GLB, the FTC has now put the question to the European Commission as to whether GLB meets the requirements of Article 25 of the EU Data Protection Directive by providing an adequate level of protection for data transferred to the US. The Commission's decision will give a guideline for national Data Protection Authorities (DPAs) as to how to assess this question in their national jurisdictions.

The Commission has not yet declared its position. According to the findings of the EU Article 29 Data Protection Working Party, a two-part analysis must be applied to the adequacy test. Firstly,

compliance with the minimum principles of (a) purpose limitation, (b) data quality and relevancy, (c) processing transparency, (d) data security, (e) data access, correction and objection and (f) restrictions of onward transfer, and secondly, whether an effective enforcement regime is provided.

THE GERMAN LAW PERSPECTIVE

As long as the Commission has not come to a conclusion about the question of adequacy, national DPAs will have to assess the protection offered by GLB without a common guideline. Under German law each respective *Land* DPA is competent. They will apply Section 4(b) paragraph 2, 3 of the BDSG which stipulates almost the same wording as Article 25 of the EU directive:

> "Particular consideration for the adequacy of the afforded level of protection shall be given to the nature of the data, the purpose, the duration of the proposed processing operation, the country of origin, the recipient country and the legal norms, professional rules and security measures which apply to the recipient."

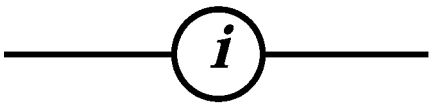
These provisions will have to be interpreted in the light of the test described by the Article 29 Working Party.

The implementation of GLB fails to meet this German law test for several clear reasons. To name some major discrepancies: firstly, as described above, GLB only governs the *disclosure* of data and does not require notification of how the collector, its affiliates or third parties will *use* the information. Therefore, GLB does not efficiently relate the collection, processing and use of the data, to the purpose, the intended use or to a particular data subject. The limitation of the use of personal data is an important principle of German data protection law and expressly mentioned in Section 4(b) paragraph 3 of the BDSG.

Secondly, GLB does not contain clauses on data quality and relevancy. There are no norms for the relevance of the information collected, its currency or reliability. And finally GLB does not stipulate extensively the data subject's right to access the data, to rectify inaccurate information and potentially to object to the processing.

CONCLUSION

For these reasons, it is unlikely that a German data protection authority will assume that GLB provides an adequate level of protection in the financial sector. Companies transferring personal data from Germany to the US will still have to adopt the Safe Harbor principles or keep using other adequate safeguards, such as the standard contractual clauses of the European Commission. However, in each individual case the DPAs will have to acknowledge that the legislation for the financial sector in the US has moved towards a stricter regulation.



AUTHOR: Dr Jan-Peter Ohrtmann is a lawyer in the Dusseldorf office of Bird & Bird. He can be contacted by e-mail at: jan-peter.ohrtmann@twobirds.com

GRAMM-LEACH BLILEY: For further details see the FTC's website: www.ftc.gov/privacy/glbact

---

Italy's data protection code, continued from p.25

Section 122 states that it is forbidden to use an electronic communications network to either access information on subscribers, or to monitor them. Exemptions allowing access to this data will be covered in a separate code of conduct as provided for in section 133. Section 123 of the code states that subscribers' traffic data should be deleted or made anonymous when it is no longer necessary to keep it. However, for billing purposes, the operator can keep relevant traffic data for a maximum of six months in order to respond to possible complaints.

Another important provision on traffic data, which is in line with European trends, is contained in section 132. This provision reduces the maximum data retention period of traffic data for use in crime assessment and prevention to 30 months.

E-MARKETING

Section 130 relates to unsolicited marketing communications. It states that communications via channels such as e-mail, fax or SMS can be sent only with consent from individuals. However, consent is not required in situations where a company is marketing similar products and services to individuals whose details were collected in the course of the sale of a product or service. In this case, individuals must be adequately informed as to how their data will be processed and be given the right to refuse further marketing information.

CONCLUSION

Italy's new Personal Data Protection Code consolidates, simplifies and harmonises existing provisions, bringing the regulatory system of personal data protection up-to-date and in line with the most recent European legislative trends. Most specific sectors await detailed regulation in the form of codes of conduct, which will be binding as per the code's provisions. The choice to leave the regulation of these sectors to the relevant players will lead to the adoption of rules in line with the specific sectors' needs. Hopefully these provisions will be at the forefront of data processing technologies and respond to the most current needs in data protection regulation.

AUTHOR: Lilly Taranto, MSc in Privacy and Media Regulation, London School of Economics. She can be contacted by e-mail at: lilly_taranto@yahoo.com.

FURTHER INFORMATION: An English translation of the code is available on the Italian data protection authority's website: www.garanteprivacy.it