Financial Data Handling Principles for Banks and Non-Banks

Banks and non-banks collect, use, process, transfer, dispose of and share financial data, including personal data, in the ordinary course of business. GFMA has developed a set of principles in relation thereto which are drawn from international best practice, including the US NIST Cybersecurity Framework and the EU General Data Protection Regulation (GDPR). The NIST Cybersecurity Framework consists of voluntary standards, guidelines and best practices to manage cybersecurity-related risks. The GDPR is an EU regulation on data protection and privacy which applies in Europe and to non-European firms which offer services to individuals in Europe or monitor individuals in Europe.

These principles are voluntary and not legally binding. They do not constitute legal or other advice.

1. Limit the collection, processing and use of personal data to that which is necessary to accomplish a lawful purpose.
2. Provide a reasonable means for data subjects to check and correct the accuracy of personal data held about them.
3. Limit access to personal data to users on a need to know basis and monitor such access on a periodic basis.
4. Protect against unauthorized or unlawful access to, or removal of, personal data using a risk-based approach with reasonable technical and procedural measures.
5. Use a risk-based approach to employ appropriate safeguards, such as encryption, when transferring data.
6. To the extent reasonably feasible, securely eradicate, dispose of, or destroy personal data without delay when there is no longer a valid business, legal or regulatory purpose to retain it.
7. Only provide personal data to external entities with data protection policies and procedures consistent with these principles or where required by law.
8. Implement a monitoring programme designed to identify and resolve data security issues, gaps or weaknesses; and remediate any issues found.
9. After establishing that a loss or compromise of personal data has occurred, promptly notify regulators and individuals who have been substantially harmed.
10. Work together with other financial institutions and regulators in exchanging views and intelligence with a view to continually improving data security.

Note: Terminology in this field can be confusing. The term “data protection” in Europe broadly equates to the US term “data privacy”; and the term “data processing” in Europe broadly encompasses the US concepts of both “data collection” and “data usage”.

The Global Financial Markets Association (GFMA) brings together three of the world’s leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London and Brussels, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, visit http://www.gfma.org.