JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 3(2012)

The Data Protection Compliance Program

Rosario Imperiali
Member of EPA's Scientific Advisory Committee
European Privacy Association
rosario.imperiali@imperiali.com

On January 25, 2012, the EU Commission set forth a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. The Draft Regulation, once approved by the European Parliament and the Council, should replace Directive 95/46/EC (the "Data Protection Directive") which has been criticized for being laden with loopholes and legal uncertainty. A stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market as well as put individuals in better control of their own data, is intended to prevent fragmentation in the way personal data protection is implemented across the Union. The proposed regulation would essentially create a single, unified law that applies to all 27 member states. It sets forth a new legal regime which would foster protection for individuals based on a complete compliance program companies must demonstrate to fulfill.

1. Synthesis

The proposed EU Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] aims to introduce in the management aspect a legal model so that the use of personal data is highly protected. The regulatory action, entrusted at a future EU Regulation with direct effect in Member States, requires the adoption of a model of management and control, where you can see the appeal to the cycle of continuous improvement, already present in quality processes.

The data protection compliance program is conceived by the combined reading of the following provisions of the proposed Regulation:

Procedures and mechanisms for exercising the rights of the data subject
Article 12 obliges the controller to provide procedures and mechanism for exercising the data subject's rights, including means for electronic requests, requiring response to the data subject's request within a defined deadline, and the motivation of refusals.

Responsibility of the controller

Article 22 takes account of the debate on a "principle of accountability" and describes in detail the obligation of

[1] 2012/0011 (COD)

responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance.

Data protection by design and by default

Article 23 sets out the obligations of the controller arising from the principles of data protection by design and by default, by implementing "appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation".

Documentation

Article 28 introduces the obligation for controllers and processors to maintain documentation of the processing operations under their responsibility, available to the Supervisory Authority upon request, to ensure the verification of the effectiveness of the measures in order to demonstrate compliance.

Security of processing

Article 30 obliges the controller and the processor to implement appropriate measures for the security of processing, extending that obligation to processors, irrespective of the contract with the controller.

Notification of a personal data breach

Articles 31 and 32 introduce an obligation to notify personal data breaches to the Supervisory Authority and to the data subject within a short time frame.

Data protection impact assessment

Article 33 introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations.

Prior authorisation and prior consultation

Article 34 concerns the cases where authorisation by, and consultation of, the Supervisory Authority is mandatory prior to the processing "in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects".

Data protection officer

Article 35 introduces a mandatory data protection officer for both public sector and private sector, for large enterprises or where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring. Article 36 sets out the position of the data protection officer. Article 37 provides the core tasks of the data protection officer.

Certification

Article 39 introduces the possibility to establish certification mechanisms and data protection seals and marks.

It will be important, therefore, that companies operate a "cultural leap", from an approach of "respect of formalistic compliance" to a policy of daily "conformity behavior".

2. The Plan

The proposed EU Regulation sets forth a new legal regime for the protection of personal data based on a complete compliance program. The proposal aims at introducing a legal model in the corporate management structure in order to ensure that personal data are processed in an environment, which provides adequate safeguards. Instead of limiting its intervention to principles and rules of law, the legislator from Brussels has narrowed the entrepreneurial freedom of choice in the management policy, by setting out specific legal provisions and obligations related to corporate organization in order to handle personal data adequately. An overall reading of the document clearly shows the intention of depicting an organic personal data handling system, imposed on data controllers.

This compliance program is structured on the PDCA model cycle (Plan, Do, Check, Act of the known Deming's wheel), which is at the basis of the ongoing programs for the control and continuous improvement of processes and products, such as those for quality certification.

The parallel should not be of surprise, considering that the scope of both the Directive 95/46 and of the subsequent proposed Regulation is to ensure a high level of safeguards to personal data processed by third parties. This goal can be better achieved by a management method applied to the whole personal data handling process. The structure of the proposed data protection model can be summarized as follows:

Plan – The objectives are set out by principles and rules contained in the law together with the obligation of responsibility of the controller to be compliant (so called accountability principle). The objectives established by controllers (through the corporate commitment stated in the data protection policy) which are interpreted according to the characteristics of the controllers' data processing environment, are then translated into processes necessary to deliver results according to the expected goals (high data protection standards). This requires knowledge and understanding of when and how data protection law affects the company, identification, duties and authorities of key persons for everyday processing operations and compliance oversight as well as awareness of corporate internal controls that have been established and implemented to ensure compliance.

Do – The implementation of the plan is ensured by the adoption of organizational measures made of an organizational chart according to data protection legal roles and instructions, description of company's data protection functions and of any management and control structures for implementing and tracking compliance (e.g. methodology used to identify type of processing and categories of data the company handles, from the time the company receives data to the time the company transmit them to other controllers).

Check – Establishment and implementation of corporate internal controls to ensure compliance as well as maintenance of documentation of the processing operations – as a record keeping system and as evidence of compliant diligence - considering that the burden of proof stays with the controller. Independent supervision is provided also through the mandatory institution of the data protection officer for large enterprises and in case of systematic monitoring. It involves the possible establishment of certification mechanisms and data protection seals and marks, to enhance transparency and compliance; as well as regular periodical audits by persons reporting to top management, to ensure integrity of data protection compliance program.

Act – In conclusion, the adoption of technical measures is not only limited to the traditional security safeguards, but also includes innovative tools aimed at facilitating the protection of personal data (by design or by default). By doing so, the expectation of a high level of protection for personal data is ensured in the phases of both product and services design and of implementation of usage options of same (by default). Thus citizens become protected before coming to the market.

The action plan get completed by written statements and procedures to foster employee discipline, by process to ensure education, training, and provision of guidance to all employees involved, as well as finally, by the emphasis appointed on importance of compliance, to avoid jeopardizing corporate business and heavy sanctions against the data controller and responsible individuals.

3. Conclusion

For a wise company that intends to have the goal of compliance with data protection according to an implemented path that will create less organizational and economic impact we must bear in mind the following aspects:

1. promote the "cultural leap", from an approach of "respect of formalistic compliance" to a policy of daily "conformity behavior".
2. operate synergies and integration between the model of data protection and other models of management and internal controls (e.g. the organizational model for anticorruption, that on job security, the model anti-money laundering, one for the tracking of waste and environmental impact, the eventual company's quality systems).
3. implement an integrated compliance training program for staff involved.
4. set up a control room of compliance, defined as a functional unit capable of monitoring the effective and efficient law enforcement in its various forms (anticorruption, data protection, job security, information security, etc.) on behalf of business operations.
5. provide accurate reports and information flows between the control room of compliance and the roles of legal compliance (anticorruption internal supervisor, data security officers, data protection processors, auditors and internal control bodies, etc.).

* * * *

Cite as: Imperiali, Rosario. *Data Compliance Program*, Journal of International Commercial Law and Technology, vol.7 Issue 3 (July, 2012)