Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 5 >>> MAY 2016

European Accountability and U.S. Compliance Principles

By Winston Maxwell and Sarah Taïeb, Hogan Lovells

Winston Maxwell is a partner at Hogan Lovells LLP in Paris. He was appointed in 2014 to the French National Assembly's Commission on Digital Rights and contributed to the French Counseil d'Etat's 2014 report on fundamental rights in the digital age.

Sarah Taïeb is a senior associate at Hogan Lovells LLP in Paris, and is the International Association of Privacy Professionals' Young Privacy Pro Leader in the Paris area.

U.S. Sentencing Guidelines Define 'Effective Compliance Programs'

The term accountability often refers to compliance programs: An organisation with a robust data protection compliance program is said to be "accountable." Compliance programs have become commonplace as a result of the U.S. government's 1991 Sentencing Guidelines.[1] The U.S. Sentencing Guidelines provide for reduction in federal sanctions when companies have implemented an "effective compliance and ethics program." The Sentencing Guidelines apply to all kinds of federal offenses, including environmental law violations, corruption, antitrust violations, and fraud.

To establish an "effective compliance and ethics program," companies must implement standards and procedures to prevent and detect criminal conduct. The

[1] U.S. Sentencing Commission Guidelines, Sentencing for Organizations, 56 Fed. Reg. 22,762 (1991), as modified with effect from Nov. 1, 2004, Fed. Reg. 28,994-29,028 (May 19, 2004).

company's board must be knowledgeable about the content and operation of the compliance and ethics program and exercise reasonable oversight with respect to its implementation.

One or more specific individuals within senior management must be assigned overall responsibility for the compliance and ethics program, and other individuals must be delegated day-to-day responsibility for the program. Those individuals must be given adequate resources, appropriate authority and direct access to the board or an appropriate subgroup of the board.

The company must put into place training programs, audits and mechanisms for reporting violations. It must ensure that employees have incentives to comply with the program, and that violations are punished. The Sentencing Guidelines led to the emergence of the position of Chief Compliance Officer (CCO) in most large corporations. After the Enron scandal, the U.S. Congress reinforced compliance obligations with the adoption of the Sarbanes-Oxley Act[2] , and reinforced them yet again with the adoption of the Dodd Frank Act[3] .

The 2013 OECD Guidelines and ISO 29100

The 2013 revisions to the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines[4] require that companies put into place a "privacy management programme." The management programme must, among other things, provide for appropriate safeguards based on privacy risk assessment, and include plans for responding to inquiries and incidents. The company must be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority. Finally, the company must "provide notice, as appropriate, to privacy enforcement authorities . . .where there has been a significant security breach."

ISO standard 29100 also contains detailed rules on accountability, requiring documented policies, the appointment of a data protection officer (DPO), appropriate safeguards when transferring personal data to third parties, training, internal complaint handling procedures, and data breach notification obligations. According to the ISO standard, "establishing redress procedures is an important part of establishing accountability."

The European Approach to Accountability

Both the 2013 OECD Guidelines and ISO 29100 share many points in common with the 1991 U.S. Sentencing Guidelines. What about Europe? In 2010, the Article 29 Working Party issued an opinion on accountability, listing measures that companies should take to ensure compliance with the EU Data Protection Directive (95/46/EC), and to demonstrate such compliance.[5] The Article 29 Working Party opinion defines accountability as putting the emphasis "*on showing how responsibility is exercised and making this verifiable.*"

Binding Corporate Rules (BCR) provide a good example of European accountability in action. BCR are an internal code of practice designed to ensure that an organisation treats personal data coming from Europe in a manner consistent with European privacy norms. BCR require documented policies, an appropriate governance structure, training and audits.[6]

Accountability à la Française

In 2015, the French data protection authority (CNIL), published a "data protection governance standard."[7] The standard is divided into 25 requirements relating to the existence of policies for the protection of personal data and to the appointment of a DPO, with enhanced powers and responsibilities.

Entities complying with CNIL's 25 requirements can obtain a privacy governance seal from CNIL. The governance seal is currently the "gold standard" of accountability in France, and so far few companies have obtained it. Appointing a DPO with enhanced powers and responsibilities goes to the heart of CNIL's governance seal. To obtain the seal, a company must have a DPO with responsibilities in line with the forthcoming European Union General Data Protection Regulation (GDPR).

The data protection officer informs, provides guidance and monitors the application of the principles of the EU General Data Protection Regulation.

CNIL standard requires that the DPO report to a member of the company's senior management body. The company must provide the DPO with regular training, a specific budget and sufficient means to perform his or her task. The DPO must be consulted on all projects involving processing of personal data and is responsible for conducting training and internal awareness actions. The DPO must conduct a legal analysis of data processing operations, formulate recommendations and propose a preventive action plan and/or corrective actions. He or she must ensure that a privacy risk analysis has been conducted for significant data protection operations.

---

[2] Sarbanes Oxley Act (SOX) 18 U.S.C. § 1514A

[3] Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law 111-203, 124 Stat. 1376 (2010)

[4] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, 1980, updated in 2013 (13 WDPR 31, 9/20/13).

[5] Opinion 3/2010 on the principle of accountability, WP 173 of July 13, 2010 .

[6] CNIL's Guide on BCR "*Tout savoir sur les BCR.*"

[7] Deliberation No. 2014-500 of 11 December 2014 on the Adoption of a Standard for the Issuance of Privacy Seals on Privacy Governance Procedures .

   ISSN 1473-3579

Accountability and the GDPR

Like the OECD Guidelines, the GDPR[8] requires that data controllers be able to demonstrate compliance with the general principles of processing personal data under the GDPR. Demonstrating compliance can be done by putting into place appropriate technical and organisational measures, implementing policies for the protection of personal data, and adopting codes of conduct and certification mechanisms.

Under the GDPR, the function of DPO will be significantly reinforced. The DPO must be selected for his or her expertise. He or she must report to the highest level of the company's management. The DPO occupies a strategic position within the company, like the CCO under the U.S. Sentencing Guidelines. He or she must be involved in all issues relating to the protection of personal data within the company, in particular by organizing training and a network of persons aware of the data protection issues within the company. The DPO must ensure that audits are implemented and must contribute to the preparation of impact assessments.

The company must make available all resources and information that are necessary in order to conduct these tasks as well as the means for the DPO to benefit from continuing education. The DPO is a point of contact for supervisory authorities and must cooperate with them. He or she informs, provides guidance and monitors the application of the principles of the GDPR.

The obligation to "take account" of a company's compliance measures suggests that regulators should consider accountability as a mitigating factor, just as in the U.S. Sentencing Guidelines.

Will Accountability Reduce Sanctions Under the GDPR?

The GDPR will significantly increase the level of administrative sanctions for data protection violations. Sanctions can potentially reach 4 percent of the global turnover of the data controller. When applying sanctions under the GDPR, regulatory authorities will have to take into account the measures taken by the data controller in order to ensure compliance (technical and organisational measures taken to prevent or mitigate damages, the level of cooperation with the supervisory authority, the implementation by the company of codes of conduct and/or certification procedures).

The GDPR is less explicit than the U.S. Sentencing Guidelines, in that the GDPR does not affirmatively state that an effective compliance program will necessarily reduce sanctions. But the obligation to "take account" of a company's compliance measures suggests that regulators should consider accountability as a mitigating factor, just as in the U.S. Sentencing Guidelines.

The Three Facets of Accountability

Accountability today is a three-faceted prism:

First, accountability consists of a form of normative co-regulation, where the regulator delegates to the company the responsibility for developing internal compliance rules that take into account the specificities of the company. The company will always have more information than the regulator about the company's own operations, and is in a better position to create effective and adapted rules. Detailed rules developed by a regulator may miss their mark due to inadequate information.

The DPO will have an important role in developing these internal rules. Bamberger and Mulligan[9] refer to the chief privacy officer (CPO) as a "norm entrepreneur" because of the CPO's role in developing normative frameworks for the organization. The new role of DPO under the GDPR will incorporate this "norm entrepreneur" function.

Data protection authorities may guide companies in the creation of this internal normative framework. The CNIL, for example, recently created compliance recommendations for certain professional sectors, such as insurance, which are designed to help companies put together their own internal compliance frameworks.[10]

Second, accountability consists of effective monitoring and enforcement of the rules. This can be done by training staff, motivating employees to adopt a "culture of compliance," as well as implementing mechanisms to detect non-compliant activities through audits, internal investigations, and whistleblowing systems. A governance system is necessary to avoid conflicts of interests: the persons in charge of verifying and enforcing compliance cannot report to the persons in charge of the relevant business operations that are being audited. The role of the DPO is particularly important here. By reporting to the highest management body of the company, the DPO can in theory maintain his or her independence from the various business units where processing is taking place, thereby avoiding conflicts of interest.

Third, accountability consists of creating trust among stakeholders, including customers, employees, data subjects and regulators. The protection of personal data is now mainly defined by what clients of the company expect in relation to the processing of their data.[11] As mentioned by the Article 29 Working Party, "*Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed.*" Compliance, and the ability to demonstrate compliance to third parties, help companies increase third party trust.[12]

[8] 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) [first reading]—Analysis of the final compromise text with a view to agreement, 15039/15, 15 December 2015 .

[9] Kenneth A. Bamberger and Deirdre K. Mulligan, Privacy on the Books and on the Ground, 63 Stan. L. Rev. 247 (2010).

[10] CNIL, Les packs de conformité: un succès grandissant, 21 October 2014.

[11] Bamberger & Mulligan *supra* note 9.

[12] CNIL, Activity report of 2014, p.42.

Accountability Certification Mechanisms

Under the GDPR, accountability will depend in large part on norms developed by national regulatory authorities as part of future certifications mechanisms. The GDPR puts considerable emphasis on certification mechanisms, which will be set up at a national or EU level. The CNIL is a leader here, having already developed a privacy governance seal for companies that implement accountability programs meeting the CNIL's governance criteria. The CNIL's governance standard incorporates the key elements of accountability required by the GDPR, and could serve as a model for a future European accountability certification mechanism.

Accountability and Fiduciary Duty

So was accountability born in the U.S.? Probably not. While we can see a family resemblance between European examples of accountability and the U.S. Sentencing Guidelines, the history of accountability is much older. Accountability is linked to the equitable concepts of fiduciary duty and rendering accounts, which were born in England several centuries ago. But the modern version of the "effective compliance program" has its genesis in the U.S., and will no doubt inspire how data protection governance programs are built in Europe.

   ISSN 1473-3579