Data protection compliance policies

Steven De Schrijver and Jan Dhont, Lorenz

www.practicallaw.com/5-385-8628

This chapter explores the key issues for companies operating in more than one jurisdiction (both inside and outside the EU) that intend to set up a data protection compliance system. In particular, it examines:

- Reasons for data protection law compliance.
- Legal requirements.
- Carrying out a data protection audit, including:
  - pre-audit stage;
  - performance of the audit; and
  - assessment stage.
- Establishing a data protection system, including:
  - appointing a data protection officer;
  - privacy policy;
  - internal register of databases;
  - contractual clauses;
  - fair processing notices and rights of data subjects;
  - international data transfers;
  - registration requirements; and
  - data security.
- Implementing the compliance system.
- Maintaining compliance.

REASONS FOR DATA PROTECTION LAW COMPLIANCE

Companies are processing ever increasing volumes of employees', customers' and suppliers' personal data. The storage and processing of personal data have become so ubiquitous in modern businesses that failing to observe data protection law can create a minefield for companies. In particular, businesses operating or processing personal data in several jurisdictions face a major challenge in ensuring compliance, not least because of the diversity of the rules on data protection.

The creation, handling, storage and transfer of personal data have increased so rapidly that the EU has deemed it necessary to put safeguards in place to protect the privacy of persons. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) lays down a framework for the protection of personal data. Because the Directive is only a framework which is subsequently transposed into the national laws of all EU member states, the rules applicable in each member state differ to some extent. Further, more and more jurisdictions outside the EU have enacted privacy laws, including Norway, Switzerland, Argentina, Canada and Japan.

More than ten years after the adoption of the Data Protection Directive, companies in the EU can no longer afford to claim ignorance or innocence, as non-compliance is pursued more severely. Breaches of data protection law can lead to the imposition of sanctions, including fines or, in serious cases, even imprisonment. Data protection authorities may also be entitled to order companies to give up or modify non-compliant data processing operations, causing costly business interruptions. Further, data protection authorities have recently been calling for more powers. For example, the UK data protection authority has sought more inspection and enforcement powers following a series of high profile data security breaches.

Even apart from the sanctions, compliance should figure high on the agenda of many businesses because of the increased sensitivity of individuals to their privacy. Public awareness is fuelled by press reports about serious data security breaches which put personal data at risk. As a result, individuals have begun to exercise their rights under data protection law more often. For instance, disgruntled employees or consumers can lodge complaints with data protection authorities and claim damages. Increasingly, employees have also successfully invoked breaches of data protection law in civil or employment law proceedings, for example, to challenge their dismissal.

Companies operating in the EU also risk significant damage to their reputation if they do not comply with high levels of data protection. Bad publicity can be extremely harmful for any business that relies on customer goodwill and the harm from "naming and shaming" in the press or in publications such as data protection authorities' annual reports has the potential to harm a company even more than facing sanctions and damage claims.

However, data protection compliance is not only about risk minimisation; it can bring about real benefits as well. It can increase employee or consumer confidence and trust and can be used as an additional marketing and sales tool, enhancing brand image. It

can also assist information management by avoiding duplications, thereby freeing valuable server space and ensuring that databases are up to date and fully usable. Finally, it reminds companies of the real need to apply strict security rules to protect not only personal data, but also company data and business secrets in general.

LEGAL REQUIREMENTS

Under EU data protection laws, responsibility for ensuring the legality of the processing of personal data lies in principle with the controller, that is, the (legal) person who alone or jointly with others determines the purposes and means of the processing of personal data. The controller is also the person who will be held primarily liable for any breaches of data protection law. In most cases of processing personal data of employees, customers or suppliers, companies will be considered to be the controller of the respective personal data and therefore liable to ensure data protection law compliance.

While some countries have issued guidance in relation to particular data protection law related issues, in general, the controllers are left to determine how best to ensure compliance.

The first and best way to determine whether and to what extent an organisation is in compliance with data protection law is to conduct an audit. Indeed, the starting point for developing a data protection compliance system should be to establish the status quo of an organisation's data processing activities. This is a prerequisite to developing appropriate compliance tools and setting up and maintaining an effective system suitable to the particular organisation.

CARRYING OUT A DATA PROTECTION AUDIT

A data protection audit consists of a systematic and independent examination of the scope of an organisation's data processing activities and an assessment of the existing level of compliance.

The exact scope of a data protection audit depends on an organisation's needs and requirements, including the audited organisation's expectations in terms of the level of compliance it wants to achieve, the timeframe and the budget.

A data protection audit is a time-consuming task, which usually involves meeting and interviewing various key people. It is very important that the audit is carried out in a timely fashion, as outcomes will inevitably be inaccurate if different parts of the organisation are looked at over different time periods, during which factual and legal situations may have changed.

For this reason, an organisation may decide to call on third party auditors rather than carry out the audit itself. While internal auditors will have a better knowledge of the structure and functioning of the organisation, external auditors may be more experienced in carrying out such audits and may be able to devote more time and resources. Additionally, external auditors are more likely to approach the matter with an open, independent and objective mind.

Any audit needs to take the structure of the organisation into account. For example:

- Is the audited organisation a single legal entity or does it belong to a group of companies?
- What business units exist and what functions do they have?
- Does the audited organisation have a matrix structure?
- How are the data processing activities structured? In particular, have certain functions been centralised or are they carried out locally? Are databases shared among business units or legal entities?

Although each audit will be different, there are three main audit phases, discussed in detail below:

- Pre-audit stage.
- Performance of the audit.
- Assessment stage.

Pre-audit stage

The outcome of an audit depends, to a large extent, on the quality of the input. The pre-audit stage is therefore very important; the audited organisation must set aside the necessary resources in terms of manpower and time. The better the preparation, the more smoothly and swiftly the audit can be carried out, and the more accurate the audit findings will be.

As a first step, the audit scope should be defined. A bigger organisation with a presence in several countries will need to determine which countries' data protection laws govern its data processing activities. Further, it must decide whether the audit will cover:

- All business units or only some of them (typically at least human resources, IT or marketing).
- All data processing activities or only particular key processes or areas that have been identified as (potential) high risk areas or business drivers.
- The whole group or only certain legal entities that are more important from a business perspective or are considered to be representative. However, even where only some companies are audited, the compliance solution needs to consider the data flows within the entire group as well as the existence of global or shared databases and the (intra-group) outsourcing of certain processing activities (for example, the operation of a central IT Helpdesk).

Once the scope of the audit has been defined, the key business drivers, processes and personnel within the audit scope must be identified. This information is essential for drawing up an accurate audit schedule that determines which departments and personnel will be involved in the audit process, in which order and within what timeframe.

It is also very important at this stage to obtain the support of senior management and the staff members involved in managing the audit and providing the audit responses. This is necessary to make sure that the audit is taken seriously. Employees should be informed in advance of the audit and its purpose and told to make all information available.

Next, a benchmark against which data protection law compliance will be measured must be defined. For this purpose, up-to-date sta-

tus reports on the relevant national data protection laws should be prepared. These status reports will be used as an information and reference tool during the audit and thereafter, as they can be easily updated to keep the organisations' compliance efforts current. Although their content may differ based on the scope of the audit, status reports will usually set out the main elements and rules applicable to data protection in a particular jurisdiction, including:

- Definitions of key terms, such as personal data.
- The main rules applying to the processing of personal data, including the rules on the lawfulness of data processing, data quality and international data transfers.
- Information obligations vis-à-vis data subjects.
- The rights of data subjects.
- The rules applicable in case of the use of processors, that is, persons who process personal data on behalf of the controller.
- Data security requirements.
- Registration requirements.
- The competent authorities.
- Liabilities, sanctions and judicial remedies.

The status report should also highlight any particularities of the laws and their application or interpretation by the competent authorities in the relevant jurisdiction.

Although an organisation may decide to carry out an audit based only on interviewing key staff members, the use of written audit questionnaires is recommended to ensure that the audit is conducted to the same standard in terms of quality and depth of investigation across the organisation. The questionnaires, which must be adjusted to the audit scope and take into account the structure of the organisation, should be designed to establish the scope of data processing and the existing level of compliance. Typically, the questionnaires should ask for information concerning:

- The legal entity or business unit being audited.
- Existing policies, procedures, contracts and compliance measures as regards data protection.
- Databases and software applications as well as data processing activities.
- The categories of personal data (including sensitive data) being processed.
- The categories of data subjects whose personal data is being processed.
- The controllers, processors and any other players.
- The data flows within and outside the audited organisation, and inside and outside of the EU.
- The technical and organisational security measures.

Completion of the audit questionnaires usually requires a certain understanding of data protection law. For this purpose, the status reports can be circulated. However, it is often useful to accompany the audit questionnaire with written audit guidance providing an explanation of key terminology, the purposes and importance of the audit and the purpose of each audit question. Such guidance will also set out the minimum standard for responses and may include examples. Pre-audit training can further increase the value of the audit process and help to avoid a flawed or delayed audit process.

Performance of the audit

The actual audit mainly consists of completing the audit questionnaires and providing supporting documents. Reasonable time and effort is required to provide comprehensive and meaningful responses. In particular, it must be ensured that the responses are sufficiently concise, complete and clear, and that they are prepared by the right people.

The responses to the audit questionnaire must be carefully reviewed to identify any gaps or contradictions in the responses provided. In some cases, further clarification or additional information will need to be sought.

Meeting and interviewing key personnel may facilitate the process of completing the audit questionnaires properly and can also give auditors an opportunity to check whether the answers that have been provided to the questionnaire are actually correct and complete.

Assessment stage

Once properly completed, the questionnaire responses, including any supporting documents, must be reviewed and assessed under the applicable national data protection laws. The status reports can facilitate this process. By the end of the review, all shortcomings and weaknesses of the organisation's data protection law compliance should have been identified.

Areas of non-compliance should then be prioritised according to their seriousness and described in detailed compliance reports which should also set out the possible remedies. The compliance reports can also be used in presenting the audit findings to senior management whose support will be required for the implementation of the compliance tools.

Once the compliance reports have been circulated and reviewed by the organisation, there should be a meeting to discuss the audit results, remedies and available options as well as their pros and cons. After the organisation has decided on the actions it wants to take, the compliance reports should be converted into concrete action plans that provide a brief summary and ranking of the main areas of concerns. The action plans should identify the following for each compliance issue/task:

- Proposed action.
- Responsible party.
- Due date.

The action plans therefore provide an easy-to-use checklist for the organisation and allow progress to be easily monitored.

ESTABLISHING A DATA PROTECTION COMPLIANCE SYSTEM

The audited organisation will need to establish a data protection compliance system to appropriately address the areas of non-compliance and risks that were identified in the compliance reports. In addition, the system must ensure that any future practices are implemented in a compliant manner.

The method and means best suited for a particular organisation to achieve compliance will depend, to some extent, on the applicable data protection laws and the audit findings. However, account must also be taken of the organisation's structure and requirements as well as the culture and business practices in different jurisdictions. The company must also decide whether to adopt a single standard approach across the group (typically the highest standard existing) to ensure uniformity or whether jurisdiction-specific approaches would be more appropriate.

A compliance solution will typically combine several methods and tools. A data protection compliance system may, for instance, require an organisation to change certain data processing activities, to put in place certain procedures or processes or to conclude particular agreements to ensure the lawfulness of all its data processing activities. Some areas of non-compliance will require action to be taken at group level (for instance, in relation to international data transfers), while others will be country- or entity-specific (for example, notifications), though some sort of local action is likely to be required in all cases.

The key element of any data protection compliance strategy is, however, the allocation of responsibilities, backed up by certain organisational measures and complemented by a range of actual compliance measures.

Appointing a data protection officer

Except for Germany, none of the national data protection laws in the EU legally require companies to appoint a data protection officer (DPO), though some of them provide for the possibility. However, the co-ordination and implementation of a data protection compliance system can be significantly aided by the appointment of a DPO, even where this is not required by law. Companies are well advised to appoint someone to assume responsibility for overseeing data protection law compliance. A DPO can also act as a contact person, monitor and supervise all data protection activities, drive the data protection compliance strategy and provide training to staff members.

In large organisations or where data processing activities or processes are particularly complex it may be necessary to appoint other individuals within the organisation to assist the DPO in carrying out his tasks.

Unless the national data protection law contains provisions to this effect (as in Germany), it is recommended that the organisation clearly defines the competences, powers and duties of the DPO. A DPO should act independently and with sufficient authority. It may also be necessary to impose reporting and other obligations on staff members to assist the DPO in carrying out his tasks.

Privacy policy

Another key element of a data protection compliance system is the drawing up and implementation of policies that set out the procedures and steps that each business unit of an organisation must apply with respect to data protection. It is good company practice to adopt a privacy policy that provides the basic framework for all data protection compliance activities. It should set out the basic principles and procedures governing the processing of personal data. It is therefore a reference tool for employees and others which increases transparency and trust in the workplace. A privacy policy also conveys a clear signal that data protection law compliance is taken seriously and may help to demonstrate an organisation's commitment.

To ensure compliance, the privacy policy should reflect the corporate culture and language of the organisation concerned. A privacy policy is usually high level and needs to be complemented by other more specific policies and procedures concerning, for example, data security or data retention. Existing policies and procedures, including on human resources, information security and computer use practices, will need to be checked against the relevant parts of the privacy policy to ensure consistency.

Any such policies must be properly communicated, possibly supported by training, to ensure that the staff members are aware of the rules and understand them. Compliance with the policies must be regularly monitored and breaches sanctioned.

Internal register of databases

The audit should have identified all the organisation's data processing activities within the scope of the audit, including all:

- Databases that include personal data.
- Categories of personal data that are being processed.
- Players, including the data subjects, the controllers and the processors.
- Data flows within and outside the audited organisation, including disclosure to third parties and international data transfers.
- Existing contractual clauses, policies, notifications and authorisations.
- Existing security measures.

In some jurisdictions (such as Germany) keeping an internal register is mandatory. However, irrespective of whether such a statutory obligation exists, organisations are well advised to keep an internal register of databases and to regularly update it. Such a register does not only constitute an important source of information for the development of the actual compliance measures, it also facilitates the management and maintenance of the data protection compliance system (including the preparation of notifications or responses to data subjects' requests).

Contractual clauses

The audit will have identified relevant relationships with third parties, including data processors and data controllers. The audited organisation may want to put in place contractual arrangements with these third parties to ensure compliance with data protection law.

Where controllers use data processors, the national data protection laws lay down certain requirements, including a written processor agreement.

Clauses within employment contracts may also be required, or at least advisable, to ensure that personal data handled by employees is kept confidential. Terms and conditions of employment agreements may need to be amended in this respect.

Organisations should also obtain contractual assurances from third parties from whom they receive personal data to ensure that the data has been lawfully collected and can be used for the intended purposes.

A contract management system should be set up to identify any third party or supplier/customer contracts which needs to be reviewed and possibly revised. Further, the organisation needs to ensure that the appropriate clauses are inserted into all new contracts.

Fair processing notices and rights of data subjects

Under data protection laws, certain information must be provided to data subjects, such as the identity of the controller and the purposes for which the personal data will be processed. This information must usually be provided at the time of the collection of the data.

Existing notices and forms may need to be amended and so-called fair processing notices developed to ensure that all the required information is provided. Processes may also need to be implemented to ensure that this information is provided at the right time.

Besides complying with their information obligations, organisations will also need to implement procedures to enable data subjects to effectively exercise their rights. The internal register of databases can assist the organisation in responding to data subject requests within the applicable time periods.

International data transfers

Where personal data is transferred abroad, controllers must ensure that this can be done lawfully. Basically, the national data protection laws implementing the Data Protection Directive prohibit the transfer of personal data to any third countries outside the EU that do not provide an adequate level of protection. Very few jurisdictions have been officially recognised by the European Commission as providing an adequate level of protection. These countries are: Argentina, Canada (subject to certain limitations), Guernsey, the Isle of Man, Jersey and Switzerland as well as data transfers to US companies that have registered with the so-called US Safe Harbour scheme.

If an organisation intends to transfer personal data to any other third country outside the EU or to an organisation in the US which is not Safe Harbour-registered, it must implement adequate safeguards to protect the personal data transferred. Such safeguards can be provided, for example, by means of contractual clauses (such as, on the basis of one of the three sets of standard contractual clauses which the European Commission has adopted) or, in case of intra-group data transfers, by means of binding corporate rules. The organisation will also need to comply with any registration requirements applicable to international data transfers.

Registration requirements

Many audits show that companies do not comply with existing registration requirements. The data protection laws provide for prior notification requirements (subject to exceptions). In some cases the data protection authorities will carry out prior checking of notified processing. In other cases the processing can only begin once the data protection authority has granted authorisation (often in case of the processing of sensitive data or international data transfers).

The audit should have identified all databases and processes that require notification to, prior checking by or authorisation from the relevant data protection authorities. It should also have been determined whether these registration requirements have been met. Where this is not the case and additional registration is required, all particulars required for registration will usually have been collected in the course of the audit.

The relevant notifications and/or authorisation requests will need to be prepared and submitted to the relevant authorities. It should be noted that the registration requirements and procedure have not been harmonised in the EU and therefore differ from country to country. A co-ordinated approach among different departments and legal entities may be required in relation to central databases or certain data processing activities, such as international data transfers, which may require action to be taken at group level so as to ensure uniformity of approach.

Data security

Under the national data protection laws implementing the Data Protection Directive, adequate organisational and technical security measures must be taken to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and all other unlawful forms of processing.

Although companies have typically implemented a range of security measures, in particular in relation to IT security, these measures are often aimed at company data and business secrets and do not always cover personal data. Therefore, additional security policies may need to be established or existing policies amended with respect to personal data. There should also be a system ensuring that compliance with the policies is monitored and security breaches are brought to the attention of the DPO and the managers in charge of security so as to allow for remedial action to be taken in due time and to prevent similar breaches from happening in the future.

In addition, more specific security measures may be needed, including:

- Physical access control, which aims to prevent unauthorised persons from gaining access to data processing systems. This may include measures to secure the premises (for example, securing entries and exits) as well as measures within the building (for example, alarm systems and restricted access to server rooms).

- Control of use and access to data, which aims to protect data processing systems from unauthorised use. Persons entitled to use a data processing system must only have access to the specific personal data they are authorised to use, and safeguards must be put in place which prevent personal data from being read, copied, modified or removed without authorisation (for example, by establishing and maintaining an up-to-date user account management system, including user identification and authorisation, and strict password requirements).

- Control of data transmission, which aims to ensure that personal data cannot be read, copied, modified or removed without authorisation during transmission or transport (whether electronic or not). In addition, it must be possible to check and establish to whom the personal data will be transmitted (for example, by keeping logs of data transfers and mobile data carriers, the encryption of electronic data and the control of remote access to databases).

- Input control, which aims to ensure that it is possible to check and establish whether and by whom personal data has been input into data processing systems, modified or removed (for example, by keeping input logs or using audit trails).

- Availability control, which aims to ensure that personal data is protected from accidental destruction or loss (for example, by virus protection, backups and the implementation, regular testing and maintenance of a business continuity and disaster recovery plan).

IMPLEMENTING THE COMPLIANCE SYSTEM

Once the compliance tools described in the previous section have been prepared, they need to be rolled out.

The roll-out of the data protection compliance system needs to be co-ordinated with all the relevant business units of the organisation. For this purpose, the parties that are responsible for each compliance task/issue should be designated and deadlines set for each task to be completed. There should be regular reporting on the status of implementation to allow monitoring of any progress made.

To ensure that the data protection compliance system is being applied in practice, proper communication is necessary so that all employees understand the meaning and purpose of the measures and are applying them properly. Employees must be educated about their responsibilities and the applicable rules.

Therefore, in addition to making the privacy policy and other applicable rules available to the employees in the appropriate format (for example, through inclusion in employment contracts, work rules, staff handbooks, employee notices and the intranet), there should be formal training sessions for employees, including introductory sessions for new staff members and regular refresher courses for long-standing employees. Ideally, the training should be tailor-made with a practical focus on answering the day-to-day questions which may arise in relation to the organisation's handling of personal data and with concrete examples.

Employees should also have the possibility of raising questions and providing feedback in relation to data protection law matters. For this purpose, the organisation should designate a contact person (typically, the DPO) to which employees can turn.

MAINTAINING COMPLIANCE

A data protection compliance system not only needs to be properly implemented but also to be maintained throughout the life of the organisation. Data protection law compliance is an ongoing process. Data processing operations constantly evolve: new databases are created or existing databases are changed, companies switch providers or change their processing operations (for example, by centralising or outsourcing certain data processing activities) or acquire new software or hardware. Each change will demand a corresponding change in the company's data protection compliance system.

The organisation must create a compliance culture so that data protection becomes a consideration in the day-to-day business decisions of the organisation and that any future changes are implemented in a data protection law compliant manner. This will require certain reporting and information obligations. Further, the compliance system and existing compliance tools must be regularly updated, amended and adjusted to keep abreast of all important changes to the processing environment, including changes to the data protection laws themselves.

Regular monitoring is also crucial to ensure that an organisation remains data protection law compliant. There should be regular checks, including occasional audits and spot checks. Breaches, including breaches of data security, must be brought to the attention of the DPO and designated persons, and appropriate escalation procedures must be followed. Any such breaches must also be sanctioned.

CONTRIBUTOR DETAILS

Steven De Schrijver
Lorenz
T +32 2 239 2000
F +32 2 239 2002
E *s.deschrijver@lorenz-law.com*
W *www.lorenz-law.com*

Areas of practice/expertise. Partner Steven De Schrijver is Head of the IT & New Media Department of Lorenz. His practice covers commercial IT law (data protection, e-commerce, software licensing, website development and hosting, technology transfer, digital signature and IT-outsourcing) and technology-related transactions. He regularly publishes and speaks in these fields and is involved in the Computer & Telecommunications Law Commission of the UIA, the IP/IT Commission of AIJA, ITechLaw, and is the Belgian member of EuroITCounsel.

Jan Dhont
Lorenz
T +32 2 239 2000
F +32 2 239 2002
E *j.dhont@lorenz-law.com*
W *www.lorenz-law.com*

Areas of practice/expertise. Partner Jan Dhont is Head of the Data Protection Department of Lorenz. Jan has built a truly international privacy practice advising a broad number of private sector companies as well as public bodies, including DPAs. Jan was previously in-house counsel of the Belgian DPA. He is now an active member of IAPP and often gives speeches on privacy and related matters.