Information Security

KPMG

March 2019

Contents

Introduction

The document set outs the practices adopted by KPMG S.A., a French public limited company, with registered office located at Tour Eqho, 2 avenue Gambetta CS 60055 – 92066 Paris La Défense Cedex, France, the entities that it holds and controls in France, as well as KPMG Avocats, KPMG Academy, KPMG Associés and Fondation d'entreprise KPMG France (hereinafter, 'KPMG' or, jointly, the 'firm') in the area of information security and data protection.

KPMG undertakes to maintain a reliable and secure environment for the personal data and confidential information entrusted to it, and to protect all the private data of its clients, suppliers and third parties.

KPMG views this information and the associated information systems as key assets, essential to its activity. By means of dedicated resources designed to improve practices in the area of information security, KPMG undertakes to identify the risks inherent to its data and to protect against any unauthorised access, loss or non-compliant use. In the context of managing these risks, KPMG has implemented a number of access control and security procedures and assessment tools to analyse its systems and networks.

The firm's policies and practices are communicated to all employees. Information leaflets, awareness campaigns and training programmes support the implementation of these practices. KPMG has made the information security policy available to all its staff. This policy requires employees to use KPMG's IT resources in an appropriate manner, and emphases compliance with the protection of the personal and confidential information of all employees, of KPMG and its clients. Compliance with the policies and procedures relating to information security is assessed on a regular basis.

All KPMG employees comply with the law and adhere to the applicable professional standards and to the ethics requirements imposed by the representative bodies of the professions affected by KPMG's activities (French Association of Chartered Accountants, National Auditing Body, National Council of Bars), by their regulators (French Audit Office Control Board, Accounting Standards Authority, chancellery, National Council of Bars) and by the regulatory authorities of the financial and tax system. Certain regulations are applicable to the firm and its employees, and take account of the specific characteristics of each client (in particular the French Financial Markets Authority (AMF) and Prudential Supervisory and Resolution Authority (ACPR)). Furthermore, all KPMG employees are contractually required to adhere to KPMG's information security policies.

Information security personnel

The team responsible for information security within KPMG is comprised mainly of professionals working in the Risk Management and ITS departments. It is responsible for developing and supporting KPMG's information security practices, through awareness and training activities, participating in the development of applicable standards and assessing information security and risks. By working closely together with the various KPMG business lines, information security professionals develop appropriate standards designed to ensure the security of its information and that of its clients. Through these different activities, KPMG staff have tools and resources that allow them to understand their responsibilities as regards the security and protection of their clients' information.

Information security: Key functions

- Implement policies and support users with regard to the use of KPMG's data, equipment, network and IT systems.
- Establish strategies and standards, and develop security checks to protect the information pertaining to our clients as well as any other information stored in the KPMG systems.
- Provide risk management advice.
- Manage IT security control mechanisms and ensure that they comply with the standards and policies of KPMG International.
- Manage the compliance programme, in particular:
- Report on information security and conduct risk assessment. Facilitate internal control of the ITS department and KPMG offices.
- Understand the impact of new laws and regulations on the IT environment.
- Implement a training and awareness programme to ensure that employees understand their responsibilities as regards the protection of clients, personal data and KPMG.

Policies and standards

Information security

KPMG's information security system is based on a comprehensive array of policies, standards and procedures. These include, in particular:

- Organisation of information security
- Security policy
- Responsibility with respect to property
- Safety of personnel
- Business continuity management
- Physical and environmental security
- Management of information security incidents
- Access control
- System development
- Compliance

Client confidentiality

KPMG staff are subject to non-disclosure policies, in accordance with the code of conduct and Quality and Risk Management manual, and to internal policies on the use and circulation of information pertaining to clients. These policies include confidentiality rules and principles prescribed by law and the regulatory authorities of i) statutory auditors, under Article L. 822-15 of the French Commercial Code, Article 9 of the Code of Ethics for statutory auditors and Article 622-1 of the AMF General Regulations, ii) chartered accountants, under section 140 of the Code of Ethics for accounting professionals, Article 21 of Order No. 45-2138 of 19 September 1945 and Article 147 of Decree No. 2012-432 of 30 March 2012, and iii) lawyers, under Article 66-5 of Law No. 71-1130 of 31 December 1971 and the provisions of the RIN (French national regulations of the legal profession).

In the event that KPMG authorises a third party to use confidential or personal information on its behalf, the contract entered into with said third party shall stipulate that the latter has a duty of confidentiality when using all private and confidential information, in accordance with the policies and practices of KPMG relating to confidentiality in particular.

Controls

Access controls

KPMG has implemented security measures to manage and control physical access to the premises at which information relating to KPMG and its clients is hosted. Access to its offices is limited to authorised personnel using mechanical or electronic access control devices, or to authorised visitors. Furthermore, access to data centres is limited to authorised personnel or visitors, who must sign in and be accompanied throughout their visit.

In accordance with KPMG's information security requirements, the rules governing access to professional applications are defined by the owners of the professional applications and adopt the principle of privilege separation. KPMG's IT security policy provides for the addition, modification and removal of user accounts when employees join KPMG, change role or leave the firm. KPMG staff working outside KPMG offices have access to its network and resources via the virtual private network (VPN) only, by means of a dual authentication procedure. KPMG regularly trains its employees on their responsibilities in the area of information security.

Technical controls

KPMG's information security system provides for several levels of control. The applications used outside the local network are located in a separate and secure part of the IT infrastructure, known as the DMZ (demilitarised zone). Access to the DMZ is restricted, which limits the unauthorised use of the applications hosted in this part of the network.

KPMG has adopted a double firewall system, which can isolate the web applications used outside the local network. Connection points to the KPMG network (such as the internet or dedicated connections) reserved for third parties are protected by a firewall. Any change to the configuration of the firewall is assessed based on the risks involved, in accordance with a specific process. Firewalls are an essential element of the security control mechanism. KPMG's security system also includes several further control systems that help to secure the KPMG network.

During the configuration of personal computers (PC), portable devices, servers, hardware and operating systems, standardised security measures are applied. These measures include: antivirus, full disk encryption, external media encryption, security updates and patches, firewalls, access controls, event monitoring, network security, expiry of access authorisations, management of passwords and warning messages. The firm regularly assesses and improves these security measures in order to apply the prevailing practices in the area of technology and the standards governing its business sector.

Depending on the IT capacities and requirements of our clients, additional technical controls may be implemented upon request, such as the transparent encryption of electronic messages, the creation of a secure collaboration site, and secure data transfer (in particular external disk encryption).

Dedicated project checks

As part of the assessment procedure, we analyse new IT systems and their updates in order to comply with the level of security required by KPMG, and to protect the confidential data of its clients in an appropriate manner. The purpose of this procedure is to assess system functionality and identify the risks to information security within the system. If risks are identified, corrective measures are prepared and implemented, allowing for any confidential information pertaining to clients to be secured before it is accessible or used.

Security events

Monitoring IT security events

In order to provide an appropriate response to security events, KPMG has a number of tools enabling it to assess the operations carried out on its systems and by its staff. Furthermore, KPMG has installed antivirus software on multiple system components (including the electronic messaging system, servers and PCs), allowing for the automatic update of antivirus definitions on a regular basis and the implementation of emergency response plans, where applicable. Automated procedures allow for files of unknown origin to be blocked and possible intrusions to be identified, protecting the KPMG environment from any viral infection.

KPMG has implemented security alert monitoring procedures in order to identify system vulnerabilities and malware such as viruses and worms. These procedures involve analysing risks to the KPMG environment, updating and installing security patches, and implementing protective measures, where applicable.

Software likely to damage the integrity of the KPMG systems and networks is identified. This software must not be downloaded on KPMG computers or used on the network. The list of prohibited software includes peer-to-peer systems and file sharing, external instant messaging systems, and system utilities. The procedures allow for running scan and search functions, and for preparing reports on the applications or software installed on KPMG equipment that may present a risk. The reports identify the users concerned and send a notification for the immediate deletion of unauthorised applications or software. Disciplinary sanctions may be applied to any person who refuses to delete prohibited software or applications.

Security incidents

Procedures for managing security incidents, including the loss/distribution of data and physical security incidents:

- Any IT security incident is reported to the IT security manager.
- Any incident involving data is forwarded to the Risk Management department and the internal legal department.
- Any physical security incident is reported to the physical security manager.

Data lifecycle

Data backup

Data backup procedures have been implemented for the recovery of data following a system malfunction or any other anomaly. The data is backed up in accordance with the rules for business continuity and recovery following a system crash. The integrity of the backed-up data is tested on a regular basis, in accordance with the data recovery procedures.

Retention and deletion

KPMG applies policies relating to document retention, in accordance with the law, with regulatory requirements and with the requirements related to the professions affected by the activities of KPMG. These policies apply to any document or file, in physical or electronic form. Upon expiry of the retention period (from 7 to 10 years depending on the respective profession), the documents or files are deleted in a secure manner, in accordance with the standards governing our business sector and our policies.

Disposal of equipment

The data stored on KPMG PCs and hard disks reaching the end of their life cycle is wiped using ‘Blancco’ data eraser software.

All servers reaching the end of their life cycle are securely recycled by approved professionals.

Internal compliance

The team responsible for KPMG information security has established an internal risk assessment programme, dedicated specifically to information security, which includes:

- An annual assessment: comprised of a self-assessment and an audit. The self-assessment is based on the internationally recognised assessment programme (http://sharedassessments.org/). It ensures the continuous assessment of all KPMG member firms with regard to the management of information security and IT security. It is carried out on an annual basis by the IT security manager of each member firm. The results are sent to the management of each member firm, which is responsible for processing these results. The IPG (Information Protection) department of KPMG International is responsible for monitoring.

- An annual IT vulnerability assessment: the IPG Department of KPMG International provides member firms with vulnerability detection tools for all online software and infrastructure. This assessment is aimed at measuring the risk and identifying the patches and security measures to be implemented.

Compliance with IT standards

In accordance with internal policies, KPMG complies with IT standards and provides maintenance for the software installed on all its computers. IT standards, software versions and security patches are regularly monitored and assessed by the IT department, which ensures their validity and updates or replaces them if necessary. The products and software included in the standard configuration of KPMG computers are updated and installed across all platforms, as part of the international roll-out.

Communication

For staff

KPMG emphasises the importance of information security, ethical behaviour and client confidentiality. KPMG has a code of conduct that applies to all employees and regularly communicates its policies and procedures. The various employee training programmes include chapters on ethics, confidentiality, security, risk and quality management, and practices specific to our professions. These policies and procedures and our information leaflets are published on the KPMG intranet and are available to all employees.

Furthermore, every year KPMG employees are required to sign a statement of commitment, in which each employee undertakes to respect data confidentiality and privacy, in respect of clients in France or abroad and of any person working for the firm.

When hired by the company, KPMG employees confirm in writing that they understand KPMG's professional rules and policies, applicable in the context of using confidential client information. This statement is then renewed every year.

For further information

We hope that the information contained in this document answers any questions regarding KPMG practices in the area of security.

For more information, please first consult your manager responsible for KPMG engagement. Where applicable, you will be redirected to the team responsible for information security.

Contact

fr-nitso@kpmg.fr

www.kpmg.fr