ICLG

The International Comparative Legal Guide to:

Cybersecurity 2019

2nd Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Angara Abello Concepcion Regala & Cruz Law Offices
Bagus Enrico & Partners
Boga & Associates
BTG Legal
Christopher & Lee Ong
Cliffe Dekker Hofmeyr Inc
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Ferchiou & Associés
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
JIPYONG LLC
King & Wood Mallesons
Latham & Watkins LLP
Lee, Tsai & Partners Attorneys-at-Law
LT42 – The Legal Tech Company
Maples and Calder
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Simmons & Simmons LLP
Siqueira Castro Advogados
Stehlin & Associes
Synch
Templars
USCOV | Attorneys at Law

glg
global legal group

glg
global legal group

Contributing Editors
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Sam Friend

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
October 2018

ISBN 978-1-912509-38-6
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

France

Frederic Lecomte

Stehlin & Associes

Victoire Redreau-Metadier

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Hacking is a criminal offence pursuant to article 323-1 of the French Criminal Code (FCC) relating to unauthorised access to an automated data processing system. The punishment for fraudulent access into an automated data processing system is imprisonment and a fine of up to €60,000. When data is modified or suppressed as a result of the unauthorised access, the sanction is three years of imprisonment and a fine of up to €100,000. When the offence is committed in a public or governmental system, the sanction is raised to five years of imprisonment and a fine of up to €150,000.

Denial-of-service attacks

Article 323-2 of the FCC sanctions the impeding or slowing down of an information system. Any kind of obstruction falling within the perimeter of article 323-2 is punishable by five years of imprisonment and a fine of up to €150,000. When the offence involves a public or governmental system, the sanctions are raised to seven years of imprisonment and a fine of up to €300,000.

Phishing

Phishing is sanctioned by the following articles of the FCC and of the Intellectual Property Code:

(i) the collection of data by fraudulent, unfair or unlawful methods is sanctioned by article 226-18 of the FCC by five years of imprisonment and a fine of up to €300,000; (ii) the theft and use of a third-party identity is sanctioned by article 226-4-1 of the FCC by one year of imprisonment and a fine of up to €15,000 – the applied sanction is cumulative with the sanctions applied pursuant to (i) above; (iii) the fraud or swindle is sanctioned by article 313-1 of the FCC by five years of imprisonment and a fine up to €375,000; (iv) unauthorised introduction of data in a system, the extraction, reproduction, transmission and use of data stored in this system is sanctioned by article 323-3 of the FCC by five years of imprisonment and a fine of up to €150,000; and (v) phishing can result in an infringement of intellectual property rights, in particular on the basis of articles L.335-2, L.713-2 and L.713-3 of the French Intellectual Property Code. The owner of the reproduced or imitated website or trademark can sue the phisher for the use of his trademark on the basis of infringement. This offence is sanctioned by three years of imprisonment and a fine of up to €300,000.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

This offence can by sentenced pursuant to article 323-1 of the FCC (*see Hacking*) but also pursuant to article 323-2 of the FCC (*see Denial-of-service attacks*) and pursuant to article 323-3 of the FCC (*see Phishing*).

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Pursuant to article 323-3-1 of the FCC, the act consisting of, without a legitimate motive (in particular for research or computer security), importing, holding, offering, transferring or making available equipment, instruments, computer programs or any data designed or specially adapted to commit one or more offences mentioned in articles 323-1 to 323-3 of the FCC (*see Hacking, Denial-of-service attacks and Phishing*) is punished with the most severe sanctions.

Identity theft or identity fraud (e.g. in connection with access devices)

Pursuant to article 226-4-1 of the FCC, the act of usurping the identity of a third party is punishable by one year of imprisonment and a fine of up to €15,000.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

The offence of theft pursuant to the FCC (article 311-1) has been extended to computer theft by French courts.

French judges now consider computer data (i.e. dematerialised information), as constituting goods likely to be stolen.

Under French law, theft is punishable by three years of imprisonment and a fine of up to €45,000.

Article 226-18 of the FCC as well as articles L.335-2, L.713-2 and L.713-3 of the French Intellectual Property Code (*see Phishing*) could also be used in some circumstances.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Article L.66 of the French Post and Electronic Communications Code imposes sanctions of two years of imprisonment and a fine of up to €3,750 for any person who, by breaking wires, damaging equipment or by any other means, deliberately interrupts electronic communications.

Attacks on the fundamental interests of the nation committed by means of information technologies are punished by numerous provisions of the FCC. For example, pursuant to article L.413-10 of the FCC, the destruction, misappropriation, subtraction, reproduction of the defence secrecy or the giving of access to an unauthorised

person or making it available to the public, is sentenced to seven years of imprisonment and a fine of up to €100,000.

Failure by an organisation to implement cybersecurity measures

The failure by an organisation to implement cybersecurity measures does not constitute a criminal but an administrative offence, and the organisation would be subject to administrative fines and civil liability. Pursuant to the GDPR and the new French Data Protection Act (FDPA) n° 78-17 of January 6, 1978 (amended by the GDPR), the administrative fine imposed by the French data controlling body (the CNIL) can be up to €20 million or 4% of the company's worldwide consolidated annual turnover.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Pursuant to article 113-2-1 to the FCC, any crime or offence committed by means of an electronic communication network is deemed to have been committed on the territory of the Republic when it is attempted or committed to the detriment of a natural person residing on the territory of the Republic or a legal person whose registered office is in France.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

An offence will only be sanctioned by a court pursuant to the FCC if the intentional nature of the offence results from the facts or is demonstrated by the prosecutor. Pursuant to the GDPR as applied under French law, the lack of intentional motivation, all measures taken by the controller or the processor to mitigate the damage suffered by the data subjects, and/or the degree of cooperation to remedy the breach are considered as positive behaviour and may reduce the level of administrative sanctions. As a general principal, the level of sanction is left to the appreciation of the CNIL or the judge and will mainly depend on the situations and the behaviour of the charged party.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Many of the FCC provisions may apply or be linked to cybercrime. For example, article 226-16 to 226-24 set out the criminal offences for the violations of the FDPA. With respect to terrorism article 322-6-1 of the Criminal Code, it provides that: "*The act of disseminating by any means, except to professionals, processes allowing the manufacture of destruction devices shall be punishable by three years' imprisonment and a fine of €45,000. The penalties are increased to five years' imprisonment and a fine of €75,000 where an electronic communication network has been used for the dissemination of the processes to an unspecified public*." Moreover, article 421-2-5-1 of the same code sentences with five years of imprisonment and a fine of €75,000 the act of extracting, reproducing and intentionally transmitting data that intentionally promotes acts of terrorism.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The most important laws in the cybersecurity domain are (without being exhaustive):

- The Law Godfrain (*n°88-19 of January 15, 1988*).
- The FDPA (*Loi Informatique et Libertés n°78-17 of January 6, 1978*) successively amended by two laws: the law for confidence in the digital economy (*Loi pour la confiance dans l'économie numérique, n° 2004-575 of June 21, 2004*); and finally amended by the *Law n°2018-793 of June 20, 2018* transposing the GDPR.
- The Law for a Digital Republic (*Loi pour une République numérique, n° 2016-1321 of October 7, 2016*) and recently amended by the law transposing the GDPR (*Law n°2018-493 of June 20, 2018*).
- The Network and Information Systems Security Act transposing the NIS Directive (*Loi sur la sécurité des réseaux et systèmes d'information, n°2018-133 of February 26, 2018*).

In addition to the abovementioned law, the following texts have adapted the criminal law to certain forms of cybercrime and creating specific investigative means such as:

- The Law on Daily Security (known as LSQ *n° 2001-1062 of November 15, 2001*), *the Law on Internal Security* (*n°2003-239 of March 18, 2003*).
- The law adapting the judiciary to developments in crime (*n° 2004-204 of March 9, 2004*), the Law on Copyright in the Information Society (known as *David's Law of August 1, 2006, n°2006-961*).
- The Law OPSI II (*n° 2011-267 of March 14, 2011*).
- The Law strengthening the provisions on the fight against terrorism (*n° 2014-1353, of November 13, 2014*).
- The Law strengthening the fight against organised crime and terrorism (*n° 2016-731, of June 3, 2016*).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

In France, critical infrastructures identified as such by the law (*Law n°2013-1168 of December 18, 2013, Law n°2018-133 of February 26, 2018, Law n°2016-41 of January 26, 2016*) must comply with specific legal requirements. This is mostly the case for the following infrastructures:

- Professionals subject to the obligation of professional secrecy. For instance, pursuant to article 1111-8-2 of the French Public Health Code, healthcare institutions as well as bodies and services carrying out prevention, diagnosis or care activities shall report without delay serious information system security Incidents to the Regional Health Agency. Moreover, pursuant to article 1111-8 of the same code any person who hosts personal health data, must be accredited by the National Health Accreditation Authority for this purpose.

- Essential operators for essential services (i.e. infrastructure in the energy, transport, banking, financial market, drinking water supply and distribution and digital infrastructure sectors).
- Digital service provider.

The Network and Information Systems Directive has been implemented in France by the Law 2018-133 of February 26, 2018 about the security of networks and the information system. Pursuant to article 9 of this new law, these infrastructures must implement technical and organisational measures to prevent and reduce the impact of Incidents, identify the IT security risks that may affect their activities (failing which they incur a fine up to €100,000) and notify the ANSSI (National Agency for IT system Security) about the security Incidents they suffer (failing which they incur a fine of up to €75,000).

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Pursuant to the GDPR, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the identified risk.

Pursuant to article 34 of the FDPA, the controller (and processor) are required to take all necessary precautions, having regard to the nature of the data and the risks associated with the processing, to preserve the security of the data and, in particular, to prevent it from being distorted, damaged or accessed by unauthorised third parties.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Such conflicts may arise in France, for example, concerning the storage period of personal data (storage periods within the meaning of the FDPA may conflict with the rules of proof). Such conflicts may also arise with countries that are not a member of the European Union.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The GDPR (article 33) provides for an obligation for all data controllers to notify any Incidents to the competent data controlling body unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. This notification to the controlled body must take place within 72 hours of the discovery breach and must contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects, a detailed description of the measures taken to remedy or mitigate negative effects and the name and contact details of the data protection officer. The notification to the competent data protection authority must also describe possible harmful consequences of the unlawful access and measures taken by the controller.

The FDPA (article 34*bis*) which specifically concerns the Internet Service Providers (ISP) provides for an obligation to notify any data breach to the CNIL immediately and without conditions (the likelihood that the Incident may cause a risk to the rights and freedoms of natural persons is not required). The information to be communicated is rather similar to the abovementioned.

Finally, pursuant to article 9 of the law 2018-133 of February 26, 2018, about the security of networks and information system, critical infrastructures also have the obligation to notify security breaches to the ANSSI.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

It is possible to voluntarily notify such security breaches to other competent authorities.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Pursuant to the GDPR and the FDPA, if the breach creates a high risk to the rights and freedoms of affected individuals (article 34 of the GDPR) and/or if the breach creates a risk compromising the personal data or privacy of the person concerned (article 34*bis* of the FDPA) the controller shall have the obligation to inform each affected individual of any security breaches.

The information must detail the name and contact details of the data protection officer (DPO) and describe in clear and plain language the nature of the personal data breach, describe the likely consequences of the personal data breach and the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The GDPR covers three cases where such notification is not necessary (e.g. the implementation of post-breach measures to ensure the absence of a high risk).

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

None of these cases would change the responses to questions 2.5 to 2.7.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The CNIL controls the proper application of the FDPA and the GDPR by data controllers and processors. It also gives opinions on legislative drafts or regulatory texts.

The CNIL has important powers of control and investigation.

Finally, the CNIL has significant administrative and financial penalty powers and can take decisions such as the temporary or permanent suspension of data processing.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Depending on the nature of the offence, the penalty may vary between €10 million or 2% of the worldwide turnover, and €20 million or 4% of the worldwide turnover.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Since the entry into force of the GDPR, the CNIL has sanctioned several companies for various reasons. For example, the CNIL fined a French association €75,000 for inadequately protecting users' data on its website. The CNIL also fined OPTICAL CENTER €250,000 for not having sufficiently secured the data of their online customers on its website.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The measures to be implemented are stronger in some business areas. This is particularly the case for critical infrastructures which must comply with the law of February 26, 2018 transposing the NIS Directive (*see* question 2.2), or for Infrastructures that process sensitive data (for example, health data or data relating to criminal sentences, offences or security measures). Also, as mentioned above (*see* question 2.2), companies who host personal health data must be accredited for this purpose.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The legal requirements related to cybersecurity in the following two sectors are as follows:

(a) The financial services sector must comply with several requirements such as auditing IT systems, strengthening resistance to cyber risks, developing defences adapted to the complexity of cyber-attacks, and making several declarations to the ANSSI (ministerial orders of November 28, 2016).

(b) Pursuant to article L33-1 of the French Post and Electronic Communications Code, companies in the telecommunication sector must comply with rules relating to the conditions of permanence, quality, availability, security and integrity of the network and service, which include obligations to notify to the competent authority breaches to the security or integrity of networks and services.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Beyond the company's responsibility in case of failure of the IT system (*see* question 2.10), the company manager (i.e. in France, it is the representative of the company who has the power to bind the company, e.g.: president; CEO; and general manager) is liable under civil law towards the company and its shareholders of (i) breach of the laws and regulations or of the bylaws, and (ii) mismanagement (article 1850 of the Civil Code). Moreover, the company manager can be liable because of the behaviour of his employees if such behaviour results in damage to a third party (article 1242 paragraph 5 of the French Civil Code). Finally, French law provides numerous criminal offences which may apply to the manager of a company. Actually, pursuant to the FCC but also the French Commercial Code there are numerous provisions specifically making the company manager subject to personal criminal liability.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Please see below the Applicable Law requirements:

(a) There are no general obligations, so far, to designate a CISO. However, the GDPR sets out the obligation to appoint a DPO when (i) the data processing is carried out by a public authority or public body, (ii) the data processing requires regular and systematic monitoring on a large scale, and (iii) in cases of large-scale processing of sensitive data. Concerning the designation of the DPO, French law strictly applies the GDPR (unlike other European Union Member States, such as Germany). Consequently, apart from the three cases mentioned above, the designation of a DPO is optional in France.

(b) For the critical infrastructure, several ministerial orders of November 28, 2016 (article 10) set out the obligation to maintain a crisis management procedure in the event of major cyber-attacks. For other companies, there are no general obligations to establish a written Incident response plan or policy.

(c) Pursuant to the FDPA (article 70-13), the controller and the processor must carry out a risk assessment in order to implement measures to protect data processing systems. Moreover, pursuant to article 1110-4-1 of the French Public Health Code, health professionals, healthcare institutions and services must use information systems for the processing of health data, their storage on electronic media and their transmission by electronic means, in accordance with interoperability and security standards in order to guarantee the quality and confidentiality of personal health data and their protection.

(d) For critical infrastructures, the ministerial orders of November 28, 2016 impose audits to assess the level of security of

information systems with regard to known threats and vulnerabilities. For other companies, the French law strictly applies the GDPR according to which the controller and the processor must implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (article 32.1.d).

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Pursuant to article L.225-100-1 of the French Commercial Code and article 222-3 of the General Regulations of the French Financial Markets Authority, listed and private companies must draw up an annual management report which contains a description of the main risks and uncertainties the company had to face or is facing (which implicitly includes cyber risks). Pursuant to article L.451-1-2 of the French Commercial Code, listed companies are required to submit this report to the French Financial Markets Authority and to publish it on their website.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

To the extent that they fall within the scope of the NIS Directive and/or the GDPR, public and listed companies are subject to the requirements of these texts.

In addition, public sector infrastructures are subject to the RGS (the general security database), which aims at securing electronic exchanges from the public sphere by ensuring that the level of security of these information systems is well adapted to the challenges and risks involved (Article 1 of *Decree n°2010-112 of February 2, 2010*).

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Under French Law the general rule of civil liability is set forth under article 1240 of the French Civil Code pursuant to which any act which causes damage to another shall oblige the person by whose fault it occurred to repair it (i.e. three elements are necessary to engage liability: (i) a fault; (ii) a damage; and (iii) a causal link between the two). Moreover, under the GDPR (article 79) a civil action may be brought in the event of an Incident if the controller or the processor have not complied with the GDPR requirements. Finally, under the FDPA, the data subject shall have the right to mandate a not-for-profit body, organisation or association to stop the breach and to obtain compensation (article 43*ter*).

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There are several examples of cases that have been brought to French courts in the relation to Incidents. For example, a woman was penalised in civil and criminal terms by the Chambery Court of Appeal on November 16, 2016 for the possession of hacking data. Another example, is where on August 12, 2016, the Paris Regional Court sentenced in civil and criminal terms a man for usurping a digital identity.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

See the answers to questions 5.1 and 5.2.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber risk is partially covered by traditional insurance contracts which cover certain foreseeable consequences of certain computer threats (e.g. insurance contracts covering damage to property and civil liability). The emergence of new risks from the evolution of technologies and the increase in their uses has required and still requires the implementation of appropriate legal frameworks. To cope with these new risks, insurers have developed a new contract: the cyber contract; which is a multi-risk contract cover for damage (costs and losses incurred) and liability (non-material damage to third parties); and management services of crisis.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Pursuant to article L.113-1 of the French Insurance Code, the insurer does not cover loss or damage resulting from the insured's intentional or wilful misconduct. In addition, criminal sanctions are not insurable because they are regarded as personal sanctions. Moreover, there is still a debate about the possibility to insure administrative or financial sanctions (such as the one provided by the GDPR) to the extent they are not the result of intentional misconducts. The authors opine that this risk should be insurable.

On the subject of terrorism and cyberterrorism, the French Public Purse stated that "*insurance contracts whose purpose is to guarantee the payment of a ransom to Daech, as to any terrorist entity, are prohibited*".

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The specific requirements under the Applicable Law are as such:

(a) The monitoring of employees is authorised. Actually, the employer can control and limit the use of the Internet (site filtering devices, virus detection, etc.) and e-mail (tools for measuring the frequency of messages sent and/or the size of messages, "anti-spam" filters, etc.). The purpose of this control is to ensure the security of networks that could be attacked (viruses, Trojans, etc.) and to limit the risks of abusive or personal use of the Internet or e-mail. However, (i)

the introduction of a monitoring process to monitor employee activity requires a prior information and consultation of the employee representative committee and (ii) an individual information for employees. As a consequence, the monitoring must be proportionate, i.e. respect the balance between the employee's private life and the employer's power of control.

(b) Except for the DPO, there is no specific statutory obligation for employees to report such risks to their employer. However, internal policies (such as company rules or an IT security charter) can encourage employees to adopt a proactive reporting behaviour if they noticed an Incident. In France, there is also a "whistleblowing" mechanism available to employees (this can be, for example, an "ethical line" telephone number or a specific e-mail address). This system enables employees to report problems that could seriously affect a company's activity or seriously engage its liability. However, this mechanism remains optional. An employee cannot be sanctioned if he does not use it.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no Applicable Laws that may prohibit or limit the reporting.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In France, there are many police services specialising in cybersecurity. For example: the PICyAN (Cybercrime investigation platform and digital analysis), which analyses IT equipment seized during police searches and Internet surveillance thanks to special software; the C3N (Digital Crime Centre) whose mission includes judicial investigations and criminal intelligence; the BEFTI (Information Technology Fraud Investigation Brigade), which operates only in Paris and the surrounding suburbs and which is responsible for managing any breaches of the data processing system, software counterfeiting and classic offences such as fraud; and the OCLCTIC (Central Office for the Fight against Information and Communication Technologies Crime), which ensures the legality of published content on Internet and ordering providers to remove illegal content.

The police services mentioned above may carry out investigations, searches, interceptions, data collection, geolocation, wiretapping, infiltration, and arrest and detain suspects in police custody.

In addition, in order to ensure the effective application of the FDPA and the GDPR, the CNIL has the power to carry out extensive controls on all data controllers and processors. These controls can take place in the controlled entity's facilities, on documents, on audition or online.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There is no obligation to set up backdoors. However, the administrative and judicial authorities may require the submission of encryption keys. Actually, pursuant to article L.871-1 of the French Internal Security Code, natural or legal persons who provide encryption services aimed at ensuring a confidentiality function are required to submit within 72 hours to authorised agents (i.e. administrative and judicial authorities) at their request, agreements enabling the decryption of data transformed by means of the services they have provided. Article 434-15-2 of the FCC provides that any person who has knowledge of the secret agreement to decrypt a cryptology means that may have been used to prepare, facilitate or commit a crime or offence who refuses to surrender the said agreement to the judicial authorities or to implement it at the request of these authorities is subject to three years of imprisonment and a fine of up to €270,000.

Frederic Lecomte
Stehlin & Associes
48 avenue Victor Hugo
Paris, 75116
France

Tel: *+33 1 44 17 07 70*
Fax: *+33 1 44 17 07 77*
Email: *f.lecomte@stehlin-legal.com*
URL: *www.stehlin-legal.com*

Frederic Lecomte has been a member of the Paris Bar since 1989. Frederic joined Stehlin & Associes in 1993 after having spent five years at Coudert Brothers in Paris. He became a partner in 1998.

Frederic is the author of numerous articles in relation to technology law and is the author of a book about the GDPR *Nouvelle Donne Pour les Données* (Fauve Editions, 2018).

Practice areas: new technologies and data law; intellectual property; contract law and trade; and distribution law.

Victoire Redreau-Metadier
Stehlin & Associes
48 avenue Victor Hugo
Paris, 75116
France

Tel: *+33 1 44 17 07 70*
Fax: *+33 1 44 17 07 77*
Email: *v.redreaumetadier@stehlin-legal.com*
URL: *www.stehlin-legal.com*

Victoire Redreau-Metadier has been a member of the Paris Bar since 2017. Victoire joined Stehlin & Associes in 2017.

Victoire was involved in the writing of the book about the GDPR *Nouvelle Donne Pour les Données* (Fauve Editions, 2018).

Practice areas: new technologies and data law; intellectual property; contract law and trade; and distribution law.

Stehlin & Associés

Stehlin & Associes is an independent business law firm that was founded in 1989.

The firm's attorneys work together in a pragmatic way to implement their projected operations and solve problems encountered by clients, both in their day-to-day business as well as in specific transactions. With an international outlook from the beginning of its existence, the firm has numerous contacts with firms throughout the world. Since 2012, the firm has been the French member of the Mackrell International network, which is ranked among the top law firm networks in *Chambers* 2018, with a presence in 60 countries and 170 cities, and providing access to more than 4,500 attorneys.

Our team assists its clients in the new technologies and intellectual property fields, which include copyright and neighbouring rights, industrial property rights, Internet and new technologies rights and Privacy law.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com