ICLG

The International Comparative Legal Guide to:

Data Protection 2016

3rd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bagus Enrico & Partners
Cuatrecasas, Gonçalves Pereira
Deloitte Albania Sh.p.k.
Dittmar & Indrenius
ECIJA ABOGADOS
Eversheds SA
Gilbert + Tobin
GRATA International Law Firm
Hamdan AlShamsi Lawyers & Legal Consultants
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Rossi Asociados
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

global legal group

global legal group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Sales Director
Florjan Osmani

Account Directors
Oliver Smith, Rory Smith

Sales Support Manager
Toni Hayward

Sub Editor
Hannah Yip

Senior Editor
Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

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.
April 2016

ISBN 978-1-910083-93-2
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

France

Hunton & Williams

Claire François

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is Act No. 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties as amended (*Loi Informatique et Libertés*) (the "**Data Protection Act**" or "**DPA**") and Decree No. 2005-1309 implementing the French DPA. The DPA transposes into French law the requirements of the EU Data Protection Directive (95/46/EC) (the "**Data Protection Directive**") as well as some of the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "**ePrivacy Directive**"). The purpose of the DPA is to ensure that any use of information technology does not violate "human identity, human rights, privacy, or individual or public liberties". The DPA applies to both the public and private sectors.

1.2 Is there any other general legislation that impacts data protection?

The DPA and its implementing Decree are the only legislation explicitly governing data protection. However, some provisions of French Codes may regulate specific issues, e.g., Article L.34-5 of the French Postal and Electronic Communications Code which regulates direct marketing by electronic means.

1.3 Is there any sector specific legislation that impacts data protection?

Other provisions of the French Postal and Electronic Communications Code implement the requirements of the ePrivacy Directive. These requirements impose additional data protection obligations on telecommunications service providers, in addition to the French DPA.

1.4 What is the relevant data protection regulatory authority(ies)?

The *Commission Nationale de l'Informatique et des Libertés* (the "**CNIL**") supervises compliance with the DPA in France. The CNIL's current Chairwoman, elected in September 2011 and re-elected in February 2014, is Isabelle Falque-Pierrotin. The CNIL elects its Chairman or Chairwoman from among its members. The CNIL is an independent administrative body. It does not receive any instructions from any single authority.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  "Personal Data" means any information relating to an individual who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him/her. The concept of Personal Data is interpreted broadly and assessed on a case-by-case basis by the CNIL.

- **"Sensitive Personal Data"**

  "Sensitive Personal Data" means Personal Data that reveals, directly or indirectly, the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of individuals, or which concern their health or sexual life.

- **"Processing"**

  "Processing" of Personal Data (or "Data Processing") means any operation or set of operations in relation to such data, whether or not by automated means, especially the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

- **"Data Controller"**

  The DPA defines the "Data Controller" as a person, public authority, department or any other organisation who determines the purposes and means of the Data Processing.

- **"Data Processor"**

  The DPA defines the "Data Processor" as a person who processes Personal Data on behalf of the Data Controller.

- **"Data Subject"**

  A "Data Subject" is the individual to whom the Personal Data covered by the Processing relate.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  There are no other key definitions in particular.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Under Article 6(1) of the DPA, Personal Data must be processed fairly and lawfully. Specifically, Data Subjects must be informed by the Data Controller of how their Personal Data will be used.

  When the Data Controller directly collects the Personal Data from Data Subjects, it must provide notice, as a minimum, at the time of collection, of: (i) its identity; (ii) the purpose of the Processing; (iii) whether replies to the questions are compulsory or optional; (iv) the possible consequences for Data Subjects in the absence of a reply; (v) the categories of persons to whom the data are disclosed; (vi) the rights granted to Data Subjects; and (vii) if applicable, information on the transfers of the Personal Data outside of the EU.

- **Lawful basis for processing**

  For Personal Data to be processed lawfully, the Data Controller must have a legal basis for each Processing activity. The DPA sets out legal bases for the Processing of Personal Data in Article 7, and for Sensitive Personal Data in Article 8.

  The legal bases commonly relied upon by French Data Controllers to process Personal Data are: (i) compliance with a legal obligation of the Data Controller; (ii) the performance of a contract to which the Data Subject is a party or steps taken at the request of the Data Subject prior to entering into a contract; and (iii) the pursuit of the legitimate interest of the Data Controller, provided that this is not incompatible with the fundamental rights and freedoms of the Data Subject. In principle, the Processing of Sensitive Personal Data is only permitted with the Data Subject's consent.

- **Purpose limitation**

  Under Article 6(2) of the DPA, Personal Data may only be obtained for specific, explicit and legitimate purposes, and cannot be further processed in any manner incompatible with those purposes.

- **Data minimisation**

  Under Article 6(3) of the DPA, Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed. Data Controllers are therefore under a duty to process only the Personal Data necessary to achieve the purpose of the Processing, and to not collect or retain unnecessary or irrelevant Personal Data.

- **Proportionality**

  See "Data minimisation".

- **Retention**

  Under Article 6(5) of the DPA, Personal Data must not be retained for longer than is necessary for the purposes for which they are collected and further processed. The CNIL has recommended specific retention periods in its various decisions (such as its Simplified Norms).

- *Other key principles – please specify*

  - **Security**

    Under Article 34 of the DPA, Data Controllers must implement appropriate organisational and technical measures to ensure the security and confidentiality of the Personal Data. As part of this obligation, Article 35 of the DPA requires the Data Controller to conclude a written contract with the Data Processor, specifying the obligations incumbent upon the Data Processor as regards the protection of the security and confidentiality of the data and providing that the Data Processor may act only upon the instruction of the Data Controller.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  Data Subjects have the right to require the Data Controller to: (i) confirm whether it is processing their Personal Data; (ii) provide a description of the Processing (i.e., information on the purposes of the Processing, the categories of Personal Data processed, the persons or categories of persons to whom the data may be disclosed and, if applicable, information on the transfers of Personal Data outside the EU); and (iii) provide a copy of their Personal Data as well as any available information on the origin of the data. Data Subjects may make their requests in writing or on site at the premises of the Data Controller. Data Subjects must provide proof of identity. Data Controllers must respond to the requests within two months (unless the request is manifestly abusive or the data are no longer retained) and may charge a fee for providing a copy of the Personal Data.

- **Correction and deletion**

  Data Subjects have the right to require the Data Controller to, as the case may be, rectify, complete, update, block or delete their Personal Data that are inaccurate, incomplete, equivocal, expired, or whose collection, usage, disclosure or storage is prohibited. The Data Controller also has two months to respond to such requests. At the request of the Data Subjects, the Data Controller must provide confirmation that the corrections or deletions have been made and the Data Controller cannot charge any fee for doing so. If data have been shared with a third party, the Data Controller must ensure that this third party makes the requested corrections/deletions.

- **Objection to processing**

  Data Subjects have the right to object, on legitimate grounds, to the Processing of their Personal Data. Data Subjects must justify their requests and it is up to the Data Controller to assess if the reason invoked by the Data Subject is legitimate.

- **Objection to marketing**

  Data Subjects have the right to object, free of charge, to the Processing of their Personal Data for direct marketing.

- **Complaint to relevant data protection authority(ies)**

  Data Subjects may raise complaints with the CNIL. In 2014, the CNIL received 5,825 complaints. Data Subjects may submit their complaint online on the CNIL's website.

- *Other key rights – please specify*

  - **Consent**

    Data Subjects have further rights in relation to direct marketing and cookies (see section 7 below).

  - **De-listing of search engines' results**

    Data Subjects have the right to request search engines, under certain conditions, to de-list certain links to information affecting their privacy from the results for searches made against their name.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

Under the DPA, Data Controllers must register any automated Processing of Personal Data with the CNIL prior to its implementation. Several exemptions exist, e.g., for the Processing carried out by a non-profit organisation or institution with religious, philosophical, political or trade union purposes or for the Processing implemented in accordance with one of the CNIL's exemption decisions (such as for payroll administration or vendor management). Certain types of Data Processing may not benefit from any exemption and require the CNIL's prior approval (see question 5.8 below).

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Registrations must be submitted for each legal entity acting as a Data Controller and per Processing purpose.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

Organisations subject to the DPA and not benefiting from one of the registration exemptions must register their Data Processing activities with the CNIL. This includes both French legal entities and non-EU legal entities using means or equipment located in France to process Personal Data (except where the Personal Data are in mere transit through the French territory).

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

The following information must be included in the CNIL's standard registration (*Déclaration normale*): (i) identity and contact details of the Data Controller or its representative; (ii) department or organisation in charge of implementing the Processing; (iii) purpose of the Processing; (iv) categories of Data Subjects to whom the Processing relates; (v) categories of Personal Data processed, their origin, the data retention period and the categories of recipients (persons/departments/entities) to whom the data may be disclosed; (vi) steps taken to ensure the security of the Personal Data processed; (vii) if applicable, any data transfers to a country outside the EU and details about the transfers; (viii) if applicable, the combination of the Personal Data with other data contained in a different database; (ix) information on how Data Subjects are informed of their data protection rights and on the entity/department where Data Subjects may exercise their rights; (x) contact details of a person whom the CNIL may contact in case of questions; and (xi) identity, email address and function of the signatory of the registration.

5.5 What are the sanctions for failure to register/notify where required?

Failure to register with the CNIL where required is a criminal offence and may lead to up to five years' imprisonment and a fine of up to €300,000 (for individuals) or a fine of up to €1.5 million (if the company is held liable). In addition, the CNIL may impose an administrative sanction (see question 14.1 below).

5.6 What is the fee per registration (if applicable)?

This is not applicable.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

The Processing activities requiring the CNIL's prior approval include:

- the Processing of Sensitive Personal Data if it is in the public interest or if the data are subject, within a short period of time, to an anonymisation procedure approved by the CNIL;
- the Processing of biometric data;
- the Processing of genetic data (except if the Processing is carried out by doctors or biologists for preventive medicine, medical diagnosis or the administration of care or treatment);
- the Processing relating to data containing the social security number (except for organisations which have been authorised to process this number, such as public authorities and employers for HR purposes);
- the Processing of Personal Data including assessments of the social difficulties of individuals;
- the Processing of Personal Data relating to offences, convictions or security measures (except for representatives of the law);
- the Processing of Personal Data which may preclude persons from the benefit of a right, a service or a contract in the absence of any legislative or regulatory provision;
- the combination of databases, each of which was created for a different purpose;
- the Processing of Personal Data for the purpose of medical research;
- the Processing of Personal Data for the purpose of evaluation or analysis of care and prevention practices or activities; and
- transfers of Personal Data to a country outside the EU which does not provide a sufficient level of data protection, where the transfers are based on the European Commission's Standard Contractual Clauses or Binding Corporate Rules ("**BCRs**").

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

A request for approval must be completed and submitted with the CNIL (preferably online on the CNIL's website). The CNIL must issue a decision within two months of receipt of the request. This period may be renewed once. The absence of a decision within this timeframe is considered to be a refusal.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

The appointment of a Data Protection Officer (*Correspondant Informatique et Libertés* or "**CIL**") is optional.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

Organisations that appoint a Data Protection Officer are not required to register their standard Data Processing activities with the CNIL. However, Data Processing activities requiring prior approval must still be registered.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no specific qualifications prescribed by law. There is only a general requirement that a Data Protection Officer shall have the qualifications required to perform his/her duties. The Data Protection Officer may be an employee or an external person in organisations with fewer than 50 persons involved in the Processing or having access to the data. The Data Protection Officer should, in principle, be an employee in larger organisations.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

The responsibilities of the Data Protection Officer prescribed by law include: (i) establishing and keeping a list of the organisation's Data Processing activities for which he/she was appointed; (ii) ensuring compliance with the DPA; (iii) advising the organisation, in particular on any new Data Processing activities to be included on that list, prior to their implementation; (iv) receiving Data Subjects' requests and complaints relating to these Data Processing activities; and (v) submitting an annual report of his/her activities to the organisation and making it available to the CNIL. In practice, typical duties also include: developing internal policies and procedures; conducting compliance checks; preparing (and delivering) staff training; reviewing contractual clauses relating to data protection; advising on appropriate notices to Data Subjects; registering with the CNIL the Data Processing activities subject to prior approval; and generally raising awareness of data protection issues throughout the organisation.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, organisations that appoint a Data Protection Officer must notify the CNIL of the appointment.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

The sending of marketing communications by post and by live telephone calls requires (i) notice, and (ii) a simple and free means of opting out of receiving marketing communications, at the time of collection of the postal address or telephone number.

The sending of marketing communications by automated recorded calls requires prior opt-in consent. In addition, each telephone recorded message must specify the identity of the advertiser and provide a simple means to opt-out of receiving new marketing communications. This must not result in any additional cost for the individual (e.g., no premium-rate number must be used).

The sending of marketing communications to consumers by email or SMS/MMS requires prior opt-in consent, unless the individual is already an existing customer and the marketing communication relates to similar products or services to those already provided by the advertiser. In addition, each marketing email, SMS or MMS must specify the identity of the advertiser and provide a simple way to opt-out of receiving new marketing communications.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. Recent enforcement actions include a fine of €15,000 imposed in June 2015 on PRISMA MEDIA, the leading press group in France, for various violations of the DPA, including for not obtaining web users' specific and informed consent to receive newsletters and for continuing to send newsletters to users who opted out of receiving them.

7.3 Are companies required to screen against any "do not contact" list or registry?

Yes, companies are required to screen against some "do not contact" lists, e.g., the Robinson list held by the French Direct Marketing Association ("**UFMD**") if they are a member of that association. The Robinson list identifies individuals who do not wish to receive marketing communications by post. The UFMD shares the Robinson list with its members who have committed to respect consumers' objection to receive such marketing communications. Also, as from June 2016, companies that wish to send marketing communications by telephone or SMS will have to screen against a new "do not contact" list managed by the French company, Opposetel. This new list will replace the Pacitel list identifying individuals who do not wish to receive marketing communications by telephone or SMS.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum criminal penalties are five years' imprisonment and a fine of €300,000 (for individuals) or €1.5 million (if the company is held liable). In addition, a fine of €750 may be imposed per marketing communication under the French Postal and Electronic Communications Code, and the CNIL may impose a maximum administrative fine of €300,000.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

Cookies and similar technologies require notice and prior opt-in consent, except where the cookie or similar technology is exclusively intended to enable or facilitate electronic communications or is strictly necessary for the provision of an online communication service as expressly requested by the user. Web analytics cookies may also qualify for an exemption from the consent requirement but under strict conditions. The law does not stipulate different types of consent for different types of cookies. Where consent is required, consent must be freely given, specific and informed. The CNIL considers that consent must result from a positive action of the user and may be implied (see question 7.6 below).

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

In December 2013, the CNIL issued a new Recommendation and a set of FAQs providing guidance on how to obtain consent for the use of cookies and similar technologies. The CNIL recommends obtaining consent using a two-stage approach, which suggests that consent may be implied under the DPA for all types of cookies subject to the consent requirement.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes. In January 2014, the CNIL imposed a fine of €150,000 on Google Inc. for not complying with French data protection requirements, including the obligation to obtain the user's consent before placing cookies on their terminal device. In January 2016, the CNIL issued formal notice to Facebook to comply with that obligation within three months.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

The maximum penalty is €300,000.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

Transfers of Personal Data from France to a country outside the EU are prohibited, unless that country ensures a sufficient level of data protection. A "transfer" includes the ability to access data from outside the EU, e.g., viewing it on a computer screen from another country.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Typically, Personal Data may be transferred to a country outside the EU if: (i) the law of that country has been recognised by the European Commission as providing a sufficient level of data protection; (ii) the data exporter adduces sufficient safeguards by signing the European Commission' Standard Contractual Clauses or adopting BCRs; or (iii) a relevant derogation applies, including the express consent of the Data Subject. The CNIL considers that derogations can only be used on an exceptional and specific basis and not for frequent or large transfers of Personal Data.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

Transfers of Personal Data outside the EU must be registered with the CNIL but do not require a separate registration: Data Controllers only need to complete the section on data transfers of the registration form. In addition to registration, transfers of Personal Data based on the European Commission's Standard Contractual Clauses or BCRs require the CNIL's prior approval. In such cases, the CNIL must issue its decision (authorising or not authorising the transfers) within two months. In 2015, the CNIL implemented a new procedure to facilitate registration requirements for data transfers based on BCRs. According to this new procedure, the CNIL will issue a single authorisation decision to each group that has implemented BCRs and wishes to participate in that procedure. The group's French affiliates bound by BCRs will then need to submit a simplified registration covering all their data transfers based on BCRs. They will no longer have to obtain the CNIL's prior approval for each of these data transfers.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

The CNIL considers that corporate whistle-blower hotlines are internal reporting mechanisms, which must be limited in scope. The CNIL has issued a decision called Single Authorisation AU-004 laying down specific requirements for corporate whistle-blower hotlines that only allow reports in the following areas: (i) finance, accounting, banking and anti-corruption; (ii) anti-competitive practices; (iii) fight against discrimination and harassment in the workplace; (iv) health, hygiene and safety in the workplace; and (v) protection of the environment.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

Anonymous reporting is discouraged. The CNIL's Single Authorisation AU-004 emphasises that whistle-blowers must identify themselves and that anonymous reports may only be processed exceptionally and subject to conditions. Companies typically inform their employees located in France that they should give their names when submitting a report through the hotline.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

As a rule, corporate whistle-blower hotlines require the CNIL's prior approval. The CNIL must issue its decision within two months. However, if the corporate whistle-blower hotline complies with all the requirements of the CNIL's Single Authorisation AU-004, only a prior simplified registration needs to be filed with the CNIL. In this case, the corporate whistle-blower hotline can be implemented as soon as the company has received a receipt from the CNIL.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

Companies operating a whistle-blower hotline are required to provide Data Subjects with clear and complete information about the Processing of their Personal Data through the hotline. The DPA or the CNIL's Single Authorisation AU-004 does not specify how this information must be provided. However, in practice, companies typically provide a separate privacy notice to comply with the notice requirement.

9.5 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

The French Labour Code requires to inform and consult works councils before implementing a whistle-blower hotline. Committees on hygiene, safety and working conditions ("**CHSCT**") should also be consulted, according to some Court decisions.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/ notification or prior approval from the relevant data protection authority(ies)?

The use of CCTV requires separate registration with the CNIL if CCTV records a place not open to the public (such as storage areas, areas dedicated to staff members, etc.). If CCTV records a place open to the public (entrance and exit areas for the public, sales counters, etc.), the use of CCTV must be approved by the prefect of the French department concerned.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Employers may control and limit the use of Internet and company emails for the purpose of ensuring network security and limiting risks of abuse of a too personal use of Internet and company emails. Employers may have access to professional emails of an employee and review the websites visited by him or her, even if the employee is not present. However, employers may not freely consult emails that employees have clearly identified as "private" or "personal", even if the private use of professional IT tools has been strictly forbidden.

An employer may also listen to or record employee telephone calls, e.g., for training, performance or quality purposes. However, such listening/recording should not be permanent and employees should be able to disconnect the recording function to receive or make private calls.

Further, employers may install GPS in company vehicles for limited purposes, and incidentally, for monitoring working time, when this cannot be achieved by other means. However, GPS may not be used to monitor compliance with speed restrictions and to permanently monitor an employee.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent is generally not considered valid in an employment context. However, notice is required. Each individual employee must be provided notice by any appropriate written means, such as IT guidelines, individual mail, a clause in the employment contract, etc.

10.4 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

Employee representatives must be consulted before implementing monitoring technologies.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

In most cases, employee monitoring requires separate registration.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Processing Personal Data in the cloud is permitted. In June 2012, the CNIL published practical recommendations for companies that consider using cloud computing services, such as the need to conduct proper risk assessments in order to define the security measures to be required from the cloud provider or to be implemented within the company, the need to identify which type of cloud computing services is relevant for the Processing envisaged, the need to review internal security policies and procedures, etc. The CNIL has also suggested some model contractual clauses, which can be included in cloud computing agreements.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no specific contractual obligations under the DPA that must be imposed on Data Processors providing cloud-based services, in addition to the general contractual obligations (see question 3.1 above). The CNIL has suggested some specific model contractual clauses but their use is not mandatory.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The utilisation of big data and analytics is a reality, and the CNIL is considering the privacy challenges associated with big data and how the principles of the DPA (see question 3.1 above) may apply in this context.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The DPA requires Data Controllers to "take all useful precautions, with regard to the nature of the data and the risks of the Processing, to preserve the security of the data". Specific standards are not stipulated by law or binding guidance. However, the CNIL has published a set of non-binding guides to help Data Controllers to choose the appropriate organisational and technical measures to protect Personal Data.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no general legal requirement to report data breaches to the CNIL under the DPA. The DPA only requires providers of publicly available electronic communications services to report data breaches to the CNIL. The service providers must notify the CNIL of any data breaches within 24 hours following their detection by completing a specific notification form available on the CNIL's website. If the service providers do not have all the information required to complete the form, they may make an initial notification to the CNIL within 24 hours following the detection of the breach and then a supplementary notification within three days following the initial notification.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Only providers of publicly available electronic communications services are required under the DPA to notify individuals of a data breach. This requirement applies when the breach is likely to adversely affect individuals' Personal Data or privacy. In this case, the service providers should notify the affected individuals without delay. However, telecommunications service providers do not have to notify the affected individuals when the CNIL has found that the service providers implemented appropriate technical security measures prior to the data breach. The CNIL has two months to make this assessment. In the absence of any feedback from the CNIL after that period, the service providers must immediately inform the affected individuals if they have not already done so. The CNIL expects other Data Controllers to notify individuals of data breaches that may adversely affect them.

13.4 What are the maximum penalties for security breaches?

The maximum criminal penalties are five years' imprisonment and a fine of €300,000 (for individuals) or €1.5 million (if the company is held liable). In addition, the CNIL may impose a maximum administrative fine of €300,000.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/ Administrative Sanction	Criminal Sanction
In May 2015, the CNIL announced that it planned to conduct approximately 550 inspections in 2015 (compared to 421 inspections conducted in 2014). The CNIL can conduct four types of investigations: ■ **On-site inspections** On this occasion, the CNIL may have access to any materials (servers, computers, applications, etc.) in which Personal Data is stored. This type of inspection currently represents the vast majority of inspections conducted by the CNIL. ■ **Documentary inspections** These inspections allow the CNIL to obtain disclosure of documents or files upon written request. ■ **Hearing inspections** These inspections consist of summoning representatives of organisations to appear at the CNIL in order to obtain any necessary information. ■ **Online inspections** Since March 2014, the CNIL may also remotely establish violations of the DPA. Two hundred online inspections were planned for 2015.	In the case of violations of the DPA, the CNIL may impose an administrative sanction, including: (i) a warning; (ii) a fine of up to €150,000 (or up to €300,000 in the case of a repeated breach within five years) if the CNIL served formal notice on the Data Controller to cease its non-compliance within a given deadline and the Data Controller did not comply with the notice served; (iii) an injunction to cease the Processing; or (iv) a withdrawal of the authorisation granted. The CNIL may make its sanction public by publishing it on its website and ordering its publication in French journals, newspapers or other media.	In addition, the CNIL may refer the case to the French public prosecutor, or a Data Subject may raise a criminal complaint and a French judge may impose a criminal sanction, which may lead to up to five years' imprisonment and a fine of up to €300,000 (for individuals) or a fine of up to €1.5 million (if the company is held liable).

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The CNIL is regarded as being an active regulator. Nevertheless, the CNIL usually issues a warning or serves formal notice on the Data Controller to cease its non-compliance within a given deadline. The CNIL imposes a fine only if the Data Controller does not comply with the notice served within this deadline.

Examples of recent enforcement action brought by the CNIL:

- In January 2014, Google Inc. was fined €150,000 for various violations of the DPA (such as the failure to provide complete notice to Data Subjects). This is the highest fine imposed by the CNIL to date.
- In August 2014, the CNIL issued a public warning against the French telecommunications service provider, Orange, for having failed to ensure the security and confidentiality of its customers' Personal Data. In April 2014, Orange notified the CNIL of a data security breach due to a technical failure of one of its Data Processors. Orange was sanctioned in particular for not having carried out a security audit of the application specifically developed by the Data Processor, prior to using that application.
- In November 2015, the CNIL imposed a fine of €50,000 on Optical Center, a distributor of optical products, for violations related to the security and confidentiality of its customers' Personal Data.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The collection and transfer of Personal Data are both Processing activities subject to the key data protection principles set out in the DPA (see question 3.1 above). Companies typically must:

- ensure that they have a legal basis to process the Personal Data (typically, companies rely on their legitimate interest to process the data; however, in the context of discovery, this requires the data to be processed in accordance with the Hague Convention and the French Blocking Statute);
- ensure that only the necessary Personal Data are processed, e.g., by using a filtering mechanism in France;
- provide notice to Data Subjects at the time of recording their data;
- ensure that the Personal Data are processed in compliance with general obligations of secrecy and confidentiality and only retained for the duration of the investigation/proceeding; and
- ensure that their existing registrations with the CNIL reflect the transfer of Personal Data and that they have an appropriate data transfer mechanism in place (see question 8.2 above).

15.2 What guidance has the data protection authority(ies) issued?

In July 2009, the CNIL issued guidance on the transfer of Personal Data in the context of discovery proceedings. The guidance reflects the key data protection principles set out in the DPA (see question 3.1 above) which a Data Controller must adhere to when processing Personal Data in the context of discovery.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In March 2014, the CNIL's investigative powers were strengthened to allow the CNIL to identify remotely, from a computer connected to the Internet, violations of the DPA. As a result, the number of inspections carried out by the CNIL has recently increased. In most cases, however, no sanction is imposed as organisations remedy the situation by complying with the DPA. Over the past 12 months, the French Supreme Court has also issued important rulings. In particular, the French Supreme Court confirmed that an employer can read SMS messages sent or received by employees on company-issued devices, without the employees being present, unless such SMS messages have been identified as private.

16.2 What "hot topics" are currently a focus for the data protection regulator?

Ensuring compliance of transatlantic data flows with the DPA is definitively an area of focus for the CNIL. In November 2015, the CNIL sent an email to organisations that have registered data transfers to the U.S. based on the Safe Harbour Principles, inviting them to implement the European Commission's Standard Contractual Clauses and update their registrations by the end of January 2016. The CNIL is currently analysing, within the Article 29 Working Party, the level of protection afforded by the new EU-U.S. arrangement known as the "Privacy Shield". Preparing organisations for their new obligations under the future EU General Data Protection Regulation constitutes another area of focus for the CNIL. In this respect, the CNIL already published in July 2015 new guides for carrying out Privacy Impact Assessments ("**PIAs**") to help Data Controllers to implement the principle of "Privacy by design".

Claire François
Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 58 00
Email: cfrancois@hunton.com
URL: www.hunton.com

Claire is a French qualified lawyer and advises a broad spectrum of clients on EU and French data protection and cybersecurity matters, including implementation of global data management strategies, international data transfers, and local data compliance. Claire also regularly represents clients before the French Data Protection Authority.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by *Computerworld* for four consecutive years as the top law firm globally for privacy and data security. *Chambers & Partners* ranks Hunton & Williams as the top privacy and data security practice in its *Chambers & Partners UK*, *Chambers Global* and *Chambers USA* guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among the *National Law Journal*'s "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy and Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

This article appeared in the 2016 edition of The International Comparative Legal Guide to: Data Protection published by Global Legal Group Ltd, London. www.iclg.co.uk

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International 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 Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

glg global legal group

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

www.iclg.co.uk