Data Protection: France

Resource type: Articles: know-how

Status: Law stated as at 01-Apr-2011

Jurisdiction: France

A Q&A guide to data protection in France.

This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects; rights to access personal data or object to its collection; and security requirements. It also covers cookies and spam; data processing by third parties; and the international transfer of data. This article also details the national regulator; its enforcement powers; and sanctions and remedies.

This article is part of the PLC multi-jurisdictional guide to data protection. For a full list of contents, please visit *www.practicallaw.com/dataprotectionhandbook*.

Stefan Naumann and Rémi Auba Bresson, SNR Denton

Contents

Regulation

1. What national law(s) regulate the collection and use of personal data? If applicable, has Directive 95/46/EC on data protection (Data Protection Directive) been implemented?

The collection and use of personal data is mainly regulated by the Act relating to data processing, data files and individual liberties (*Loi 78-17 relative à l'informatique, aux fichiers et aux libertés*) of 6

January 1978 (Data Processing Act).

The Data Processing Act refers to a number of other pieces of legislation including articles of the French Penal Code and French labour laws. It was thoroughly overhauled in 2004 by the Act relating to the protection of natural persons with respect to private data processing, which implemented the Data Protection Directive into French law.

A number of other EC Directives dealing with the collection and use of personal data were implemented into French law, including:

- Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
- Directive 2002/58/EC on the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive).

These were both implemented, notably by the Data Processing Act and Act 2004-575 (Act for the confidence in the digital economy), and partially codified in the French Code of Post and Electronic Communications. Decree 2005-1309 (as amended in 2007) was issued to determine some implementation provisions of the Data Processing Act.

In addition, Directive 2009/136/EC on consumer protection and users' rights in relation to the processing of personal data and the protection of privacy in electronic communications (Citizens' Rights Directive), which amends the Privacy and Electronic Communications Directive, should be implemented into French law before 25 May 2011. In this context, and under Article 11 of the Data Processing Act, the French Data Protection Agency (*Commission national de l'informatique et des libertés*) (CNIL) will be consulted regarding the implementation bill that is likely to change a number of aspects of French data protection law, including the rules governing the use of cookies (*see Question 17*).

2. To whom do the rules apply (EU: data controller)?

The Data Processing Act applies to data controllers, data processors and the recipients of the processed data (*Article 3, Data Processing Act*).

A data controller is the natural person, public authority, service or organisation that determines the purposes and the means of the data processing (*Data Processing Act*).

A data processor is any natural person or entity that processes the data on behalf of the data controller and under the data controller's instructions (*Article 35, Data Processing Act*).

3. What data is regulated (EU: personal data)?

The Data Processing Act regulates personal data (*Article 2, Data Processing Act*).

The term "personal data" is defined broadly under Article 2; it covers any information relating to a natural person who is, or can be, identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him.

To determine whether a person is identifiable, all the means that the data controller, or any other

person, uses or may have access to must be taken into consideration.

4. What acts are regulated (EU: processing)?

The Data Processing Act regulates:

- The automatic processing of personal data.
- The non-automatic processing of personal data provided this non-automatic processing deals with data contained in a personal data file or purports to file this data in such a file (*Article 2, Data Processing Act*).

"Data processing" is defined as any operation, or series of operations, performed on data, regardless of the kind of process used, including (*Data Processing Act*):

- Collecting.
- Saving.
- Adapting or editing.
- Extracting.
- Consulting.
- Using.
- Broadcasting.
- Linking or interconnecting.
- Locking, deleting or destroying.

A personal data file is any kind of structured and stable set of personal data that is accessible according to pre-defined criteria (*Data Processing Act*).

5. What is the jurisdictional scope of the rules?

The Data Processing Act applies to any data processing where the data controller is either (*Article 5, Data Processing Act*):

- Established in France.
- Not established in France, or anywhere else in the EU, but uses means of processing that are located in France (unless the data processing merely transits via France or another member state).

A data controller is deemed to be "settled on French soil" when the data controller practises an activity on French territory in the scope of an establishment, regardless of its legal form.

6. What are the main exemptions (if any)?

The Act does not apply to data processing carried out for the exercise of exclusively private activities (*Article 2, Data Processing Act*).

In 2004 the Data Processing Act was amended to take into account the profound changes brought about by the internet. As a result, the Data Processing Act now expressly exempts any temporary copies of personal data made by internet service providers for the purpose of providing faster internet access (*Article 4, Data Processing Act*). This exemption notably encompasses the use of proxy servers by internet service providers.

7. Is notification or registration required before processing data? If so, please provide brief details.

Chapter IV of the Data Processing Act sets out the required formalities that must be accomplished before starting a data processing. Depending on the type of data processing involved, the data controller must comply with one of four different sets of formalities.

Mere information (exemption of notification or registration)

The data controller only has to inform data subjects who requested information relating to the data processing, provided the processing is either (*Article 22, Chapters II and IV, Data Processing Act*):

- For the sole purpose of keeping a register which, under legal or regulatory provisions, is exclusively intended for the general public's information and can be consulted by the general public or anyone who can demonstrate a legitimate interest.
- In the scope of a non-profit religious, philosophical, political or trade union organisation.

Under this information requirement, the data controller must inform the data subjects of:

- The denomination and purpose of the data processing.
- The identity and address of the data controller.
- The occupation of the person or service to which the data subject should address his request to gain access to the data concerning him.
- The categories of data being processed and the recipients.
- Whether the data is transferred to a country located outside the EU.

The CNIL has currently issued 15 exemption standards to exonerate some categories of

processing from prior notification or registration (*Article 22, Chapter II, Data Processing Act*). For a complete list, see: *www.cnil.fr/nc/en-savoir-plus/deliberations/dispenses-de-declaration/?delib%5Bcur%5D=1*.

Simplified notification (*déclaration simplifiée*) and unique authorisation (*autorisation unique*)

For the most common categories of processing of personal data, where violation of privacy or liberties is unlikely, the CNIL establishes and publishes standards intended to simplify the obligation to notify a processing to the CNIL. These standards specify the purposes of the processing covered by the simplified notification, the categories of personal data and the recipients to whom the personal data is disclosed.

Processing corresponding to one of these standards is subject to either:

- A simplified notification of conformity to the CNIL (*Article 24, Data Processing Act*).
- A unique authorisation (*Article 25, II, Data Processing Act*).

The CNIL has currently published 35 simplified notification standards and 26 unique authorisations. For a complete list, see *www.cnil.fr/nc/en-savoir-plus/deliberations/normes-simplifiees/?delib%5Bcur%5D=1* and *www.cnil.fr/en-savoir-plus/deliberations/autorisations-uniques*

Notification (*déclaration*)

This is the default regime, under which the data controller only has to:

- Notify the CNIL of his intention to start a personal data processing before the processing begins.
- Undertake that the processing complies with French data protection law (*Article 23, Data Processing Act*).

The CNIL sends an acknowledgment of receipt (*récépissé*) as soon as it receives the notification. The data controller can then start its processing. However, the CNIL can, at any time, verify whether the processing actually complies with French data protection law (*see Question 23*).

Authorisation

Prior authorisation from the CNIL is required for processing deemed potentially harmful to privacy and liberties. Article 25 of the Data Processing Act provides a list of types of processing which fall under this authorisation process, including:

- Processing, whether automatic or not, of data relating to criminal offences, convictions or security measures, except for those carried out by representatives of justice when necessary to carry out their task of defending data subjects.

- Automatic processing, the purpose of which is the combination of legal entities' files whose main purposes are different.
- Processing relating to data which contain the data subject's national identification number.

The CNIL has two months, renewable once, to grant or deny its authorisation. If the CNIL has not granted its authorisation within this period, the authorisation is denied and the processing cannot be legally started.

Under Article 30 of the Data Processing Act, the notifications and authorisation requests submitted to the CNIL must specify:

- The identity and address of the data controller.
- The purpose of the processing.
- If necessary, the combinations, with other processings.
- The personal data processed, its origin and the categories of data subjects.
- The period of storage of the processed information.
- The department responsible for the carrying out of the processing.
- The authorised recipients to whom the data can be disclosed.
- The function of the person or the department where the right of access is exercised (*see Question 13*).
- The steps taken to ensure the security of the processing and data, and, if necessary, information on recourse to a sub-contractor.
- If applicable, any transfer of personal data to a country that is not an EU member state.

Main data protection rules and principles

8. What are the main obligations imposed on data controllers to ensure that data is processed properly?

The data controllers must process the data in compliance with the rules set out under Article 6 of the Data Processing Act, as follows:

- Data must be collected and processed fairly and lawfully.
- Data must be collected for a determined, explicit and legitimate purpose and must not be

subsequently processed in a manner incompatible with this purpose.

- The collected data must be adequate, relevant and non-excessive regarding the purposes for which it was collected and subsequently processed.
- The data must be accurate, complete and up-to-date.
- The data must be stored in a form that allows the identification of the data subjects for a period no longer than necessary for the purposes for which it was obtained and processed.

Data processing for statistical, scientific and historical purposes should ordinarily be considered compatible with the initial purposes of the data collection (*Article 6, Data Processing Act*).

9. Is the consent of data subjects required before processing personal data? If so:

- **What rules are there concerning the form and content of consent? Does online consent suffice?**
- **Are there any special rules concerning consent by minors?**

Form and content of consent

The Data Processing Act does not define consent nor provide any indication as to its form and content. However, particularly sensitive data can only be collected with the data subject's express consent (*Article 8, Chapter II, Data Processing Act*).

Therefore, under the Data Processing Act and unless expressly mentioned otherwise, implied consent is sufficient. This follows the general principle of consent under French law, which is defined as any free, specific and informed indication of will, and generally does not require express consent.

In addition, as the Data Processing Act does not provide otherwise, and under the CNIL's recommendations, online consent is generally sufficient to comply with the consent requirement under the Data Processing Act.

Finally, in the specific case of consent given to a data controller for direct marketing purposes, express consent (opt-in rule) is required for use of such personal data (*see Question 18*).

Consent by minors

The Data Processing Act does not provide any indication in this respect. However, the CNIL has made a number of recommendations; data controllers should only collect minors' personal data if they both:

- Obtain the minors' legal guardians' consent.

- Provide clear information by specifying whether providing the personal data is mandatory and, if necessary, that the data will be transferred to third parties.

In addition, the collecting of sensitive data, as defined under Article 8 of the Data Processing Act, is prohibited with respect to minors.

Finally, regarding the collection of minors' personal data through the internet, the CNIL allows the webmaster to collect the minor's age and email address but no other kind of personal information.

10. If consent is not given, on what other grounds (if any) can processing be justified?

If consent is not given, the processing can be justified on the following grounds (*Article 7, Data Processing Act*):

- Compliance with any legal obligation to which the data controller is subject.
- Protection of the data subject's life.
- Performance of a public service mission entrusted to the data controller or the recipient of the processed data.
- Performance of either:
  - a contract to which the data subject is a party; or
  - pre-contractual measures undertaken at the data subject's request.
- The pursuit of the data controller's or recipient's legitimate interest, provided this does not contravene the data subject's interests, or fundamental rights and liberties.

11. Do special rules apply for certain types of personal data, for example sensitive data? If so, please provide brief details.

There are a number of special rules that must be complied with when processing certain types of personal data (*Chapter II, Section 2, Data Processing Act*).

The collecting and processing of sensitive data is prohibited; that is, data directly or indirectly disclosing the data subject's (*Article 8, I, Data Processing Act*):

- Racial or ethnic origins.
- Political, philosophical or religious opinions.
- Membership of a trade union.

- Health or sexual life.

However, there are exceptions to this general rule; Article 8, II of the Data Processing Act provides that when the purpose of the processing requires it, personal data can be used in processing:

- For which the data subject has given his express consent, except where the law provides that the personal data prohibition cannot be lifted by this express consent.
- Necessary to save human life, but to which the data subject cannot consent as a result of a legal incapacity or physical impossibility.
- Set up by a non-profit religious, philosophical, political or trade union organisation.
- Of personal data made public by the data subject.
- Necessary to the establishment, enforcing or defending of a legal claim.
- Performed by the French Institute of Statistics.

In addition, under Article 8, III of the Data Processing Act, if the data collected is meant to be quickly made anonymous, the CNIL may authorise the collection of sensitive data.

The processing of sensitive data is permitted if the processing has been authorised and is performed in the public's interest (*Article 8, IV, Data Processing Act*).

Processing personal data that relates to criminal offences and convictions is restricted, and may be set up exclusively by (*Article 9, Data Processing Act*):

- The courts, public authorities and legal entities that manage public services and those acting within the scope of their authority.
- Legal professionals, but strictly as required for the exercise of their functions as granted by law.
- Copyright collecting agencies acting on behalf of victims of infringements of the rights provided for in the Intellectual Property Code, and for the purposes of ensuring the defence of these rights.

Rights of individuals

12. What information should be provided to data subjects at the point of collection of the personal data?

The data subject must be provided with the following information when or before the personal data is collected (*Article 32, I, Data Protection Act*):

- The identity of the data processor and its representative.

- The purpose of the data processing.
- Whether or not the data subject must answer the questions.
- The potential consequences of not answering the questions.
- The recipient.
- The rights granted to the data subjects (*see Question 13*).
- Whether the data is transferred outside the EU.

13. What other specific rights (such as a right of access to personal data or the right to object to processing) are granted to data subjects?

The specific rights granted to data subjects are as follows (*Chapter V, Section 2, Data Processing Act*).

- **Right to object.** Any natural person has the right to object, for legitimate reasons, to his personal data being processed (*Article 38, Data Processing Act*). In addition, the data subject is entitled to object, at no cost to himself, to the use of his personal data for purposes of direct marketing. The data subject has no right to object where the processing is under a legal obligation, or where the right to object is excluded by an explicit provision of the decision authorising the processing.
- **Right to access.** Any data subject who is a natural person who can prove his identity has the right to access the following information by requesting the following from the data controller of a personal data processing:
  - confirmation of whether or not his personal data is being processed;
  - information relating to the purposes of the processing, the categories of personal data processed and the recipients;
  - if applicable, information relating to the transfer of the personal data outside the EU;
  - communication of the personal data as well as any available information regarding its origin; and
  - information enabling the data subject to understand and challenge the underlying logic of the automatic processing in the event a decision that directly impacts the data subject was taken based on this processing.

  In addition, the data controller must provide copies of any personal data if requested by the data subject (*Article 39, Data Protection Act*).

- **Right to rectification.** Any data subject who is a natural person who can prove his identity has a right of rectification (*Article 40, Data Protection Act*). That is, the data subject can demand that the data controller rectify, complete, update, lock or delete any personal data that is inaccurate, incomplete, ambiguous, out-of-date or expired, and which concerns the data subject, or whose collection, use, communication or conservation is prohibited.

Security requirements

14. What security requirements are imposed in relation to personal data?

The data controller must take all necessary security precautions, with respect to the nature of the data and the risks caused by the processing to preserve the safety of the data, and notably to prevent them from being distorted, damaged or accessed by non-authorised third parties (*Article 34, Data Processing Act*).

In October 2010, the CNIL published a "Guide to the security of personal data", setting out various essential recommendations to data controllers regarding the security of personal data, including:

- Carrying out, at the outset, a risk assessment to put in place a protection that is adequate to the type of personal data stored by the data controller.
- Creating a user account managing procedure with user profiles and privileges to restrict the number of people who can have access to the data.
- Securing the computers used to access the personal data (for example, lockdown, strict password policy, and so on).
- Securing access to the local network.
- Securing access to the premises where the data is physically stored.

15. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

There is no requirement to notify personal data security breaches to data subjects or the CNIL.

However, the CNIL must, under Article 11 of the Data Processing Act, inform the district attorney (*Procureur de la République*) of any personal data security breaches of which it is aware.

Processing by third parties

16. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

Article 35 of the Data Processing Act provides that private data cannot be processed by a data processor, a person acting under the authority of the data controller or data processor, unless they follow the data controller's instructions.

The data processor must offer adequate safeguards to ensure the setting up of the security and confidentiality measures (*see Question 14*). This requirement does not relieve the data controller from its obligation to check that these measures are complied with.

Finally, the data controller and the data processor must sign an agreement. This agreement must mention the obligations regarding the security and confidentiality measures imposed on the data processor. The agreement must also provide that the data processor can only act following the data controller's instructions.

Electronic communications

17. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

Data controllers can store cookies or equivalent devices on the data subject's terminal equipment provided the data controller (or its agent) clearly and fully informs the data subject of (*Article 32, II, Data Processing Act*):

- The purpose of this storage on the data subject's equipment.
- How to prevent this storage.

However, there is no obligation to inform the data subject in the event the storage of the cookies is either:

- Only meant to allow or facilitate electronic communication.
- Strictly necessary to provide an online communication that was expressly requested by the data subject.

With the implementation of the Citizens' Rights Directive into French law (*see Question 1*), the above rules may be modified in the near future.

18. What requirements are imposed on the sending of unsolicited electronic commercial communications ("spam")?

Unsolicited electronic commercial communications can only be sent if the intended recipient has given his prior consent to receiving this communication (*Article L 34-5, French Code of Post and Electronic Communications*).

In this context, "consent" is defined as any manifestation of specific and informed free will through which a person accepts that his personal data can be used for unsolicited commercial communication. Unsolicited commercial communication is defined as any message intended to

promote directly or indirectly, goods, services or the image of a person who sells these.

There are two exceptions as follows.

Pre-existing commercial relationship

In the context of a pre-existing commercial relationship, the sending of unsolicited electronic commercial communication is authorised but strictly controlled. The unsolicited electronic commercial communication can only be sent if all of the following apply:

- The recipient's e-mail address was collected directly from the recipient.
- This collection occurred within the context of the sale of a product or the providing of a service of a similar nature to the one intended to be advertised.
- The communication and the commercial relationship must involve the same two parties.
- The recipient must be expressly and unambiguously offered the possibility, at no cost to himself, to stop his e-mail address from being used both at the time it is collected and each and every time an additional unsolicited electronic commercial communication is sent to him.

Business-to-business communications

On 17 February 2005, the CNIL issued an opinion that Article L 34-5 of the French Code of Post and Electronic Communications must not be strictly applied to business-to-business communications. The CNIL authorised the sending of unsolicited electronic commercial communication to the work e-mail address of natural persons, without their prior consent if the communication is sent to natural persons in their capacity exercised within the company or public agency that assigned them the e-mail address used by the sender.

International transfer of data

19. What rules regulate the transfer of data outside your jurisdiction?

Transfers of personal data outside France are governed by three different sets of rules:

- **No specific formalities.** The transfer of personal data to EU/EEA countries is subject to the same rules regulating the transfer of personal data within France.
- **Notification.** The transfer of personal data must be notified to the CNIL under Article 23 of the Data Processing Act (*see Question 7*) when it is either:
  - to countries or companies recognised by the EU as ensuring an adequate level of protection. These currently include:
    - Andorra;

- Argentina;
- Canada;
- the Faroe Islands;
- Guernsey;
- Isle of Man;
- Israel;
- Jersey;
- Switzerland.

In addition, the European Commission considers that the US companies that are signatory to the Safe Harbor Agreement ensure an adequate level of protection and are thus subject to the same notification regime.

- made under paragraph 1, Article 69 of the Data Processing Act, whereby a data controller can transfer personal data to countries not recognised as ensuring an adequate level of protection if the data subject has given express consent to this transfer. A data controller can also transfer personal data to such countries if the transfer is necessary for one of the following reasons:
  - preserving the data subject's life;
  - protecting the public interest;
  - complying with obligations designed to ensure the establishment, exercise or defence of a legal claim;
  - the consultation, in accordance with legal conditions, of a public register that, according to laws and regulations, is intended for public information and is open for public consultation or consultation by any person demonstrating a legitimate interest;
  - the performance of a contract between the data controller and the data subject, or the steps taken at the request of the data subject before entering into a contract; or
  - the conclusion or performance of a contract, either concluded or to be concluded in the interest of the data subject between the data controller and a third party.

- **Authorisation.** A processing can ensure an adequate level of protection to the privacy and the

freedoms and fundamental rights of the data subject through contractual clauses or binding corporate rules (BCRs) governing the process (*paragraph 2, Article 69, Data Processing Act*). These can be authorised by the CNIL (*Article 25, Data Processing Act*) (*see Question 7*) using the "Transfer outside of the European Union Schedule".

For a non-EU/EEA company, a certified country, or a signatory to the Safe Harbor Agreement (in which case the transfer is not subject to any specific issue), the most efficient way to proceed with a transfer is by requesting the CNIL to authorise it under paragraph 2 of Article 69 of the Data Processing Act, using either contractual clauses or BCRs (*see Question 20*).

20. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

The CNIL was the first European data protection agency to offer data controllers the possibility to transfer private data using a data transfer agreement.

There are currently three different sets of standard contractual clauses providing a framework to data controllers in France wishing to transfer data outside an EU/EEA country. In addition, data controllers can draft their own data transfer agreements.

The three sets of standard contractual clauses are the Commission's standard contractual clauses:

- Decision 2010/87/EU governing controller to processor transfers.
- Decisions 2001/497/EC and 2004/915/EC, which are alternative standard clauses for controller to controller transfers.

The BCRs provide an alternative to data transfer agreements for multinational corporations. BCRs constitute a code of good practices based on European data protection standards, which multinational organisations can voluntarily adopt to ensure adequate safeguards for transfers of personal data between companies that are part of the same corporate group and are bound by these corporate rules.

A corporation can either draft BCRs from scratch or use the Article 29 Working Party's documents, which provide a framework and a "model checklist" for BCRs.

In October 2008, the Article 29 Working Party decided to launch a mutual recognition procedure to make the use of BCRs more attractive to corporations. Since October 2008, 19 data protection authorities have agreed to mutually recognise BCRs that have been approved by one of these agencies. The agencies engaged in the mutual recognition procedure are those of Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, France, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, The Netherlands, Norway, Slovenia, Spain and the UK.

21. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

Using a data transfer agreement is not sufficient, in itself, to legitimise a transfer. The data controller must request the CNIL's authorisation to transfer data outside the EU/EEA in this way,

and cannot start transferring data before it has received the CNIL's authorisation.

22. Does the relevant national regulator need to approve the data transfer agreement? If so, please provide brief details.

When the transfer serves a legitimate purpose, and if the data controller has used the standard contractual clauses in their entirety, the transfer is deemed by the CNIL to ensure an adequate level of protection (*Article 26(4), Data Protection Directive*).

Non-standard contractual clauses can also be used to set up data transfers. However, the CNIL does not encourage this use because:

- These clauses usually do not provide the same judicial safety.
- Any departure from the standard contractual clauses release the CNIL from its obligation to approve the contract, which could delay the authorisation process.

The CNIL assesses the level of protection afforded by non-standard contractual clauses on a case-by-case basis, and by reference to the level of protection ensured by the standard contractual clauses.

While the CNIL no longer requires the data controller to systematically send the transfer agreement together with the data transfer authorisation request, the CNIL can, at a later stage during its decision-making process, request to review the actual agreement.

Enforcement and sanctions

23. What are the enforcement powers of the national regulator?

Articles 11 and 44 of the Data Processing Act, as amended by the Act of 29 March 2011, set out the CNIL's enforcement powers. CNIL agents have the authority to check and inspect any data processing and, if necessary to their mission, to obtain copies of any relevant documents. They can:

- Collect any relevant information.
- Access computer programs.
- Be assisted by an expert.

The agents carrying out the on-site inspection must inform the person responsible for the site that he can object to the inspection, in which case the inspection can only take place once a judge has given the authorisation.

However, since 29 March 2011, when urgency justifies it (that is, where the circumstances leading to the inspection are serious, or where there is danger of evidence being destroyed or hidden), the judge's authorisation can be given before the inspection without the person responsible for the site being informed.

24. What are the sanctions and remedies for non-compliance with data protection laws? To what extent are the laws actively enforced?

Chapters VII and VIII of the Data Processing Act set out the administrative and criminal sanctions that can be imposed for non-compliance with data protection laws.

The selected committee of the CNIL can impose the following administrative sanctions (*Article 13, Chapter VII, Data Processing Act*):

- Publication of the sanctions imposed, as well as an order for the sanctioned person or entity to have the sanction published in newspapers (*Article 46, Data Processing Act*).
- A fine not exceeding EUR150,000 for a first violation, and not exceeding EUR300,000 (or no more than 5% of the benefit not including any taxes if the violator is a legal entity) for a repeated violation committed within five years of the first violation (*Articles 45 and 47, Data Processing Act*). (As at 1 April 2011, US$1 was about EUR0.7)
- An order to stop the processing for a determined or unlimited period of time (*Article 45, Data Processing Act*).
- A request, in summary proceedings, that the competent jurisdiction order any security measures necessary for the protection of the rights and freedoms mentioned in Article 1 of the Data Processing Act (*Articles 1 and 45, Data Processing Act*).

Chapter VII of the Data Processing Act sets out the criminal provisions. Impeding the action of the CNIL is punishable by a one-year prison sentence and a EUR15,000 fine (*Article 51, Data Processing Act*). In addition, the processing of personal data in violation of the Act may be punishable under the French Criminal Code (*Article 50, Data Protection Act*). Violation of a provision of the Data Processing Act by a natural person is punishable by a maximum fine of EUR300,000 and up to five years in prison.

Under the French Criminal Code, the maximum potential fines and penalties that a company can incur for breaching French data protection rules and regulations are as follows:

- Up to EUR1.5 million in fines for legal entities.
- Up to five years in prison for the person(s) responsible for breaching the rules and regulations.

In addition, legal entities can incur the following additional penalties:

- Prohibition to practice (indefinitely, or for up to five years) one or more professional or not-for-profit activities.
- Placement under judicial supervision for up to five years.
- The closure (indefinitely or for up to five years) of the office(s) that were used to commit the

incriminated acts.

- Exclusion from public procurements (indefinitely or for up to five years).
- Prohibition, for up to five years, to use cheques or credit cards.
- Seizure of the item(s) that permitted, or was meant to permit, the breaching of the rules and regulations.
- Publication of the ruling rendered against the legal entity.

These are the maximum fines, and have never actually been imposed. However, on 21 March 2011, the CNIL imposed a fine amounting to EUR100,000 on Google for multiple violations with respect to Google's "Maps", "Latitude" and "Street View" services.

The regulatory authority

National Agency on computer science and freedoms (*Commission national de l'informatique et des libertés*) (CNIL)

W *www.cnil.fr*

Main areas of responsibility. The CNIL is an independent administrative agency that monitors and enforces the Data Processing Act, and drafts data protection standards. It also advises on any data protection bill or decree, suggests to the government legislative or regulatory measures pertaining to data protection, and plays a major role in informing professionals and members of the public about data protection law, and their rights and obligations under the law.

Contributor details

Stefan Naumann

SNR Denton

T +33 1 53 05 16 00

F +33 1 53 05 97 27
E *stefan.naumann@snrdenton.com*
W *www.snrdenton.com*

Qualified. France, 1993; California, 1992; England and Wales, 2000

Areas of practice. Intellectual property (transactional and litigation); data protection; patent litigation; domain name arbitrator.

Recent transactions

- WIPO domain name decisions.
- Patent litigation: represented Instrumentation Laboratory in a successful patent infringement lawsuit with respect to medical devices that allow the diagnosis of blood coagulation disorders.
- Representing BioAgency in patent infringement litigation related to gamma / delta T cell activators research.
- Defending Dentsply International in patent cancellation lawsuit against European patent on dental instrument.
- Advice on data transfers to multinational corporations in the fields of apparel retail, pharmaceuticals, and semiconductor manufacturing industry.

Rémi Auba Bresson

SNR Denton

T +33 1 53 05 16 00
F +33 1 53 05 97 27
E *remi.auba-bresson@snrdenton.com*
W *www.snrdenton.com*

Qualified. New York, June 2011

Areas of practice. Intellectual property (transactional and litigation); data protection.

Resource information

Resource ID: 6-502-1481

Law stated date: 01-Apr-2011

Products: Data Protection , Data Protection 2011_12, PLC Commercial, PLC Cross-border, PLC Employment Law, PLC Financial Services, PLC IPIT & Communications, PLC Law Department, PLC Public Sector, PLC US Intellectual Property & Technology, PLC US Law Department Series: Country Q&A

Related content

Topics

Data protection (http://crossborder.practicallaw.com/topic8-103-1271)

Financial and corporate crime (http://crossborder.practicallaw.com/topic7-103-1182)

Miscellaneous: financial services (http://crossborder.practicallaw.com/topic1-201-4090)

Privacy (http://crossborder.practicallaw.com/topic6-383-8687)

Topics from other jurisdictions

Intellectual Property and Technology (http://crossborder.practicallaw.com/topic7-500-0077)

Privacy and Data Security (http://crossborder.practicallaw.com/topic6-383-8687)

Articles: know-how

Data Protection: Argentina (http://crossborder.practicallaw.com/topic6-502-5219)

Data Protection: Austria (http://crossborder.practicallaw.com/topic0-502-0328)

Data Protection: Belgium (http://crossborder.practicallaw.com/topic2-502-2977)

Data Protection: Canada (http://crossborder.practicallaw.com/topic6-502-0556)

Data Protection: Colombia (http://crossborder.practicallaw.com/topic7-502-5167)

Data Protection: Germany (http://crossborder.practicallaw.com/topic3-502-4080)

Data Protection: Hungary (http://crossborder.practicallaw.com/topic3-502-4056)

Data Protection: Ireland (http://crossborder.practicallaw.com/topic6-505-8262)

Data Protection: Italy (http://crossborder.practicallaw.com/topic9-502-4794)

Data Protection: Luxembourg (http://crossborder.practicallaw.com/topic6-502-0405)

Data Protection: Mexico (http://crossborder.practicallaw.com/topic8-502-5162)

Data Protection: Philippines (http://crossborder.practicallaw.com/topic0-503-0761)

Data Protection: Portugal (http://crossborder.practicallaw.com/topic2-502-1949)

Data Protection: Russian Federation (http://crossborder.practicallaw.com/topic2-502-2227)

Data Protection: South Africa (http://crossborder.practicallaw.com/topic5-503-0787)

Data Protection: Sweden (http://crossborder.practicallaw.com/topic8-502-0348)

Data Protection: Switzerland (http://crossborder.practicallaw.com/topic9-502-5369)

Data Protection: UK (England and Wales) (http://crossborder.practicallaw.com/topic1-502-1544)

Data Protection: United States (http://crossborder.practicallaw.com/topic6-502-0467)

Dealing with data breaches in Europe and beyond (http://crossborder.practicallaw.com/topic6-505-9638)