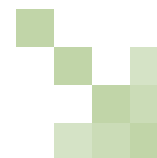


France

Thierry Dor, Gide Loyrette Nouel



www.practicallaw.com/5-385-6709

REGULATION

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

Data protection is primarily regulated by the Act No 78-17 on Data Processing, Data Files and Individual Liberties as amended by the Act No 2004-801 (DPA), which implemented the Data Protection Directive. Some provisions of the French Penal Code apply to breaches of data protection rules. The Decree No. 2005-1309, as amended by Decree No. 2007-457, contains provisions for the implementation of the DPA. In addition, the French Code of Post and Electronic Communications contains rules relating to collection and use of personal data, implementing some provisions of Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Electronic Commerce Directive) and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive).

More generally, rules of the French Civil Code on privacy as well as labour law rules applying to employee data may also have an impact on the processing of personal data.

The data protection authority is the *Commission nationale de l'informatique et des libertés* (CNIL).

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

The DPA provisions primarily apply to data controllers, that is, any individual, private entity, public authority, or any other organisation which determine the purposes and means of the data processing. Some provisions of the DPA also apply to data processors, that is, any individual or private entity processing personal data on behalf of data controllers (*Article 3, DPA*).

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

The DPA applies to personal data, defined as all the information concerning an individual, which is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to this person. To determine whether a person can be identified, all the identification resources the data controller or any other person uses or may have access to should be taken into consideration (*Article 2, DPA*). For example, a phone number or an ID picture are personal data.

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

The DPA applies to the automatic processing of personal data (*Article 2, DPA*).

Processing of personal data means any operation or set of operations in relation to personal data, whatever the mechanism used, particularly the obtaining, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

The DPA also applies to non-automatic processing of personal data, to the extent that the personal data is or will be included in a file (*Article 2, DPA*). A file means any structured and stable set of personal data that is accessible according to specific criteria.

5. What is the jurisdictional scope of the rules?

DPA provisions apply when (*Article 5, DPA*):

- The data controller is established on French territory. The data controller who carries out its activity on French territory within an establishment, whatever its legal form, is considered established on French territory.
- The data controller is not established on French territory or in another EU country, but uses means of processing situated on French territory, except for the processing used only for the purpose of transit through the French territory or the territory of another EU country.

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

The DPA provisions do not apply to processing carried out for the exercise of exclusively private activities.

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

The processing of personal data by an individual or a private entity is subject to one of the prior CNIL formalities: notification formalities (simplified notification or ordinary notification) or authorisation formalities (authorisation request or notification of

conformity with a unique authorisation), unless it benefits from an exemption. In addition, for processing carried out by the state or by public entities, a specific authorisation process applies.

The following are expressly exempted from prior formalities (*Article 22, DPA*):

- Processing whose purpose is keeping of a public register which, according to laws and regulations, is intended exclusively for public information and is open for public consultation or by any person demonstrating a legitimate interest.
- Processing carried out by an association or any other non-profit religious, philosophical, political or trade union body and limited to the functioning of that association or body.

The CNIL has adopted 13 exemption standards to exonerate some categories of common and harmless processing from prior CNIL formalities, provided they comply with the restrictions specified in such decisions, for example, exemption from notification for payroll processing carried out by private entities (*decision of 9 December 2004*) and exemption from notification for the processing relating to the management of suppliers' files (*decision of 18 January 2005*).

Non-automatic processing (that is, manual processing of files) is exempt from notification formalities, but not from authorisation formalities.

The data controller can appoint a personal data protection officer, who is in charge of ensuring the compliance with the obligations provided for by the DPA. The appointment of such officer must be notified to the CNIL. Such appointment exempts the data controller from notification formalities, but not from authorisation formalities.

In addition, exceptions apply to the processing of personal data carried out for the sole purpose of literary and artistic expression and professional journalism. In particular, subject to conditions, these processing are exempt from prior CNIL formalities.

Simplified notification

The DPA provides for the CNIL to establish and publish standards intended to simplify the obligation to notify relating to the most common categories of processing of personal data which are not likely to be a violation of privacy and liberties (*Article 24, DPA*). The CNIL has adopted 36 simplified notification standards, such as:

- For both private and public sectors, processing performed by the public and private authorities for the management of their staff (simplified standard No. 46 of 13 January 2005).
- For all organisations except bank institutions, insurance companies, health professionals, and professionals of the education sector, management of the files of clients and prospects (simplified standard No. 48 of 7 June 2005).

Ordinary notification

Ordinary notification applies by default, when the processing is neither exempted, nor subject to simplified notification or authorisation formalities.

Authorisation

The DPA requires prior authorisation of the CNIL for processing which are potentially harmful to privacy and liberties, in particular (*Article 25, DPA*):

- Processing, whether automatic or not, of data relating to offences and convictions, except for those carried out by representatives of justice when necessary to carry out their task of defending data subjects.
- Automatic processing which can, due to its nature, importance or purposes, exclude persons from the benefit of a right, a service or a contract in the absence of any legislative or regulatory provision.
- Processing relating to data which contain the social security number.
- Automatic processing of data including assessments of the social difficulties of individuals.
- Automatic processing including biometric data necessary for the verification of an individual's identity.

Unique authorisation

To simplify the authorisation procedure for some categories of personal data processing, the CNIL has adopted 17 unique authorisation standards, such as:

- For banking, finance and credit activities, unique authorisation No 5 of 9 July 2008, relating to credit scoring.
- In the labour field, unique authorisation No 4 of 8 December 2005, relating to whistle-blowing systems.

If the processing complies with the conditions of a unique authorisation standard, the data controller only needs to notify such conformity to the CNIL.

Authorisation by ministers or the Conseil d'Etat after an opinion of the CNIL

For processing of personal data carried out on behalf of the state or public entities, the DPA requires an authorisation of the competent minister or ministers (*Article 26, DPA*), or an authorisation of the *Conseil d'Etat* (*Article 27, DPA*) to be granted after an opinion of the CNIL.

Content of notifications and authorisation requests

Both ordinary notifications and authorisation requests must specify information such as (*Article 30, DPA*):

- Identity and address of the data controller (or its representative, if any).
- Purpose or the purposes of the processing.
- Personal data processed.
- Categories of recipients.
- Period of storage of the processed information.

- Any transfer of data which is envisaged towards a non-EU country.

Simplified notifications and notifications of conformity to a unique authorisation only require specific information concerning the data controller and the CNIL standard they are complying with.

Filing a formality with the CNIL is free of charge.

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 comply with the following obligations that the data must be (*Article 6, DPA*):

- Obtained and processed fairly and lawfully.
- Obtained for specified, explicit and legitimate purposes, and must not subsequently be processed in a manner that is incompatible with those purposes.
- Adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing.
- Accurate, complete and, where necessary, kept up-to-date. Appropriate steps must be taken to delete and rectify data that is inaccurate or incomplete in relation to the purposes for which it is obtained and processed.
- Stored in a form that allows the identification of the data subjects for a period no longer than necessary for the purposes for which they are obtained and processed.

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

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

Consent of data subjects is required before processing personal data unless at least one of the statutory justifications (*see Question 10*) is met (*Article 7, DPA*).

Form and content of consent

Even though the DPA does not give a specific definition of the notion of consent, consent is commonly defined under French law as any free, specific and informed indication of will. Generally, simple consent (that is, with no specific form) is sufficient. However, some processing are subject to express consent (that is, formal consent), for example, processing of sensitive data and transfers of personal data to third countries. Online consent is acceptable. In the specific case of consent given to a data controller

for canvassing purposes, express consent (opt-in rule) is required for use of such personal data:

- By the data controller's business partners.
- For the online offer of other products or services than the ones ordered at the time the consent was given.

The burden of proof relating to consent lies with the data controller and consent can be revoked by the data subject at any time.

Consent by minors

Generally, minors are legally considered as not having the capacity to give consent, except for ordinary everyday life acts. Whether consent obtained from a minor is valid depends on the actual circumstances, that is, the age of the minor and the extent to which the minor understands the consequences of giving consent. The same principle applies in relation to consent given for the processing of personal data. There is no specific provision in the DPA concerning consent by minors. However, the CNIL recommends that data controller adopts a cautious approach when obtaining minors' consent. The CNIL considers that in some circumstances, the consent of the parents is necessary (for example, collection of sensitive data or collection of a minor's contact details for marketing purposes).

10. If there is no consent, on what other grounds (if any) can processing be justified?

In case there is no consent, the processing can be justified in the following circumstances (*Article 7, DPA*):

- Compliance with any legal obligation which the data controller is subject to.
- Protection of the data subject's life.
- The performance of a public service mission entrusted to the data controller or the data recipient.
- The performance of either a contract to which the data subject is a party or steps taken at the request of the data subject before entering into a contract.
- The pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject.

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

Some processing of personal data such as the processing of sensitive data, the processing of personal data relating to offences and convictions, and the processing of personal data for the purpose of medical research, are potentially harmful to privacy and liberties, and therefore subject to specific restrictive rules.

The DPA prohibits the collection and processing of sensitive data defined as personal data which reveals, directly or indirectly, the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of persons, or which concern their health or sexual life (*Article 8, DPA*).

However, such prohibition does not apply in limited cases such as processing:

- For which the data subject has given his express consent, except in cases where the law provides that the above prohibition cannot be lifted by the consent of the data subject.
- Necessary for the protection of human life, but to which the data subject is unable to give his consent because of a legal incapacity or physical impossibility.
- Carried out by an association or any other non-profit religious, philosophical, political or trade union body and limited to the functioning of that association or body.
- Relating to personal data that the data subject has made public.
- That is necessary for the establishment, exercise or defence of a legal claim.

In addition, the processing of personal data relating to offences and convictions is restricted, and such processing may be put in place only by (*Article 9, DPA*):

- The courts, public authorities and legal entities that manage public services, within the scope of their attributions.
- Legal professionals, for the strict needs of the exercise of the functions granted to them by the law.
- Bodies for authors' rights management, on behalf of victims of infringements of the rights provided for in the French Intellectual Property Code, and for the purposes of ensuring the defence of these rights.

The processing of personal data for the purpose of medical research is also subject to specific rules (*Article 53 seq., DPA*).

RIGHTS OF INDIVIDUALS

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

The data controller must provide a data subject with the following information, except where he already has such information (*Article 32, DPA*):

- The identity of the data controller.
- The purposes of the processing for which the data is intended.
- The compulsory or optional nature of the replies to the questions.

- The possible consequences of the absence of a reply.
- The recipients or categories of recipients of the data.
- The rights granted to him (*see Question 13*).
- When applicable, the intended transfer of personal data to a non-EU country.

Whenever the personal data has not been obtained from the data subject, the data controller must at the time of recording the personal data or, if disclosure to a third party is planned, no later than the time when the data are first disclosed, provide the data subject with the above information. However, such obligation of information does not apply when informing the data subject proves impossible or would involve disproportionate efforts.

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?

Right of access (Article 39, DPA)

Any individual providing proof of identity is entitled to question a data controller to obtain information, such as:

- Confirmation as to whether his personal data is processed by the data controller.
- General information on the processing which should have been given at the time of collection of his personal data (*see Question 12*).
- In the case of a decision taken on the basis of automatic processing and producing legal effects in relation to the data subject, information allowing the data subject to know and to object the logic involved in the automatic processing.

Data subjects can receive a copy of their personal data held by the data controller at their request. Data controllers can require payment of a sum of money for the delivery of the copy which shall not exceed the cost of the copy.

Right of rectification (Article 40, DPA)

Any individual providing proof of identity can ask the data controller to, as the case may be, rectify, complete, update, block or delete personal data relating to him that is inaccurate, incomplete, equivocal, expired, or whose collection, usage, disclosure, or storage is prohibited.

At the request of the data subject, the data controller must justify, at no cost for the data subject, that it has carried out the necessary operations required as described in the previous paragraph.

Right to object (Article 38, DPA)

Any person is entitled, on legitimate grounds, to object to the processing of any personal data relating to him.

The data subject is entitled to object, at no cost to himself, to the use of his personal data for purposes of canvassing, in particular

for commercial ends, by the data controller.

There is no right of objection where the processing satisfies a legal obligation, or where an explicit provision of the decision that authorises the processing excludes the right of objection.

SECURITY REQUIREMENTS

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

The data controller must take all useful precautions, in relation to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent its alteration and damage (that is, protect both its physical and logical integrity), or prevent access by non-authorised parties (that is, protect its confidentiality) (*Article 34, DPA*).

In relation to the security of personal data processing, the CNIL recommends:

- A control of hardware and software reliability.
- The security of information technology systems.
- An assessment of risks and a general security study for each new processing.
- The implementation of an internal security code defining the security rules and procedures.
- The allocation of responsibilities between the persons in charge of security.

In addition, the CNIL recommends specific security requirements relating to access, connection, encryption and so on, depending on the category of data processed and the economic sector concerned.

PROCESSING BY THIRD PARTIES

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

A data processor, or a person who acts on behalf of the data controller can process personal data only under the data controller's instructions.

A data processor must offer adequate guarantees to ensure the implementation of security and confidentiality measures (see *Question 14*). This requirement does not exempt the data controller from its supervision obligations.

A written contract must be concluded between the data controller and the data processor. It must specify the obligations of the data processor in relation to the protection of the security and confidentiality of the data and provide that the data processor can only act on the instructions of the data controller (*Article 35, DPA*).

If the data processor is established outside the EU/EEA, the transfer of personal data to the data processor is subject to the rules on international transfer (see *Question 16*).

INTERNATIONAL TRANSFER OF DATA

16. What rules govern the transfer of data outside your jurisdiction?

EU/EEA countries

Personal data transfers towards an EU/EEA country are possible without any specific formality.

Countries recognised by the European Commission as offering an adequate level of protection

The European Commission (Commission) has adopted adequacy decisions making personal data transfers towards the following countries possible without specific formalities:

- Argentina.
- Canada.
- Guernsey.
- Isle of Man.
- Jersey.
- Switzerland.
- US (where the US company is a signatory to the Safe Harbor Agreement or under the 2007 Agreement on the processing and transfer of Passenger Name Records).

Other countries

A data controller cannot transfer personal data to any other country, except in the following cases (*Article 69, DPA*):

- The data subject has expressly consented to the transfer.
- The transfer is necessary for:
 - the protection of the data subject's life;
 - the protection of the public interest;
 - the meeting of obligations ensuring 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 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;

- 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.

A transfer can also be authorised by a decision of the CNIL where the processing guarantees a sufficient level of protection of individuals' privacy, liberties and fundamental rights, particularly on account of contractual clauses (data transfer agreement) or binding corporate rules (BCRs) relating to the processing (see *Question 17*).

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

Transfer of personal data to third countries can be secured by two types of instruments:

Data transfer agreements

A data transfer agreement is an agreement for the transfer of personal data between at least two parties. When a data transfer agreement is based on the Commission's standard contractual clauses (EC Clauses) for transfers to third countries (Commission Decision No. 2002/16/CE, concerning data transfers from data controller to data processor; Decision No. 2001/497/CE and Commission Decision No. 2004/915/CE, concerning data transfers from data controller to data controller), the CNIL will authorise the transfer without further review. For that reason, most data transfer agreements are based on EC Clauses. A copy of the data transfer agreement must be sent to the CNIL (see *Question 19*).

BCRs

The BCRs constitute a code of good practices based on European data protection standards, which multinational organisations can draw up and follow voluntarily to ensure adequate safeguards for transfers of personal data between companies that are part of a same corporate group and are bound by these corporate rules.

In practice, when they have the choice, multinational companies tend to prefer data transfer agreements based on the EC Clauses rather than the BCRs, because of the long approval procedure of the BCRs by the data protection authorities. However, the situation may change as the BCRs could become more attractive. In October 2008, the Article 29 Working Party decided to launch a mutual recognition procedure. The data protection authorities of France, Germany, Ireland, Italy, Latvia, Luxembourg, the Netherlands, Spain and the UK, joined in December 2008 by Cyprus, Iceland, Liechtenstein and Norway, agreed to engage to mutually recognise the BCRs, that is, provide their authorisation without further review once a draft with a positive opinion is circulated by the data protection authority co-ordinating the approval procedure.

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

Provided the general requirements for making the processing legitimate are met (see *Questions 8 to 11*), a data transfer agreement is not sufficient and CNIL authorisation is still needed (see *Question 17*).

THE REGULATORY AUTHORITY

Commission nationale de l'informatique et des libertés (CNIL)

W www.cnil.fr

Main area of responsibility. The CNIL is responsible for supervising compliance with the DPA.

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

Data transfer agreements based on the EC Clauses are systematically approved by the CNIL (see *Question 17*).

Other data transfer agreements are reviewed by the CNIL. The CNIL will authorise the transfer only if the agreement provides sufficient guarantees. The CNIL assesses the guarantees provided with reference to those resulting from the EC Clauses (see *Question 16*).

ENFORCEMENT AND SANCTIONS

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

CNIL agents can conduct on-site inspections to carry out verifications relating to all processing by a data controller and to obtain copies of useful documents (*Article 11, DPA*).

The CNIL can issue a warning to a data controller that does not comply with the obligations resulting from the DPA. It can also order the data controller to cease the non-compliance within a time limit that it determines.

If the data controller is in breach, the CNIL can notably:

- Impose a financial penalty (*Article 45, DPA*) (see *Question 21*).
- Issue an injunction to stop the processing (*Article 45, DPA*).
- Ask, in summary proceedings, the competent jurisdiction to order any security measure necessary for the protection of human identity, human rights, privacy or individual or public liberties (*Article 45, DPA*).
- Inform the Public Prosecutor of offences of which it has knowledge and present its remarks in criminal proceedings (*Article 11, DPA*).

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

Administrative sanctions

The CNIL may impose a financial penalty which shall be of an amount that is proportional to the seriousness of the breach committed and the profits obtained from the breach.

For the first breach, the penalty cannot exceed EUR150,000 (US\$190,100). For the second breach within five years from the date when the previous financial penalty becomes definitive, the penalty cannot exceed EUR300,000 (US\$380,200) or, for a private entity, 5% of turnover for the latest financial year, with a maximum of EUR300,000 (*Article 47, DPA*).

Criminal sanctions

Impeding the action of the CNIL is punishable by one year imprisonment and a fine of EUR15,000 (about US\$19,000) (*Article 51, DPA*).

The processing of personal data in violation of the DPA can constitute criminal offences sanctioned by the French Penal Code (*Article 50, DPA*).

The major criminal offences are punishable by a maximum fine of EUR300,000 and up to five year imprisonment, in particular:

- Failure to comply with:
 - the formalities required by the DPA before the processing of personal data;
 - an injunction to stop the processing or the withdrawal of an authorisation;
 - the simplified notification or exemption standards when they are applicable (*see Question 7*);
 - the rules applicable to the transfer of personal data to a non-EU country (*see Question 16*).
- Failure to implement the security measures required by the DPA.
- Collection of personal data by fraudulent, unfair or unlawful means.
- Processing personal data of a natural person despite that person's objection, when the processing is done for canvassing purposes, or when the objection is founded on legitimate grounds.
- Recording and preserving in computerised memory sensitive data of a person without his express consent.
- Retaining personal data beyond the applicable retention period.

The penalties applicable to private entities for such criminal offences are a maximum fine of EUR1.5 million (about US\$1.9 million) and additional sanctions including placement under judicial supervision, closure of establishment and disqualification for public tenders.

The following minor criminal offences are punishable by a maximum fine of EUR1,500 (about US\$1,900) (EUR3,000 (about US\$3,800) in case of second offence within one year):

- Failure to comply with the rules concerning the information to be provided to the data subject (*see Question 12*).
- Failure to answer the requests of a data subject exercising his right of access (*see Question 13*).
- Failure to deliver a copy of the personal data of an individual requesting it (*see Question 13*).
- Failure to implement the changes requested by a data subject exercising his right of rectification (*see Question 13*).

When the offender is a private entity, such criminal offences are punishable by a maximum fine of EUR7,500 (about US\$9,500), or EUR15,000 (about US\$19,000) in case of second offence within one year.

The above administrative and criminal sanctions are theoretical maximum levels, and in practice, the penalties that have actually been imposed by the CNIL or by the courts in data protection matters are much lower.

CONTRIBUTOR DETAILS

Thierry Dor
Gide Loyrette Nouel
 T +33 (0)1 40 75 29 46
 F +33 (0)1 40 75 37 98
 E dor@gide.com
 W www.gide.com

Areas of practice/expertise. Thierry Dor is the partner in charge of information technology law in the Intellectual Property, Telecommunication, Media and Technology Department of Gide Loyrette Nouel in Paris. He has substantial experience in the field of information technology projects, internet, e-commerce, software and data base protection, and personal data processing and transfers.

Partners in know-how
www.practicallaw.com

PRACTICAL LAW COMPANY