Data protection in France: overview

by Myria Saarinen, Elise Auvray and Floriane Cruchet, Latham & Watkins

Country Q&A | Law stated as at 01-Dec-2018 | 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.

To compare answers across multiple jurisdictions, visit the Data protection *Country Q&A tool*.

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

Regulation

Legislation

1. What national laws regulate the collection and use of personal data?

General laws
The key national regulations relating to personal data are:

- Act No. 78-17 on Information Technology, Data Files and Civil Liberties dated 6 January 1978, as amended by Act No. 2018-493 dated 20 June 2018 on Personal Data Protection, (DPA), which:
  - incorporates certain provisions of Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR)), which came into application on 25 May 2018;
  - takes a position on some of the opening clauses of the GDPR; and
  - implements Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

Following the enactment of Act No. 2018-493, the DPA only partially complies with the GDPR, as a number of provisions of the DPA need to be revoked and certain provisions of the GDPR need to be implemented. For the time being, the DPA must be read in combination with the GDPR, with the GDPR taking precedence in the case of conflicting provisions. Under Act No. 2018-493, the French Government has until December 2018 to overhaul the DPA to provide a simple and coherent new legislative scheme, and will need to pass an ordinance to do so.

- Decree No. 2005-1309 of 20 October 2005, modified by Decree No. 2018-687 of 1 August 2018 (DPA Decree), which takes the amended DPA into consideration.

The French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*) (CNIL) supervises the enforcement of the DPA and frequently issues decisions and guidelines on the DPA.

See box, *Regulator details*.

Sectoral laws

There are a bundle of laws and regulations relating to personal data protection regulating specific sectors, including the:

- Postal and Electronic Communications Code (*Articles L.34 et seq and Articles R.10 et seq*) (regulating the provision of online electronic communication services to the public).
- Consumer Code (*Articles L.223-1 et seq*) (on telemarketing).
- Public Health Code (*Articles L.1110-4 et seq, L.1111-8 et seq, L.1115-1 et seq, L.1122-1 et seq, L.1435-6, L.1460-1 et seq, R.1111-1 et seq*) (on the processing of health data).
- Property Code (*Article L.212-3*) (on the retention of personal data contained in public archives).

These provisions have not been amended following the entry into application of the GDPR.

Scope of legislation

2. To whom do the laws apply?

The DPA applies to:

- **Data controllers.** A data controller is any natural or legal person, public authority, agency or any other body that determines the purposes and the means of the data processing.
- **Data processors.** A data processor is any natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller.

- **Data recipients.** A data recipient is any authorised person to whom the data is disclosed (other than the data subject, the data controller, the sub-contractor and persons who, due to their functions, are in charge of processing the data).

The DPA also provides rights and guarantees to data subjects (that is, individuals whose data is processed).

Whether a person is a data controller, data recipient, data processor or data subject is determined on a case-by-case basis, regardless of what has been agreed by parties to an agreement.

Other categories of persons are also subject to the DPA, such as communications service providers (*see Question 16*).

3. What data is regulated?

The DPA applies to the processing of personal data.

Personal data is defined as any information relating to a natural person who is or can be identified, either directly or indirectly, by reference to an identification number or to one or more factors specific to them (*Article 2, DPA*). This includes, for example, a person's name, date of birth, telephone number, email address and social security number. To determine whether a person is identifiable, all the means that the data controller or any other person uses or has access to must be taken in consideration.

In a decision dated 3 November 2016, the French Supreme Court (*Cour de cassation*) put an end to the conflicting rulings of lower courts, holding that IP addresses must be considered as personal data. This decision is in line with a previous ruling of the European Court of Justice where the court held that dynamic IP addresses held by a website operator are personal data where the operator has "the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person" (*Breyer v Bundesrepublik Deutschland, Case C-582/14*).

Special categories of data are those that:

- Reveal, either directly or indirectly, racial and ethnic origin.
- Reveal, either directly or indirectly, political, philosophical or religious opinions.
- Reveal, either directly or indirectly, trade union membership or affiliation.
- Constitute genetic or biometric data.
- Include details about health, sexual orientation or sex life.

4. What acts are regulated?

The DPA regulates the automatic and non-automatic processing of personal data that is or may be contained in a personal data filing system. There is an exception for processing carried out for the exercise of exclusively private activities.

Processing of personal data is broadly defined under the DPA and means any operation or set of operations in relation to the data, regardless of the mechanism used, especially (*Article 2, DPA*):

- Collecting.
- Recording.
- Organisation.
- Retention.
- Adaptation or alteration.
- Retrieval.
- Consultation.
- Use.
- Disclosure by transmission.
- Dissemination or otherwise making available.
- Alignment or combination.
- Restriction.
- Deletion or destruction.

In a company, most personal data is processed in relation to human resources management, information technology or clients and prospects, for example:

- Recruitment.
- Payroll.
- Client and prospective client files.
- Whistleblowing hotlines.
- CCTV.
- Electronic devices.

5. What is the jurisdictional scope of the rules?

The DPA is not fully consistent with the rules on jurisdiction of Article 3 of the GDPR, which will prevail in cases of conflict.

The national rules adopted in areas for which the GDPR allows member states to legislate (for example, age of consent) apply to data subjects residing in France even if the data controller is not established in France, except for processing relating to freedom of expression and information where the applicable law is that of the EU member state where the data controller is established (*Article 5-1, DPA*). There is an "establishment" where there is an effective and real exercise of an activity through stable facilities. A data controller that is not established in France or an EU member state must designate a representative in France.

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

The DPA does not apply to:

- Data processing carried out for the exercise of exclusively private activities (for example, a personal address book).
- Temporary copies made in the context of technical operations of transmission and provision of access to a digital network, for the purpose of automatic, intermediate and transitory retention of data and with the sole aim of allowing other recipients of the service to benefit from the best access possible to the transmitted information (*Article 4, DPA*).

Notification

7. Is notification or registration required before processing data?

The prior filing requirements with the CNIL have been abolished following the entry into application of the GDPR. However, prior formal requirements still apply to the following three types of processing:

- **Processing of health data.** These processing activities must be:
  - compatible with the CNIL's certification criteria or standard regulations; and
  - implemented after the data controller has submitted a declaration of certified conformity.

A processing activity that does not conform with a certification or standard regulation can only be implemented after being duly authorised by the CNIL. The CNIL must issue its decision within two months from receipt of a request for authorisation. This time period can be extended once by a reasoned decision of the President of the CNIL or when the case is submitted to the National Institute of Health Data. A request is deemed accepted if the CNIL does not issue an opinion within this period (*Article 54, DPA*).

- **Processing implemented on behalf of the state.** These processing activities must be duly authorised by order of the relevant minister taken after a reasoned and published notice of the CNIL if they relate to either:
  - national security, defence or public health; or
  - the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

  (*Article 26 I, DPA*.)

  Processing that also concerns the special categories of data listed in Article 8 of the DPA must be duly authorised by a decree taken after a reasoned and published notice of the CNIL (*Article 26 II, DPA*). Additionally, all processing activities implemented on behalf of the state in the exercise of its prerogatives of public powers, which include genetic data or biometric data and are necessary for the authentication or control of the identity of individuals, must be duly authorised by a decree taken after a reasoned and published notice of the CNIL (*Article 27, DPA*).
- **Processing of social security numbers.** The DPA maintains a protective regime for the processing of social security numbers, known in France as directory registration numbers (*Numéros d'Inscription au Répertoire* (NIRs)), but has lightened the applicable formalities (*Article 22, DPA*).

The DPA envisages the adoption of a framework decree, to be enacted after a reasoned and published notice of the CNIL, which will enable certain categories of data processors to bypass the CNIL formalities when processing personal data for specific purposes.

Main data protection rules and principles

Main obligations and processing requirements

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

The data controller must ensure that personal data is:

- Collected and processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes, and subsequently processed in a manner that is compatible with those purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate, complete and kept up to date (every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy)).
- Kept in a form that allows identification of the data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

Data subjects must receive appropriate information about the processing, unless they have already received all relevant information (*Articles 13 and 14, GDPR*). Article 32 of the DPA, which has been applicable since the entry into force of the Digital Republic Law of 7 October 2016, also provides that data subjects must obtain information on their right to define guidelines concerning the processing of their personal data after their death.

The data controller must take all useful precautions to preserve the security of the data, having regard to the nature of the data and the risks presented by the processing (*Article 34, DPA*) (*see Question 15*).

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

A data controller can lawfully justify the processing of personal data if it has received the previous, free, non-ambiguous and informed consent of the data subject. In practice, consent must be given in French (provided that the data subject is a French speaker), either in writing or by a click-through, if given over the internet.

Express consent is required in specific cases for:

- The processing of sensitive data (unless another legal ground can be used under Article 8 II of the DPA).
- Re-use of data for different purposes.
- Commercial market research.
- Cookies.

After heated debates between the National Assembly and the Senate, French law now determines that a minor can consent alone to the processing of his or her data in relation to information society services on reaching the age of 15 (*Article 7-1, DPA*). This position, defended by the National Assembly and approved by the French Constitutional Council (*Conseil Constitutionnel*), aims to ensure consistency with other legislation currently applicable (for example, a 15-year-old can already request his or her doctor not to disclose medical information related to him or her). If the minor is less than 15 years and the processing is based on consent, the processing activity requires both the consent of the minor and that of the holder of parental rights. The Constitutional Council has ruled that the GDPR allows member states to decide either that:

- Consent is given for the minor by the holder of parental rights.
- The minor is authorised by the holder of parental rights to consent (double consent).

Clear information must be provided to the minor, using terms that are adapted to his/her age. Adequate vigilance and warning systems must be implemented (such as awareness messages, age controls, or possibility of parental supervision).

Where personal data is provided to a third party (who is also a data controller) and there is a deletion request, the data controller that was asked to delete the data must take reasonable measures to inform the third party of the deletion request.

Obtaining consent from employees is subject to certain exceptions because it is assumed that they cannot freely consent. The employer must rely on other grounds to justify data processing.

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

The processing of personal data can be justified on any of the following grounds:

- Compliance with any legal obligation to which the data controller is subject.
- Protection of the data subject's life or that of any other natural person.
- Performance of a public service mission.
- Performance of a contract to which the data subject is a party (or of steps taken at the request of the data subject before entering into a contract).
- Pursuit of the data controller's or data recipient's legitimate interest, provided that it is not incompatible with the interests or fundamental rights and liberties of the data subject.

(*Article 7, DPA; Article 6, GDPR*.)

Special rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

As a general principle, the collection and processing of sensitive data is prohibited (*Article 8, DPA*). Sensitive data include, among others, data related to racial or ethnic origin, political opinions, religious or philosophical beliefs,

trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation.

However, this prohibition may be lifted, subject to certain conditions, such as when the processing is:

- Expressly consented to by the data subject.
- Necessary for the protection of human life.
- Carried out by an association or any other non-profit organisation of a religious, philosophical, political or trade union nature.
- Based on personal data that was made public.
- Necessary to establish, exercise or defend a legal claim.
- Necessary for certain medical purposes.
- Carried out for statistical purposes.
- Related to health data processed for public interest purposes.
- Related to biometric data that is strictly necessary for the control of access to workplaces as well as for equipment and applications used by employees, agents, trainees or service providers in their assignments.
- Related to the re-use of public information contained in judgments and decisions.
- Necessary for public research.

Processing data relating to offences, convictions and security measures can only be done by a limited number of persons identified in Article 9 of the DPA and Article 41 of the DPA Decree. The French Constitutional Council invalidated a 2004 law amending the DPA under which legal persons could process data relating to offences, convictions and security measures when they were either the victims of offences themselves or acting on behalf of victims, provided that the processing was aimed at preventing and combating fraud or making reparation for the resulting harm suffered. The Constitutional Council held that these terms were not precise enough to bring a sufficient level of protection with regards to the sensitivity of the data and the probability that such processing activity could be carried out on a large scale. The DPA, as amended in 2018, now specifies that both legal and natural persons can process data relating to offences, convictions and security measures to:

- Prepare and, if necessary, bring and follow legal proceedings as a victim, a person of interest or someone acting on behalf of a victim or person of interest.
- Enable the execution of a judgment.

The processing activity can only last for as long as is strictly necessary to achieve these aims.

The CNIL has established a regime of strict control over the processing of NIRs, as these can provide access to a significant amount of personal data and connections to many databases (*see Question 7*).

Rights of individuals

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

Data subjects must be given information on how personal data will be processed at the time the data is collected, unless they have already received all relevant information (*Article 13, GDPR*). Additionally, Article 32 of the DPA provides that data subjects must obtain information on their right to define guidelines concerning the processing of their personal data after their death.

Where the data was not obtained from the data subject, the information must be provided 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 is first disclosed (*Article 14, GDPR*).

It is recommended that this information be provided in writing.

13. What other specific rights are granted to data subjects?

Rights granted to data subjects by the DPA include the rights to:

- Object on legitimate grounds to the processing of any data relating to them, except where the processing satisfies a legal obligation or where an explicit provision of the decision that authorises the processing excludes the right to object (*Article 38, DPA*).
- Object, at no cost to them, to the use of data relating to them for canvassing purposes, in particular for commercial ends, by the controller of a current or further data processing (*Article 38, DPA*).
- Request the following information from the data controller:
    - confirmation as to whether the personal data is to be used;
    - the purpose of the processing, the categories of personal data processed and the recipients or categories of recipients to whom the data are communicated;
    - whether the data will be transferred outside the European Economic Area (EEA);
    - the communication, in an accessible form, of processed personal data and of any available information as to their origin; and

- information on, and how to object to, the logic involved in the processing.

(*Article 39, DPA*.)

- Obtain a copy of the processed data (*Article 39, DPA*).
- Request the data controller to rectify, complete, update, block or delete personal data relating to them that are inaccurate, incomplete, equivocal, expired, or whose collection, usage, disclosure or retention is prohibited (*Article 40, DPA*).
- Request the data controller to erase as soon as possible personal data collected in the context of the offer of information society services, where the data subject was a minor at the time of collection, except when the processing is necessary (for example, to comply with a legal obligation or to exercise the right to freedom of expression) (*Article 40, DPA*).
- Define general or specific guidelines on the retention, erasure and disclosure of their personal data after their death (*Article 40-1, DPA*) (*see Question 14*).
- Bring a class action before the competent civil or administrative court, where several natural persons in a similar situation suffer damage as a result of a similar breach by a data controller or processor. The applicant must inform the CNIL of any such action (*Article 43 ter, DPA*).

The Digital Republic Law supplemented Article 1 of the DPA by creating a fundamental right for data subjects to decide on and control the use made of their personal data. Any provider of electronic communication services to the public must offer a free service allowing consumers to recover their data.

Articles 92 to 100 of the DPA Decree set out certain conditions in relation to the exercise of their rights by data subjects (for example, the types of information that can be required by a data controller to verify the identity of the requesting individual).

14. Do data subjects have a right to request the deletion of their data?

See *Question 13*.

Any natural person providing proof of his/her identity can request a data controller to rectify, complete, update, block or delete personal data concerning them which are inaccurate, incomplete, ambiguous, out of date or whose collection, use, communication or storage is prohibited (*Article 40, DPA*).

Minors have a right to be forgotten and to request deletion of any personal data that was collected when they were still a minor (*Article 40, DPA*).

Data subjects can create instructions during their lifetime to keep, delete and communicate their data after their death (*Article 40-1, DPA*). All providers of online electronic communications services to the public must inform users about what will happen to their data when they die and allow them to choose whether or not their data will be transferred to a designated third party.

Security requirements

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

Data controllers must take all useful precautions to preserve the security of personal data, having regard to the nature of the data and the risks of the processing (*Article 34, DPA*).

Data controllers must protect personal data against accidental or unlawful destruction, loss, alteration and disclosure, particularly when processing involves the transmission of data over networks.

Data processors must provide sufficient guarantees to ensure the implementation of security and confidentiality measures. This requirement does not discharge the data controller of its obligation to ensure compliance with these measures (*Article 35, DPA*).

The DPA introduced a requirement to conduct a data privacy impact assessment (DPIA) in certain circumstances. Where data processing is likely to result in a high risk to the rights and freedoms of natural persons (for example, because it involves the processing of special categories of data listed in Article 8 of the DPA), the controller must, prior to the processing, carry out an impact assessment of the envisaged processing operations on the protection of personal data (*Article 70-4, DPA*).

Data controllers and data processors must also keep a register of data processing activities. The register must contain the following information:

- A general description of the measures aimed at ensuring a level of security appropriate to the risk, in particular with regard to the processing of special categories of personal data.
- An indication of the legal basis of the processing, including any intended transfers of personal data and the use of profiling (if any).

(*Article 70-14, DPA*.)

In 2010, the CNIL issued guidelines on the security measures to be implemented by a data controller to guarantee the security of personal data processing. In 2012, it published a second set of guidelines on the protection of privacy for high-risk or complex data processing, to help data controllers have a clear vision of the risks associated with the processing and identify the security measures to be implemented. These guidelines were revised in 2015 and 2018 with the entry into force of the GDPR, to inform data controllers of the requirements relating to DPIAs and maintenance of a register of data processing activities.

Failure to implement appropriate security measures can lead to five years' imprisonment and/or a fine of up to EUR300,000 (up to EUR1.5 million for legal persons) (*Article 226-17, Criminal Code*).

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

Several provisions provide for the notification of personal data security breaches, which differ in their scope and conditions.

Under Articles 33 and 34 of the GDPR, all data controllers must notify a personal data breach concerning either personal data they process themselves or data processed by their data processor, on notification by the processor. Notification to the national regulator must be made without undue delay and, to the extent possible, within 72 hours, whenever the data breach is likely to result in a risk to the rights and freedoms of natural persons. Notification to data subjects is only required if the breach is likely to result in a high risk to their rights and freedoms. Controllers are exempted from notifying data subjects when any of the following applies:

- They have implemented the appropriate technical and organisational protection measures to render the data unintelligible to third parties.
- They have taken measures to ensure that the risks identified are no longer likely to materialise.
- Individual notifications would require a disproportionate effort for the controller (in which case a public communication can be preferred).

The above provisions of the GDPR are fully effective in France, and co-exist with the following two specific domestic law obligations:

- Under Article 34 *bis* of the DPA, providers of public electronic communications services must notify the CNIL without undue delay (within 24 hours according to the CNIL's recommendations) in the event of a security breach affecting personal data, regardless of the impact on the rights and freedoms of natural persons. The content of such notification is equivalent to that of notifications under the GDPR. A notification form is available on the CNIL's website. Data controllers must also notify data subjects when the security breach may affect their personal data or any natural person's right to privacy, unless the data controller can prove it has successfully implemented measures to prevent such risks (for example, by rendering the personal data unintelligible to third parties). Failure by an electronic communications service provider to duly notify a security breach can trigger criminal sanctions of up to five years' imprisonment and/or a fine of up to EUR300,000 (for natural persons) or EUR1.5 million (for legal persons) (*Article 226-17-1, Criminal Code*).
- Under Article 70-16 of the DPA, a data controller established in France must notify both the CNIL and a data controller established in another EU member state without undue delay where a data security breach:
    - relates to personal data processed by a public authority or another entity on delegation by a public authority, exclusively for the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties; and
    - concerns a data controller located in France and which either has received the data from a controller located in another EU member state or intends to send the data to such a controller.

When this specific regime applies, notification to data subjects is required in the same circumstances as under Article 34 of the GDPR (that is, when the breach is likely to result in a high risk to their rights and freedoms). However, the DPA provides that notification can be delayed, limited or forgone altogether when such restriction constitutes a necessary and proportionate measure in a democratic society, taking into account the fundamental rights and legitimate interests of data subjects, to:

- safeguard public security and national security;
- protect the rights and freedoms of citizens;
- further the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties; and
- further investigations and judiciary or administrative proceedings.

Under the above notification regimes, data controllers must document security breaches and maintain a record of past events, to be handed to the CNIL in the event of control. In addition, the CNIL can order data controllers to notify breaches to data subjects when they have not done so in due time, subject to daily penalty payments.

Processing by third parties

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

A data controller must impose a number of requirements on a data processor to ensure that information is collected and processed in accordance with the data controller's instructions and the DPA (*Article 35 I, DPA*).

When the processing activity is within the scope of either the GDPR or Directive (EU) 2016/680, Article 35 I of the DPA does not apply and the contract between the data processor and the data controller must comply with the requirements of EU law (that is, Article 28 of the GDPR and Articles 22 and 23 of the Directive).

When the processing activity is outside the scope of these instruments, the contract between the data processor and the data controller must detail the security and confidentiality measures to be implemented by the data processor and provide that the processor can only act on instructions from the controller, for example, with regard to:

- Data access protection (with a clear access and password policy).
- Electronic data storage.
- Data transfer (for example, through encryption).
- Data disposal (for example, the data processor can commit to take all necessary steps to ensure that all business-critical information is removed from any decommissioned computers or external drives).

- End user awareness (for example, through training programmes).

Electronic communications

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

A data controller can install cookies or equivalent devices if prior consent is given by the user. This applies to website publishers, advertising networks, social networks and editors of audience development solutions.

The data controller must use a banner notice giving brief information and allowing users to take steps to disable the website's cookies if they wish to do so before continuing to use the site. In addition, the data controller must inform users on how to disable cookies and how disabling them may affect their experience on the website.

The CNIL considers that consent is only valid for 13 months at a time.

Certain types of cookies are not subject to the obligations above (for example, where their purpose is to allow or facilitate online communication).

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

Sending unsolicited messages is prohibited without prior consent from the recipient (*Article L.34-5, Postal and Electronic Communications Code; Article L.121-20-5, Consumer Code*). Consent from data subjects is not considered as given when they agree to general sale terms or when there are pre-checked boxes on a website.

As an exception, unsolicited electronic commercial communications can be sent to a customer without their prior consent if the following requirements are met:

- The consumer's contact details were collected in compliance with the DPA and as a result of customer purchases.
- The commercial communications concern similar products and services purchased by the customer.
- The consumer can opt out when data is collected and at each commercial communication.

There is no prior consent requirement in a business-to-business relationship, provided that the recipient has been informed that his/her email address will be used for electronic commercial communications and is given the possibility to object to it when the email address is collected. The commercial communication must be relevant to the profession of the recipient.

Marketing by post or by telephone does not require prior consent, but cannot be done if the recipient has objected to it.

International transfer of data

Transfer of data outside the jurisdiction

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

A data controller cannot transfer personal data to a state that is not an EU member state if that state does not provide a sufficient level of protection of individuals' privacy (*Article 68, DPA*). The European Commission has established a list of states that provide an adequate level of protection.

A data controller can transfer personal data to a state that does not satisfy the above conditions if the data subject has expressly consented to the transfer or if the transfer is necessary for any of the following:

- Protection of the data subject's life.
- Protection of the public interest.
- To meet obligations ensuring the establishment, exercise or defence of legal claims.
- Consultation of a public register that is intended for public information and is open for public consultation or by any person demonstrating a legitimate interest.
- Performance of a contract between the data controller and the data subject, or of pre-contractual measures taken in response to the data subject's request.
- 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.

(*Article 69, DPA*.)

There are other options to ensure an adequate level of compliance. These include using:

- Standard contractual clauses (model clauses designed by the European Commission to facilitate transfers of personal data from the EU to all third countries, while providing sufficient safeguards for the protection of individuals' privacy).

- Binding corporate rules validated by the CNIL.
- The US Privacy Shield.

A data controller must inform a data subject of the:

- State where the recipient of the data is established.
- Nature of the data transferred.
- Purpose of the transfer.
- Categories of recipients.
- Level of protection of the state concerned. If the state does not provide an adequate level of protection, the data controller must mention under which exception the transfer is allowed.

(*Article 91, DPA Decree.*)

21. Is there a requirement to store any type of personal data inside the jurisdiction?

Certain health-related data (collected in the course of prevention activities, for diagnostic purposes, medical treatment, or social or socio-medical aftercare) must be hosted by pre-approved hosting providers that must hold an appropriate certification (*Article L.1111-8, Public Health Code*).

Data transfer agreements

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

The European Commission has adopted standard contractual clauses to facilitate transfers of personal data from the EU to third countries that do not provide an adequate level of protection. Although the law does not require the use of the model clauses, the CNIL considers them to be a valid safeguard. If these standard contractual clauses are not adapted to a specific situation, data controllers can submit to the CNIL *ad hoc* contractual clauses for approval (*Article 101, DPA Decree*).

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

A data transfer agreement using standard contractual clauses or binding corporate rules is sufficient to legitimise a data transfer (*see Question 20*).

24. Does the relevant national regulator need to approve the data transfer agreement?

Data transfers based on the standard contractual clauses need not be approved by the CNIL. However, notification to the CNIL is mandatory if the data transfer agreement has modified the standard contractual clauses adopted by the European Commission.

Enforcement and sanctions

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

The CNIL has strong enforcement powers. The CNIL can:

- Conduct on-site inspections. The members of the CNIL can have access, from 6.00 am to 9.00 pm to places, premises, or equipment used for processing personal data for professional purposes, with the exception of private homes. The public prosecutor must be informed beforehand and the person in charge of the private professional premises must be informed of their right to object to the visit. If they object, the visit can only take place after authorisation from the liberty and custody judge. However, if justified by urgency or the seriousness of the facts or by a risk of destruction or concealment of documentary evidence, the visit can take place without informing the person in charge of the premises and after authorisation from the judge. In this case, the person in charge cannot object to the visit. The visit must be carried out under the authority and control of the liberties and custody judge who authorised it, in the presence of the occupant of the premises

or his/her representative who may be assisted by a counsel of his/her choice, or in the presence of two witnesses who are not placed under the authority of the persons responsible for carrying out the inspection.

- Carry out other control operations. In particular, the CNIL can consult data on an online communication service to the public which are freely accessible or made accessible, including through negligence, imprudence or the actions of a third party, if necessary by accessing and maintaining an automated data processing system for the time necessary for the operation. The CNIL can record data in any appropriate manner in documents directly available for the purposes of the control. Agents of the CNIL can use a false identity to carry out any online operations necessary for the exercise of their mission. Secrecy cannot be raised against CNIL agents, except for information protected by attorney-client privilege, the protection of journalistic sources, or medical confidentiality (*Article 44, DPA; Article 65-1, DPA Decree*).
- Submit written requests for communication of documents or files.
- Conduct hearing inspections.

Since the adoption of the Consumer Protection Act 2014, the CNIL can conduct online inspections (reviewing any publicly available information such as online privacy policies, online consent mechanisms, and compliance with cookie requirements).

Impeding the action of the CNIL (by resisting the exercise of the duties of the CNIL, refusing to communicate the information and documents requested, or supplying inappropriate information) can result in one year's imprisonment and a EUR15,000 fine (*Article 51, DPA*).

Since the introduction of the Digital Republic Law, the CNIL's chairperson can start summary proceedings for necessary measures in cases of serious and immediate violations of the rights and freedoms of data subjects (*Article 52, DPA*).

26. What are the sanctions and remedies for non-compliance with data protection laws?

The restricted committee of the CNIL can impose the following penalties on a data processor or data controller that has breached their obligations under the applicable legislation:

- A warning (optional).
- A temporary or definitive limitation on a processing operation, a ban on processing, or withdrawal of a granted authorisation.
- An injunction to bring processing operations into compliance with the DPA or to answer a data subject's request to exercise his or her rights, accompanied by a penalty that cannot exceed EUR100,000 for each day the processing operations continue beyond the deadline for compliance.
- Withdrawal of a certification or an order to the relevant certification body to withdraw an issued certification.
- An order to suspend data flows to a recipient in a third country or to an international organisation.

- Partial or full suspension of a decision approving binding corporate rules.
- An administrative fine of up to, depending on the violation:
  - EUR10 million or 2% of an undertaking's total worldwide annual turnover of the preceding financial year, whichever is higher; or
  - EUR20 million or 4% of an undertaking's total worldwide annual turnover of the preceding financial year, whichever is higher.

In the context of recently introduced obligations, the CNIL has indicated that its controls will first be aimed at guiding entities on compliance with the law. However, the CNIL will continue to rigorously investigate suspected non-compliance with the main data protection principles (for example, fairness of the processing, relevance of the data processed, retention period, and data security).

Status of national GDPR implementation law

France's national GDPR implementation law was enacted on 20 June 2018 and amended the Act No. 78-17 of 1978. Key variations between French law and the GDPR include:

- The application of domestic rules adopted under the opening provisions of the GDPR to data subjects who live in France, regardless of the location of the data controller (except for processing operations related to freedom of expression and information).
- The authorisation to process personal data relating to criminal convictions and offences under certain circumstances (for example, by entities collaborating with the justice public service, victims, and users of public information available in judicial decisions).
- The reduction of the age of consent for minors to 15 years and the requirement for double consent (that of the minor and that of the holder of parental rights) when the minor is below 15 years.
- The power of the data protection authority to impose additional sanctions.
- The possibility to bring class actions in connection with personal data breaches and to claim compensation for material and moral damages caused by violations of personal data rights.

Regulator details

French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*) (CNIL)
W *www.cnil.fr/en/home*

Main areas of responsibility. The CNIL is an independent administrative authority responsible for ensuring that information technology remains at the service of citizens, and does not jeopardise human

identity or breach human rights, privacy, or individual or public liberties. It supervises enforcement of the DPA and frequently issues decisions and guidelines on it. The 2018 amendments to the DPA have increased the regulatory and coercive powers of the CNIL, which otherwise uses soft law prerogatives. The CNIL assists data subjects and uses its extended powers of control to impose penalties in compliance with personal data protection law.

Online resources

Legifrance
W *www.legifrance.gouv.fr*

Description. Legifrance is the French Government entity responsible for publishing legal texts online. This website provides access to an English translation of the French DPA (*www.legifrance.gouv.fr/Traductions/Catalogue-des-traductions*).

Contributor profiles

Myria Saarinen, Partner

Latham & Watkins

T +33 1 4062 2000
F +33 1 4062 2062
E *myria.saarinen@lw.com*
W *www.lw.com*

Professional qualifications. France, Avocat à la Cour

Areas of practice. Data privacy, security and cybercrime; complex commercial litigation; litigation; white collar defence and investigations; securities litigation and professional liability; product liability; mass torts and consumer class actions; energy regulatory and markets; intellectual property litigation; technology transactions.

Languages. French, English

Publications

- *France Enacts Sweeping New Data Protection Law, Client Alert, 2018.*
- *France Chapter, The Technology, Media & Telecommunications Review, 2017.*
- *French Digital Republic Law Expands Rights of Users and Regulators (Law No 2016-321 of 7 October 2016), Client Alert, 2016.*
- *5 Questions About France's New Health-related Class Action Law, Client Alert, 2016.*
- *France Chapter, International Fraud & Asset Tracing - 3rd Edition, 2015.*
- *Class Actions Enter into Force in France as of 1st October 2014, Client Alert, 2014.*
- *Introduction of Class Actions in France: A Growing Threat to Professionals?, Client Alert, 2014.*

Elise Auvray, Associate

Latham & Watkins

T +33 1 4062 2000
F +33 1 4062 2062
E *elise.auvray@lw.com*
W *www.lw.com*

Professional qualifications. France, Avocat à la Cour

Areas of practice. Data privacy, security and cybercrime; complex commercial litigation; litigation and trial practice.

Languages. French, English

Publications

- *France Enacts Sweeping New Data Protection Law, Client Alert, 2018.*
- *France's Major Anti-Corruption Reform: What's Next for Companies and Their Top Management?, Client Alert, 2016.*
- *French Anti-Corruption Reform Expected In 2016, Client Alert, 2016.*

Floriane Cruchet, Associate

Latham & Watkins

T +33 1 4062 2000
F +33 1 4062 2062
E *floriane.cruchet@lw.com*
W *www.lw.com*

Professional qualifications. France, Avocat à la Cour

Areas of practice. Data privacy, security and cybercrime; complex commercial litigation; litigation and trial practice.

Languages. French, English

Publications. *France Enacts Sweeping New Data Protection Law, Client Alert, 2018.*

END OF DOCUMENT