DATA PROTECTION LAWS OF THE WORLD

France

FRANCE

Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (“GDPR” or ”**Regulation**”) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. This is the “*establishment criterion*”. An 'establishment' may take a wide variety of forms and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behavior*" (Article 3(2)(b)) as far as their behavior takes place within the EU. This is the “targeting criterion”.

France updated Law No. 78-17 of January 6, 1978 on information technology, data files and civil liberties (the “**Law** ”) to GDPR with the enactment of (i) Law No. 2018-493 of June 20, 2018 on the protection of personal data, and (ii) Order No. 2018-1125 of December 12, 2018, adopted pursuant to Article 32 of Law No. 2018-493, updates the Law and other French laws relating to personal data protection in order to “simplify the implementation and make the necessary formal corrections to ensure consistency with EU data protection law”. France domestic data protection legislation was further completed with the adoption of Decree No. 2019-536 of May 29, 2019, adopted for the application of the Law (the “**Decree**”). The Decree clarifies procedural rules of the French data protection authority, including its control and sanctions, and further specifies data subject rights.

The Law and the Decree have been updated:

- in 2021, (i) Law No. 2021-988 of July 30, 2021, on the prevention of acts of terrorism and intelligence amended articles 48 and 49 of the Law to create exceptions to the rights of individuals when processing is justified by national security and (ii) Law No. 2021-1017 of August 2, 2021, relating to bioethics which modified article 75 of the Law relating to processing in the health field; and

- in 2022, (i) Law No. 2022-52 of January 24, 2022, on criminal liability and homeland security amends articles 10, 20, 125 of the Law and created article 22-1 to introduce the simplified sanction procedure of the French data protection authority and (ii) Decree No. 2022-517 of April 8, 2022, amends the Decree to define the modalities of this simplified sanction procedure as introduced by Law No. 2022-52 of January 24, 2022. The objective of these new texts is to introduce more flexibility in the use of formal notices or sanctions.

Territorial Scope

As of today, Article 3 of the Law provides that it applies when (i) the data controller or data processor is established in France (whether the processing takes place in France or not) or (ii) the data subjects reside in France (for the possible legal variations as permitted from time to time of the GDPR. Contrary to the GDPR, the Law has not included the “targeting criterion”.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions under the Law are the same as under the GDPR. Article 2 of the Law makes an express reference to GDPR definitions, thus harmonizing the definitions and concepts of French law with the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the CNIL in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single

establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The « *Commission Nationale de l’Informatique et des Libertés* » or « CNIL » is the French supervisory authority

Address

3 place de Fontenoy
TSA 80175
75334 Paris Cedex 07

Telephone

01 53 73 22 22

Website

cnil.fr

The CNIL has different missions and powers, which mainly include:

i. informing data subjects and data controllers / processors (whether public or private) about their rights and obligations;
ii. ensuring compliance of all personal data processing with French and EU data protection rules as well as data protection rules resulting from international commitments of France;
iii. anticipating new challenges and issues arising from innovation and the use of new technologies, including privacy in general and ethics;
iv. controlling and sanctioning.

In addition, the Law provides for mutual assistance and joint operations with other EU Supervisory Authorities, as well as cooperation with non-EU supervisory authorities.

The CNIL has a range of tools to complete its missions including e.g., publication of reference frameworks created after consultations with the stakeholders or sectors at hand, among which standard regulations (which are mandatory in respect of processing of biometric, genetic, health or criminal convictions and offences data), reference methodologies in the sector of health, guidelines, recommendations and standards, approval of codes of conduct and certifications, broad range of on-site and off-site investigation powers and sanctions. The Law provides further precisions on the functioning of the CNIL and its specific tasks and powers, notably the extent of on-site investigations and procedural requirements, in connection with the missions described above.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or

processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Prior formalities with the CNIL are no longer required and are replaced by the obligation to hold a record of processing which include the same categories of information as those initially requested in the filing forms.

However, formalities are maintained for the processing of data in the health sector which is subject either to a declaration of conformity to specific requirements defined by the CNIL or an authorization by the CNIL. In this respect, the CNIL has issued eight (8) methodologies of reference ("*Methodologies de Reference*" or "MR") for various types of research in the health sector. A formal commitment to comply with these methodologies exempts the data controller – generally the sponsor of the research – from having to apply for a formal authorization with the CNIL.

Certain specific processing of personal data must be authorized by decree of the State Council (*Conseil d’Etat*) or ministerial order, taken after a motivated and public opinion of the CNIL. These processing are as follows:

- Processing of the social security number (with a few exceptions);
- Processing carried out by or on behalf of the State, acting in the exercise of its public authority prerogatives, of genetic or biometric data necessary to the authentication or identity control of individuals;
- Processing carried out on behalf of the State (i) which concern State security, defense, national security, or (ii) which purpose is the prevention, investigation, detection or prosecution of criminal offences, or enforcement of criminal convictions or security measures.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope, or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;

- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Law provides that controllers processing personal data under the scope of the EU Data Protection Directive on Police and Criminal Justice Cooperation must appoint a DPO, with the exception of jurisdictions acting within the scope of their judicial activity.

The Decree specifies the mandatory information to be communicated to the CNIL by data controller(s) or processor(s) in the DPO notification form.

On 20 September 2018, the CNIL issued two standards regarding the certification of DPO skills: one regarding the skills and know-how expected to be certified as DPO (CNIL Deliberation No. 2018-318), and the other one regarding the criteria applicable to certifying DPO organizations (CNIL Deliberation No. 2018-317). These Deliberations were recently updated notably to adapt the procedure of accreditation of the organizations authorized to certify the DPOs’ skills and to enable candidates to take the certification test remotely (CNIL Deliberation No. 2022-128 and CNIL Deliberation No. 2023-062).

On March 2022, the CNIL also published a Guide for DPOs that combines useful knowledge and best practices to help organizations in appointing and supporting DPOs.

COLLECTION & PROCESSING

Data protection principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal basis under article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special category data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 legal basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal convictions and offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a secondary purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (privacy notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the data subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Special category data

The Law contains specific provisions regarding the processing of health data (e.g. see above regarding authorization requirements), as well as additional provisions regarding processing of special categories of personal data.

Criminal convictions and offences data

The following categories of persons can process such personal data:

- Courts, public authorities and legal persons entrusted with a public service, acting within the scope of their legal functions, as well as entities collaborating with judicial entities as listed in the Decree;
- Auxiliaries of justice, for the strict exercise of their functions;
- Individuals and private entities to prepare, bring or defend a claim in court as a victim or defendant, and to execute the court decision, for the duration strictly necessary for these purposes. It is possible to share such information with third parties under the same conditions and for the same purposes;
- Collective IP rights management organizations for the purpose of defending those rights; and
- Persons reusing public information appearing in published rulings, provided that the processing has neither the purpose or effect of allowing the re-identification of the concerned persons.

In addition, the following categories of persons are authorized by the Decree to process personal data relating to criminal convictions, offenses or related security measures:

- Victims support associations contracted by the Ministry of Justice;
- Associations of assistance to the reintegration of persons placed under the authority of justice, in the respect of their social object;
- The establishments mentioned in 2 ° of I of Article L. 312-1 of the Code of Social Action and Families as part of their mission of medico-social support;
- The establishments and services mentioned in 4 ° and 14 ° of I of Article L. 312-1 of the Code of Social Action and Families;
- The drop-in and reception centers mentioned in III of Article L. 312-1 of the Code of Social Action and Families; The medical or medico-educational establishments authorized mentioned in articles 15 and 16 of the order No. 45-174 of 2 February 1945 relating to delinquent childhood;
- The public or private educational or vocational training institutions, authorized and appropriate boarding schools for juvenile school-aged offenders mentioned in Articles 15 and 16 of the aforementioned order of 2 February 1945;
- Private legal entities exercising a public service mission or the authorized associations mentioned in Article 16 of the aforementioned order of 2 February 1945;
- The legal representatives for the protection of the adults mentioned in Article L. 471-1 of the Code of Social Action and Families.

The CNIL may issue standard regulations, prescribe additional measures to be implemented, including of a technical and organizational nature, and / or complementary warranties for processing of special categories of data, including notably criminal convictions and offences data, by public and private entities (except for processing carried out in connection with the exercise of public authority by or on behalf of the State).

In addition, processing of criminal convictions and offences data which purpose is the prevention, investigation, detection or prosecution of criminal offences, or enforcement of criminal convictions or security measures by or on behalf of the State is subject to an order of the competent Ministry.

Transparency (privacy notices)

The Law mandates data controllers to provide data subjects with information relating to their right to define directives relating to the processing of their personal data after their death (digital legacy).

In addition, where the data is collected from a data subject under 15, the data controller must provide the mandatory information provided for by Art. 13 GDPR in a clear and easily accessible language.

The French data subjects should be also provided with the information relating to the processing of their personal data in French (notably in accordance with Act no. 94-665 dated 4 August 1994 related to the use of the French language).

Rights of the data subjects

The Decree describes the conditions in which the data subjects can exercise their rights (and more precisely, the conditions to check the identity of the data subject making the right request).

Data subjects’ rights can be restricted notably to avoid obstructing administrative investigations, inquiries or procedures, to safeguard the prevention, investigation, detection and prosecution of criminal offences, as well as of administrative enquiries, or to protect the rights and freedoms of others.

Digital legacy

Data subjects have the right to give instructions regarding the storage, deletion and communication of their personal data after their death (Articles 48 and 85 of the Law). Such instructions can be either:

- General, in which case they apply to all their personal data, irrespective of who the controller is. Such instructions can be given to a trusted third party certified by the CNIL; however, the implementing decree in this respect has never been adopted since the adoption of this provision in 2016; or
- Specific to one or several services, in which case the data subject can also give his / her instructions to the relevant data controller. It is required to obtain the specific consent of the data subject, and such consent cannot derive from his/her consent to general terms and conditions.

If the data subject has not given any instructions in his / her lifetime, then his / her heirs can exercise certain rights, in particular:

- The right of access, if it is necessary for the settlement of the succession; and
- The right to close the deceased’s accounts and to cease the processing of his / her personal data or, request the update of the personal data of the deceased.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay, New Zealand, Japan, the United Kingdom, the Republic of Korea and the United States (for companies certified under the EU-US Data Privacy Framework).

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules and standard contractual clauses. Controllers should also take additional requirements provided by the EDPB Recommendations 01/2020, following-up to the CJUE Schrems II Decision, i.

e., Transfer Impact Assessment and where necessary, supplementary measures. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

In the event processing of personal data involves a transfer of data outside the European Union territory, data subjects must be provided with mandatory information on, inter alia, the data transferred, the purpose of the transfer, the recipients of the data and the transfer mechanism used in accordance with the GDPR.

With respect to transfers made on the basis of Article 49(1)§2 of GDPR ("compelling legitimate interest"), the Decree provides that the CNIL will define templates (including annexes) to be used by data controllers to inform the CNIL about such transfers.

With respect to transfers made on the basis of code of conduct or other certification mechanism approved by the CNIL in accordance with the Law and the Decree, the Decree provides that data controller / data processor that rely on such transfer mechanisms shall provide the CNIL with a binding and enforceable commitment to apply appropriate safeguards to data subjects’ rights and freedoms in the concerned third-country.

For more information, please visit our Transfer – global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Although there is no specific requirements other than those set forth in the GDPR, the CNIL and the French Cyber Security Agency (“ANSSI”) have issued security guidance and recommendations containing state-of-the-art security practices, in particular: the 2023 version of the Personal Data Security Guide and the 2022 version of the recommendations on password and other shared secrets.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Article 85 of Decree restricts the obligation of notification under Article 34 of the GDPR for the following processing:

- Processing including personal data allowing to identify, directly or indirectly, individuals whose identity is protected under Article 39 sexies of the French law on the freedom of the press; and
- Administrative, financial and operational data, as well as health data processing for which the notification of an unauthorized disclosure or access is likely to result in a risk for the national security, defense or public, due to the volume of data affected by the breach and the private information it contains (such as the family address or composition).

The Law provides that a Decree by the State Council, adopted after seeking the CNIL’s opinion (yet to be adopted) will specify a list of categories of processing and processing operations that derogate to the data breach notification requirement. Such derogation will only apply to processing that are necessary pursuant to a legal obligation bearing on the data controller or a public interest mission vested in the data controller, where such data breach notification would likely result in a risk to homeland security, defense or public safety.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

> For instance, in France, criminal penalties which can go up to 5 years of prison and EUR 300,000 fine for natural persons and EUR 1,500,000 for legal persons.

In May 2023, the EDPB issued Guidelines 04/2022 on the calculation of administrative fines under the GDPR.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Since 24 January 2022, the CNIL can investigate and use corrective powers following the simplified sanction procedure (Article 22-1 of the Law). This accelerated procedure can be used when a case does not present a specific issue (e.g. there is an established case law on the issue, the factual and legal issues are considered as simple). In such case, the CNIL can pronounce one or more of the following measures: warning, injunction to bring the processing into compliance including a penalty payment of up to €100 per day of delay, and / or an administrative fine of up to €20,000. Sanction decisions issued pursuant to the simplified sanction procedure are not published.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Law does not contain explicit provisions with respect to electronic marketing. However, Article L. 34-5 of the French Postal and Electronic Communications Code regulates electronic marketing in France. The CNIL has issued guidelines on the basis of this provision.

The CNIL distinguishes between B2B and B2C relationships. In any event, all electronic marketing messages must specify the name of the advertiser and allow the recipient to object to the receipt of similar messages in the future.

Electronic marketing to consumers (B2C)

Electronic marketing activities are authorised provided that the recipient has given consent at the time of collection of his / her email address.

This principle does not apply when:

- the concerned individual is already a customer of the company and if the marketing messages sent pertain to products or services similar to those already provided by the company; or

> Note that the CNIL considers that the creation of an account does not prejudge the eventual ordering of products or services from the company. The CNIL considers that in the absence of a purchase, the company cannot purposefully invoke the benefit of the soft opt-in exception created by article L. 34-5 of the French Postal and Electronic Communications Code.

- the marketing messages are not commercial in nature.

In any event the concerned individual, at the time of collection of his / her email address, must be informed that it will be used for electronic marketing activities, and be able to easily and freely object to such use.

Electronic marketing to professionals (B2B)

Electronic marketing activities are authorized provided that the recipient has been, at the time of collection of his / her email address:

- informed that it will be used for electronic marketing activities, and
- able to easily and freely object to such use.

The message sent must relate to the concerned individual’s professional activity. Please note that email addresses such as contact@companyname.fr are not subject to the requirements of prior consent and the right to object.

ONLINE PRIVACY

Cookies

The EU Cookie Directive has been implemented in the Law. It states that any subscriber or user of electronic communications services must be fully and clearly informed by the data controller or its representative of:

- the purpose of any cookie (i.e. any means of accessing or storing information on the subscriber’s / user’s device, e.g. when visiting a website, reading an email, installing or using software or an app); and
- the means of refusing cookies,

unless the subscriber / user has already been so informed.

Cookies are lawfully deployed if the subscriber / user has expressly consented after having received information. Valid consent can be expressed via browser settings if the user can choose the cookies he / she accepts and for which purpose.

However, the foregoing provisions do not apply:

- to cookies the sole purpose of which is to allow or facilitate electronic communication by a user; or
- if the cookie is strictly necessary to provide online communication services specifically requested by the user.

Location and traffic data

The Postal and Electronic Communications Code deals with the collection and processing of location and traffic data by electronic communication service providers (CSPs).

All traffic data held by a CSP must be erased or anonymised. However, traffic data may be retained, for example:

- for the purpose of finding, observing and prosecuting criminal offences;
- for the purpose of billing and payment of electronic communications services; or
- for the CSP’s marketing of its own communication services, provided the user has given consent thereto.

Subject to exceptions (observing and prosecuting criminal offences; billing and payment of electronic communications services), location data may be used in very limited circumstances, for example:

- during the communication, for the proper routing of such communication; and
- where the subscriber has given informed consent, in which case the location data may be processed and stored after the communication has ended. Consent can be revoked free of charge at any time.

Cookies

The French Data Protection Supervisory Authority (CNIL) replaced its 2013 guidelines regarding cookies and trackers, which were no more compliant with the GDPR, by revised guidelines. Following the adoption of a version of its guidelines on cookies and other trackers on July 4, 2019, which have been partially annulled by a decision from the French highest administrative Court, the *Conseil d’Etat*, on 19 June 2020, the CNIL has adopted revised guidelines and the final version of its recommendations on the practical procedures for collecting consent concerning cookies and other trackers. The CNIL’s revised guidelines, adopted by way of deliberation No. 2020-091 of September 17th, 2020, are based on Article 82 of the Law, implementing Article 5 (3) of EU directive “ePrivacy”, into French law.

While the Revised Guidelines provide the CNIL’s guidance on how to read the relevant provisions of the French Data Protection Act, which governs the use of cookies and other trackers in France, the Recommendations adopted by a deliberation No. 2020-92 of September 17th 2020 provide practical guidance and examples to help professionals navigate the rules applicable to cookies and other trackers and comply with the requirements of Article 82 of the French Data Protection Act. These two documents constitute “soft law” and are not binding, but provide strong references for organizations to anticipate how the CNIL may conduct its compliance investigations.

Regarding consent, the CNIL has now specified that consent must be:

- **unambigous**: to align with the guidelines on consent issued by the Article 29 Working Party, the CNIL repeals its previous position according to which scrolling down, browsing or swiping through a website or app was considered as an acceptable expression of consent to cookies and allowed for cookies to be placed. Therefore, for the CNIL, continuing to navigate on a website or using an application is no more acceptable to evidence a consent to cookies. The absence of action from the user (i.e., no choice from the user) can no longer be construed as a valid consent but should rather be construed as refusal. This operates a shift from “soft opt-in” to active consent. The revised guidelines also outlines that pre-ticked boxes do not meet the GDPR standard of consent;
- **freely given**: the data subject must be able to exercise freely his / her choice. The CNIL has revised (albeit subtlety) its previous positioning regarding “cookie walls” (the practice of subjecting prior access to a website or application to the acceptance of cookies) – where the CNIL considered that consent could never be freely given when collected using cookie walls, the revised guidelines now specify that cookie walls are likely to hinder freely given consent. In addition, the CNIL has specified in its case law, that failure to provide a mean to refuse cookies “as easily” as it is to accept them (e.g., by way of dedicated buttons on a cookie banner) results in consent being not freely given, since users will lean toward accepting cookies rather than performing multiple clicks to refuse;

- **specific**: consent must be tailored to each purpose. Therefore acceptance of the general terms and conditions as a whole (“bundled” consent) does not constitute valid consent;
  informed: information to data subjects must be easily understandable by any of them. Information must be given in plain language. The use of complex technical or legal terms does not meet the requirement of prior information. Such information must at least include (i) the identity of the data controller(s) implementing the trackers (ii) a thorough list of the purpose(s) of the reading or writing operations (iii) the means available to consent or object to the use of cookies (iv) the consequences of accepting or refusing the use of cookies and (v) the right to withdraw consent;
- **evidenced**: all organizations that use cookies must implement appropriate mechanisms that allow them to demonstrate, at all times, that they have validly obtained consent from users. the revised guidelines specifically provide that users choices, be it consent or refusal, must be (i) clearly presented to users, notably as regards the available means to exercise such choice, (ii) collected and clearly evidenced (the recommendations give examples of how to ensure such evidence through the use of a consent management platform, screen capture, etc.) and (iii) recorded by data controllers, for an appropriate duration during which they would not ask the users again for their consent. Such duration may vary depending on the nature of the site or application concerned. According to the Recommendations, a good practice in that respect is 6 months Ó at the expiry of that term, controllers could ask users again to consent (or refuse) to the use of cookies and trackers; and
- **revocable**: organizations are encouraged to put in place user-friendly solutions to allow users to withdraw their consent as easily as they gave it. The CNIL highlights the fact that means to refuse cookies and trackers must be “as easy” as means available to accept use thereof. As a result, users must not be subjected to complex procedures for refusing cookies and trackers and withdraw their consent, which they must be able to do at any time. To that end, the CNIL provides practical examples and good practices in the Recommendations, from the use of a “reject all” button to the availability of a visible “cookies” icon enabling users to parameter their choices and withdraw their consent.

The updated guidelines do not provide a general rule regarding the data retention of cookies and the information collected via such cookies. The CNIL simply recommends that the user’s consent (or refusal) is renewed every 6 months. However, the CNIL has maintained, as guidance, the following data retention terms for certain analytics cookies that do not require users’ consent:

- the lifetime of these cookies should be limited to a period that allows a relevant comparison of audiences over time, as it is the case with a period of 13 months, and is not automatically extended for new visits;
- the information collected via these cookies is kept for a maximum period of 25 months; and
- the above-mentioned lifetimes and retention periods are periodically reviewed to ensure that they are limited to what is strictly necessary.

In course of 2021 and 2022, the CNIL undertook massive online investigations in order to check whether the organizations were compliant with the new guidelines. Further to said investigations, several formal notices have been sent to organizations from different sectors (major platforms of the digital economy, e-commerce companies, car rental companies, public service authorities, bank companies, etc.). The CNIL has also fined companies for non-compliance regarding the use of cookies. Heavy sanctions have been applied to GAFAM companies in particular, with administrative fines up to 90 million Euros for failures to comply with Article 82 of the Law. It is interesting to note that, in its decisions regarding cookies, the CNIL imposes its competence even in the presence of a Lead Authority appointed by the company sanctioned, on the ground that the French Supervisory Authority remains the competent authority to control compliance of the e-Privacy Directive requirements, which are specific rules prevailing on the general rules resulting from the GDPR where thus the “One Stop Shop” process does not apply. In March 2023, the CNIL announced that user tracking by mobile phones was a priority topic for its investigations in 2023. It indicated that it carried out several investigations on applications that access identifiers generated by mobile operating systems in the absence of user consent.

KEY CONTACTS

Denise Lebeau-Marianna
Partner
T + 33 (0)1 40 15 24 98
denise.lebeau-marianna@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.