

Unofficial translation

This translation is provided for reference purposes only and without any warranty or representation regarding its accuracy or completeness. Reliance on this translation is at your own risk. If you would like to report a translation error or inaccuracy, we encourage you to please contact us.

THE “DATA PROTECTION” ACT

Act No. 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties.

The new draft of the "Data Protection" Act of January 6, 1978 came into force on June 1, 2019. Most notably, it provides "room for maneuver for Member States" authorized by the General Data Protection Regulation (GDPR) which the legislator has chosen to exercise, as well as measures for Directive (EU) 2016/680 to be transposed into French law.

This new wording improves readability of the Act. It specifies the different systems that apply to the types of processing operations: processing covered by the GDPR, processing for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, processing contributing to national defense or State security etc. It also sets forth common provisions that apply to all processing operations.

It is reminded that the objective of the "Data Protection" Act is not to fully restate the provisions of the GDPR, even though it expressly refers to them in certain instances. For any processing operations that fall within the scope of the GDPR, therefore, the GDPR should be read in conjunction with the Act of January 6, 1978 in order to gain a clear understanding of the legal framework.

This new version of the "Data Protection" Act now applies in full in all of Overseas France.

Contents

Title I: Common Provisions

Chapter I – Principles and Definitions

Article 1
Article 2
Article 3
Article 4
Article 5
Article 6
Article 7

Chapter II: CNIL (*Commission nationale de l'informatique et des libertés* – French data protection authority)

Section 1: Organization and Tasks

Article 8
Article 9
Article 10
Article 11
Article 12
Article 13
Article 14
Article 15
Article 16
Article 17
Article 18

Section 2: Supervision of Processing Activities

Article 19

Section 3: Corrective Measures and Sanctions

Article 20
Article 21

Article 22

Article 23

Section 4: Cooperation

Article 24

Article 25

Article 26

Article 27

Article 28

Article 29

Chapter III: Special Provisions on the Registration Number of Natural Persons in the RNIPP (*répertoire national d'identification des personnes physiques* – national register for identification of natural persons)

Article 30

Chapter IV: Formalities Prior to Commencing Processing Activities

Article 31

Article 32

Article 33

Article 34

Article 35

Article 36

Chapter V: Obligations of Controllers and Rights of Individuals

Article 37

Article 38

Article 39

Chapter VI: Criminal Provisions

Article 40

Article 41

Title II: Processing Under the Data Protection Regime Provided For in Regulation (EU) 2016/679 of 27 April 2016

Chapter I: General Provisions

Article 42
Article 43
Article 44
Article 45
Article 46
Article 47

Chapter II: Rights of the Data Subject

Article 48
Article 49
Article 50
Article 51
Article 52
Article 53
Article 54
Article 55
Article 56

Chapter III: Obligations of the Controller and Processor

Section 1: General Obligations

Article 57
Article 58
Article 59
Article 60
Article 61

Section 2: Obligations Where Processing Is Likely to Result In a High Risk to the Rights and Freedoms of Natural Persons

Article 62
Article 63

Section 3: Processing of Personal Data Concerning Health

Article 64

Subsection 1: General Provisions

Article 65

Article 66

Article 67

Article 68

Article 69

Article 70

Article 71

Subsection 2: Special Provisions on Processing for Medical Research, Study or Evaluation Purposes

Article 72

Article 73

Article 74

Article 75

Article 76

Article 77

Section 4: Processing for Archiving Purposes in the Public Interest, Scientific or Historical Research Purposes or Statistical Purposes

Article 78

Article 79

Section 5: Processing of Personal Data for the Purposes of Journalism and Literary and Artistic Expression

Article 80

Chapter IV: Rights and Obligations for Processing in the Electronic Communications Sector

Article 81

Article 82

Article 83

Chapter V: Provisions Governing the Processing of Personal Data Concerning Deceased Persons

Article 84

Article 85

Article 86

Title III: Provisions Applicable to Processing under Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 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, and Repealing Council Framework Decision 2008/977/JHA

Chapter I: General Provisions.

Article 87

Article 88

Article 89

Article 90

Article 91

Article 92

Article 93

Article 94

Article 95

Article 96

Chapter II: Obligations of Competent Authorities, Controllers and Processors

Article 97

Article 98

Article 99

Article 100

Article 101

Article 102

Article 103

Chapter III: Rights of the Data Subject

Article 104

Article 105

Article 106

Article 107

Article 108

Article 109

Article 110

Article 111

Chapter IV: Transfers of Personal Data To Non-EU Countries or to Recipients Established in Non-EU Countries.

Article 112

Article 113

Article 114

Title IV: Provisions Applicable to Processing in the Interests of State Security and Defense

Article 115

Article 116

Article 117

Article 118

Article 119

Article 120

Chapter II: Other Provisions.

Section 1: Obligations of the Controller

Article 121

Section 2: Obligations of the Processor

[Article 122](#)

Section 3: Transfers of Personal Data To Non-EU Countries or to Recipients Established in Non-EU Countries

[Article 123](#)

[Article 124](#)

Title V: Provisions Relating to Overseas France

[Article 125](#)

[Article 126](#)

[Article 127](#)

[Article 128](#)

Title I: Common Provisions

Chapter I – Principles and Definitions

Article 1

Information technology must serve the needs of every citizen. It must evolve in the context of international cooperation. It must not violate human identity, human rights, privacy, or individual or civil liberties.

The rights of individuals in respect of deciding and controlling how their personal data is used and the obligations of the controllers processing such data are governed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, by Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and by this Act.

Article 2

This Act will apply to automated processing, in whole or in part, of personal data and to non-automated processing of personal data that are or may be contained in a personal data filing system, where the controller meets the conditions provided for in Article 3 of this Act, with the exception of processing carried out by natural persons for the exercise of strictly personal or domestic activities.

A personal data filing system means any structured set of personal data that is accessible according to specific criteria, whether this set is centralized, decentralized or distributed in a functional or geographical manner.

Unless otherwise provided, the definitions set forth in Article 4 of Regulation (EU) 2016/679 of 27 April 2016 will apply for this Act.

Article 3

I. - Nevertheless, with regard to processing within the scope of Regulation (EU) 2016/679 of 27 April 2016, and criteria laid down in Article 3 of that Regulation, all of the provisions of this Act apply to the processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in French territory, whether or not the processing takes place in France.

II. - The national rules adopted on the basis of provisions laid down in said Regulation, giving national law the responsibility to adapt or complete the rights and obligations provided for in that Regulation, apply whenever the data subject resides in France, even if the controller is not established in France.

However, where one of the processing operations referred to in Article 85 (2) of said Regulation is concerned, the national rules referred to in the first paragraph of II will be those to which the controller is subject, when established in the European Union.

Article 4

Personal data must be:

1. Processed fairly and lawfully and, for processing under Title II, transparent with regard to the data subject.
2. Obtained for specific, explicit and legitimate purposes, and not subsequently processed in a manner that is incompatible with those purposes. However, subsequent data processing for archiving purposes in the public interest, scientific and historical research purposes, and statistical purposes is considered compatible with the purposes for which the data were initially collected, if it is carried out in accordance with the provisions of Regulation (EU) 2016/679 of 27 April 2016 and this Act, which are applicable to such processing, and if it is not used to take decisions with respect to data subjects.
3. Adequate, relevant and limited to what is necessary for the purposes for which they are processed, and for processing under Titles III and IV, not excessive.
4. Accurate and, where necessary, 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.
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which they are processed. However, personal data may be kept beyond that period if they are processed exclusively for archiving purposes in the public interest, for scientific or historical research purposes, or statistical purposes.

The conditions laid down in Article L. 212-3 of the Heritage Code (*code du patrimoine*) set forth which data is to be held for archiving purposes in the public interest.

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, or access by unauthorized persons, using appropriate technical or organizational measures.

Article 5

Processing of personal data is only lawful if, and to the extent that, it meets at least one of the following conditions:

1. The data subject has given his consent to the processing, when it falls within Title II, under the conditions referred to in Article 4 (11) and Article 7 of Regulation (EU) 2016/679 of 27 April 2016 mentioned above.
2. The processing is necessary for the performance of a contract to which the data subject is a party or for the implementation of measures at the request of the data subject prior to entering into a contract.
3. The processing is necessary to ensure compliance with a legal obligation to which the controller is subject.
4. The processing is necessary to protect the vital interests of the data subject or of another natural person.
5. The processing is necessary for the performance of a task carried out in the public interest or is under the public authority entrusted to the controller.
6. Except for processing carried out by public authorities in the performance of their tasks, the processing is necessary in the legitimate interests sought by the controller or by a third party, provided that this is not incompatible with the interests or the fundamental rights and freedoms of the data subject requiring data protection, particularly when the data subject is a child.

Article 6

I. - Processing of personal data revealing "racial" or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a

natural person's sex life or sexual orientation is prohibited.

II. - The exceptions to the prohibition referred to in I are set forth in the conditions laid down in Article 9 (2) of Regulation (EU) 2016/679 of 27 April 2016 and in this Act.

III. - Likewise, automated and non-automated processing will not be subject to the prohibition provided for in I when it is in the public interest and is authorized under the rules laid down in Article 31 (II) and Article 32.

Article 7

The provisions of this Act will not preclude the application, for third parties, of provisions concerning access to administrative documents and to public archives.

Accordingly, the holder of a right of access exercised in accordance with other legislative and regulatory provisions relating to access to administrative documents and public archives may not be regarded as an unauthorized person within the meaning of Article 4 (6).

Chapter II: CNIL (*Commission nationale de l'informatique et des libertés* – French data protection authority)

Section 1: Organization and Tasks

Article 8

I. - The CNIL is an independent administrative authority. It is the national supervisory authority within the meaning of and for the application of Regulation (EU) 2016/679 of 27 April 2016. It is entrusted with the following tasks:

1. It informs all data subjects and all controllers of their rights and obligations and may, to this end, provide appropriate information to regional authorities and their associations, and to small and medium-sized enterprises.
2. It ensures that the processing of personal data is carried out in accordance with the provisions of this Act and with other data protection provisions provided for in legislative and regulatory texts, EU law and France's international commitments.

To this end:

- a) It issues an opinion on the processing referred to in Articles 31 and 32.
- b) It prepares and publishes guidelines, recommendations or standards in order to bring the processing of personal data into conformity with texts on personal data protection and to facilitate the preliminary risk assessments carried out by controllers and their processors. It encourages the preparation of codes of conduct that define the obligations incumbent upon controllers and their processors, taking into account the risk involved in processing personal data to the rights and freedoms of natural persons, in particular of children. It endorses and publishes reference methodologies to promote compliance with the processing of personal data concerning health. In all areas of its action, it takes into account the situation of persons lacking digital literacy, and the specific needs of regional authorities, of their associations and of micro, small and medium-sized enterprises.
- c) Working with public and private organizations that represent the relevant stakeholders, it establishes and publishes standard regulations intended to safeguard personal data processing systems and to regulate the processing of biometric, genetic and medical data. To this end, with the exception of processing carried out on behalf of the State exercising its public powers, it may prescribe additional technical and organizational measures, for the processing of biometric data, genetic data and data concerning health pursuant to Article 9 (4) of Regulation (EU) 2016/679 of 27 April 2016 and supplementary safeguards for the processing of personal data relating to criminal convictions and offenses in accordance with Article 10 of said Regulation.
- d) It processes claims, petitions and complaints lodged by a data subject or by a body, organization or association, and examines or investigates the subject matter of the claim, to the extent necessary, and informs the initiator of the claim as to the progress and outcome of the investigation within a reasonable time, particularly if further investigation or coordination with another supervisory authority is required.
- e) It responds to requests for advice from public authorities and, where applicable, jurisdictions, and advises individuals and organizations that set up or intend to set up automated processing of personal data.
- f) It immediately informs the public prosecutor, under the conditions set forth in Article 40 of the Criminal Procedure Code (*code de procédure pénale*), of

any offense or crime of which it has knowledge, and may present its remarks in criminal proceedings, according to the conditions set out in Article 41 of this Act.

g) It may, by special decision, appoint one or more of its members or its general secretary, under the conditions set out in Article 19 of this Act, to undertake or have its staff undertake audits of all processing operations and, where appropriate, obtain copies of all documents or information materials relevant to its tasks.

h) It may decide to provide certification mechanisms for persons, products, data systems or procedures in order to prove compliance with Regulation (EU) 2016/679 of 27 April 2016 and this Act. To this end, it takes into account the specific needs of local authorities, of their associations and of micro, small and medium-sized enterprises. It accredits, for the same purposes, certification bodies, on the basis, where appropriate, of their accreditation by the national accreditation body referred to in Article 43 (1) (b) of said Regulation, or decides, jointly with that body, that the latter may grant accreditation, under conditions specified by decree of the Council of State (*Conseil d'Etat*) passed following an opinion of the CNIL. The CNIL draws up or approves the certification and accreditation reference criteria.

i) It may certify or approve and publish general standards or methodologies for the purposes of certification by approved or accredited third parties in accordance with the methods referred to in point 2 (h) of compliance with this Act with regard to personal data anonymization processes, particularly the re-use of public information posted online under the conditions set out in Title II of Book III of the CRPA (*code des relations entre le public et l'administration* — French Code on Relations between the Public and the Administration).

Such certification is taken into account, where appropriate, for the implementation of sanctions provided for in Section 3 of this Chapter.

j) It responds to requests or referrals provided for in Articles 52, 108 and 118.

k) It may draw up a list of processing operations likely to pose a high risk which require prior consultation in accordance with Article 90.

l) It conducts awareness-raising activities with consumer mediators and public ombudsmen within the meaning of Article L. 611-1 of the Consumer Code (*code de la consommation*) to ensure correct application of this Act.

3. On request or on its own initiative, it issues a seal for products or procedures used in data protection, attesting to their conformity with the

provisions of this Act. If the complexity of the product or procedure so justifies, the Chair may use a qualified independent person to undertake an assessment of them. The cost of this assessment is borne by the company requesting the seal; it can withdraw the seal if, by any means, it finds that the conditions under which it was granted are no longer met.

4. It stays abreast of developments in information technology and publishes, where appropriate, its assessment of the consequences resulting therefrom for the exercise of the rights and freedoms referred to in Article 1.

To this end:

a) It is consulted on any draft bill or decree or any provision of a draft bill or decree relating to personal data protection or the processing of such data. It may also be consulted by the President of the National Assembly (*Assemblée nationale*), the President of the Senate (*Sénat*) or by the standing committees of the National Assembly and the Senate, and also at the request of the president of one of the parliamentary groups, on any bill relating to personal data protection or the processing of such data. In addition to the cases provided for in Articles 31 and 32, where a law provides that a decree or order is passed following consultation with the CNIL, that opinion is published with the decree or order.

b) It proposes legislative or regulatory measures to the Government in order to adapt the protection of civil liberties to developments in IT and digital processes and techniques.

c) At the request of other independent administrative authorities, it may provide assistance with data protection.

d) At the request of the Prime Minister, it may contribute to the preparation and definition of France's position in international negotiations in the field of data protection. At the request of the Prime Minister, it may take part in France's delegations to competent international and EU organizations in this field.

e) It conducts assessments on ethical and societal issues raised by developments in IT and digital technology.

f) As part of its tasks, it promotes the use of privacy enhancing technology, such as data encryption.

5. It may make observations before any court in connection with a dispute concerning the application of this Act and provisions relating to data protection provided for in legislative and regulatory texts, EU legislation,

including Regulation (EU) 2016/679 of 27 April 2016 and France's international commitments.

II. - To achieve its objectives, the CNIL may make recommendations and take individual or regulatory decisions in the cases provided for in this Act.

Each year, the CNIL submits a public report on the performance of its tasks to the President of the Republic and to the Prime Minister.

Article 9

I. - The CNIL is formed of eighteen members:

1. Two delegates and two senators, appointed respectively by the National Assembly and the Senate to ensure pluralistic representation.
2. Two members of the Economic, Social and Environmental Council (*Conseil économique, social et environnemental*), elected by this assembly.
3. Two members or former members of the Council of State, the same grade as a counsellor or higher, elected by the general assembly of the Council of State.
4. Two members or former members of the Court of Cassation (*Cour de cassation*), the same grade as a counsellor or higher, elected by the general assembly of the Court of Cassation.
5. Two members or former members of the Court of Auditors (*Cour des comptes*), the same grade as a counsellor or higher, elected by the general assembly of the Court of Auditors.
6. Three qualified public figures chosen for their knowledge of digital technology and issues surrounding individual liberties, appointed by decree.
7. Two qualified public figures chosen for their knowledge of digital technology and issues surrounding individual liberties, appointed respectively by the President of the National Assembly and the President of the Senate.
8. The Chair of CADA (*Commission d'accès aux documents administratifs* — committee on access to administrative documents) or his representative.

The CNIL also includes the civil rights ombudsman or his representative, who is entitled to a consultative voting right.

The two members appointed or elected by the same authority under points 1 to 5 will include one woman and one man. The three members mentioned in point 6 will include at least one woman and one man.

The two members mentioned in point 7 will include one woman and one man. For the purposes of this rule, any member succeeding a woman will be a man, and vice versa. However, if a member ceases to exercise his/her functions before the end of their term of office or if the term of office of the other member mentioned in point 7 is renewed, the new member appointed will be the same sex as the member being replaced.

Under the terms set forth by decree of the Council of State, half of the electoral college is renewed every two and a half years, with the exception of its Chair.

The Chair is appointed from the members by decree of the President of the Republic for the duration of his term of office. The CNIL elects two Vice-Chairs from its members, one as Deputy Vice-Chair. Together, the Chair and Vice-Chairs form the Executive Committee (*bureau*).

The Chair exercises his functions on a full-time basis. The office of the CNIL Chair is incompatible with any ownership, whether direct or indirect, of interests in a company from the electronic communication or IT sector.

The Chair's term of office is five years.

The Chair of the CNIL receives a salary equivalent to the second highest possible salary for public servants.

When required, the Deputy Vice-Chair exercises the powers of the Chair.

The general secretary is entrusted with the functioning and coordination of support services under the authority of the Chair.

The CNIL's Restricted Committee consists of a Chair and five other members elected by the CNIL from among its members. Executive Committee members are not eligible to sit on the Restricted Committee.

In the event of a tie in the voting, the Chair has the casting vote.

II. - The term of office of the members of the CNIL is five years, renewable once, subject to the tenth and eleventh paragraphs of I.

Article 10

CNIL staff members are appointed by the Chair.

Any members of staff who may be called upon to carry out the audit tasks referred to in Articles 19 and 25 must be authorized by the CNIL. This authorization does not grant exemption from application of provisions that

stipulate the procedures for authorizing access to confidential information protected by law.

Article 11

CNIL staff members are bound by a duty of confidentiality with regard to any facts, acts or information which has come to their knowledge in the course of the performance of their tasks, according to the sanctions set out in Article 413-10 of the Penal Code (*code pénal*) and, insofar as may be necessary for the preparation of the annual report, Article 226-13 of said Code.

Article 12

CNIL's rules of procedure specify the rules for deliberations, examination of files and their presentation before the CNIL, as well as methods for implementing the data protection seal procedure laid down in point 3 of Article 8 (I).

Article 13

Subject to the powers vested in the Executive Committee and Restricted Committee, the CNIL meets in plenary session.

The agenda of the CNIL plenary session is made public.

In the event of a tie in the voting, the Chair has the casting vote.

The CNIL may entrust the Chair or Deputy Vice-Chair to exercise the powers mentioned:

1. In point 2 (f) and (g) of Article 8 (I).
2. In point 2 (d) of Article 8 (I).
3. In point 4 (d) of Article 8 (I).
4. In Articles 52, 108 and 118.
5. In Article 66.
6. In Article 34 (4) of Regulation (EU) 2016/679 of 27 April 2016, for decisions giving notice of compliance with the conditions referred to in Article 34 (3).
7. In points a and h of Article 58 (3) of said Regulation.

A decree of the Council of State, following an opinion of the CNIL, lays down the conditions and restrictions under which the Chair and the Deputy Chair of the CNIL may delegate their signature authority.

Article 14

The CNIL and the CADA meet as a single electoral college, on the joint initiative of their Chairs, when a matter of common interest so justifies it.

Article 15

The CNIL may entrust the Executive Committee with exercising its powers mentioned in the last paragraph of Article 10.

Article 16

The CNIL Restricted Committee takes measures and pronounces sanctions against any controllers or processors failing to comply with the obligations provided in Regulation (EU) 2016/679 of 27 April 2016 and in this Act, under the conditions laid down in Section 3 of this Chapter.

Its members deliberate without CNIL staff members being in attendance, except for those in charge of holding the meeting.

Members of the Restricted Committee may not exercise the powers of the CNIL mentioned in points d, f and g of Article 8 (2) (I) and Article 19 of this Act.

Article 17

A Government commissioner, appointed by the Prime Minister, sits on the CNIL. Assistant commissioners may be appointed under the same conditions.

The Government commissioner attends all of the deliberations of the CNIL meeting in plenary session as well as the deliberations of meetings of its Executive Committee in relation to the exercise of the powers delegated by virtue of Article 15. He may attend Restricted Committee sessions, without being present at the deliberation. He is informed of all opinions and decisions of the CNIL and the Restricted Committee.

He may, except with regard to measures or sanctions under Section 3 of this Chapter, require a second deliberation of the CNIL, to be handed down within ten days of the first.

Article 18

Government ministers, public authorities, executives of state-owned or private companies, heads of various associations and more generally owners and users of data processing and personal data filing systems may not oppose the actions of the CNIL or its members. Rather, they must take all useful steps to facilitate its task.

Except when they are bound by professional secrecy, the persons questioned during audits carried out by the CNIL, in application of point g of Article 8 (I) (2), are bound to supply the information requested by it for the performance of its tasks.

Section 2: Supervision of Processing Activities

Article 19

I. - Members of the CNIL and operational staff accredited under the conditions laid down in the last paragraph of Article 10 have access to the places, premises, enclosures, facilities or buildings used for the processing of personal data from 6 a.m. to 9 p.m. for the performance of their functions.

The public prosecutor in the competent jurisdiction is informed about this beforehand.

When personal data processing operations are carried out, either where parts of these places, premises, enclosures, facilities or buildings are used for private purposes, or where such places, premises, enclosures, facilities or buildings are used entirely for private purposes, the visit may only take place following authorization granted by the custodial judge of the Regional Court (*tribunal de grande instance*) in the jurisdiction of the premises, under the conditions set forth in II of this Article.

II. - The person responsible for these places, premises, enclosures, facilities or buildings is informed of his right to object to the visit. If this person objects, the visit may only take place following authorization

granted by the custodial judge of the Regional Court in the jurisdiction of the premises, who rules under the conditions set forth by decree of the Council of State. However, where the urgency, seriousness of facts underlying the supervision or the risk of destruction or concealment of documents so warrants, the visit may take place without the person responsible for the premises being informed, upon prior authorization from the custodial judge. In this case, the person responsible for these premises may not object to the visit.

The visit will take place under the authority and supervision of the custodial judge, in the presence of the occupant of the premises or his representative who may be assisted by legal counsel of their choice, or, failing this, in the presence of two witnesses independent from the authority in charge of the inspection.

The order authorizing the visit is enforceable on production of the original. It will mention that a referral to the authorizing judge may be made at any time for deferment or interruption of the visit, with information about deadlines and routes of appeal. In accordance with the regulations provided in the Code of Civil Procedure (*procédure civile*), the order may be appealed before the presiding judge of the Court of Appeal (*cour d'appel*). This judge also hears appeals against the conduct of inspection operations, the purpose of which is to perform the tasks set forth in III.

III. - Pursuant to Regulation (EU) 2016/679 of 27 April 2016 and to this Act, in order to perform the tasks of the CNIL, the CNIL members and staff mentioned in the first paragraph of I of this Article may ask for all documents required for the performance of their tasks, in whatever format, and take a copy of them. They may collect, on-site or upon summons, all useful and necessary information or proof for the fulfilment of their task. They may access, under conditions of confidentiality with respect to third parties, IT programs and data, and ask for their transcription, by any appropriate process, into directly utilizable documents for the purposes of the investigation. They may not be held liable for confidentiality, except with regard to information protected by professional secrecy applicable to attorney-client privilege, by source confidentiality in journalistic processing or, subject to the second paragraph of III, by patient confidentiality.

Patient confidentiality is binding if it concerns information contained in processing necessary for the purposes of preventive medicine, medical research, medical diagnosis, administration of care or processing,

or health service management. Communication of personal data concerning health contained in this category of processing may only be requested under the authority and in the presence of a physician.

Outside of on-site investigations and those upon summons, they can carry out any inspections deemed necessary. They may also use an online public communication service to consult data that is freely accessible or made accessible, either by carelessness, negligence or by a third party, by accessing and only staying within the automated processing systems for the time needed to carry out the inspections. They may transcribe the data by any appropriate processing methods onto documents directly utilizable for investigatory needs.

When inspecting online public communication services, the members and staff mentioned in the first paragraph of I may carry out any online operations necessary for their task under an assumed identity, and such actions may not constitute incitement to commit an offense. The use of an assumed identity will not affect the regularity of the findings made in accordance with the third paragraph of III. A decree of the Council of State, passed following an opinion of the CNIL, specifies the conditions under which these members and staff proceed with their findings in such cases.

At the request of the Chair of the CNIL, the members and staff referred to in the first paragraph of I may be assisted by experts.

A report will be prepared on the inspections and visits carried out according to this Article. This report is prepared by both parties when the inspections and visits are carried out on-site or upon summons.

IV. - For processing in the interests of State security that is exempted from the publication of the regulatory ruling that authorizes it by virtue of III of Article 31, the decree of the Council of State which provides for such exemption may also stipulate that the processing will not be subject to the provisions of this Article.

V. - In exercising its supervisory powers over the processing activities covered by Regulation (EU) 2016/679 of 27 April 2016 and this Act, the CNIL will not have the authority to supervise processing operations carried out by the courts when acting in their judicial capacity.

Section 3: Corrective Measures and Sanctions

Article 20

I. - The Chair of the CNIL may issue a warning to a controller or his processor that the intended processing operations are likely to infringe the provisions adopted pursuant to Regulation (EU) 2016/679 of 27 April 2016 or to this Act.

II. - Should the controller or processor fail to comply with the obligations arising from Regulation (EU) 2016/679 of 27 April 2016 or this Act, the Chair of the CNIL may, if the breach discovered is likely to be subject to compliance, serve a formal notice, within a given deadline:

1. To comply with the data subject's requests to exercise his rights.
2. To bring processing operations into compliance with the applicable provisions.
3. With the exception of processing in the interests of State security or defense, to notify the data subject of a personal data breach.
4. To rectify or erase personal data, or to restrict processing of such data.

In the case set out in point 4 above, the Chair may, under the same conditions, order the controller or his processor to inform the data recipients of the steps it has taken.

The deadline for compliance may be set at twenty-four hours in cases of extreme urgency.

The Chair will, where appropriate, rule on the closure of the formal notice procedure.

The Chair may ask the Executive Committee to make the notice public. In this case, the ruling to close the formal notice procedure will also be published at the same time.

III. - Where the controller or his processor fails to comply with the obligations arising from Regulation (EU) 2016/679 of 27 April 2016 or this Act, the Chair of the CNIL may also, after sending him the warning stipulated in I of this Article or, in addition to issuing a formal notice stipulated in II, refer the matter to the Restricted Committee of the CNIL so that it may, following the adversarial procedure, decide on one or more of the following measures:

1. A reminder.
2. An injunction to bring the processing into compliance with the obligations

arising from Regulation (EU) 2016/679 of 27 April 2016 or this Act or to comply with the data subject's requests to exercise his rights. A fine may also be imposed in the maximum amount of EUR 100,000 per day of delay from the date set by the Restricted Committee, except in cases where the processing is carried out by the State.

3. With the exception of processing in the interests of State security or defense or processing operations covered by Title III of this Act when they are carried out on behalf of the State, a temporary or permanent suspension or prohibition of processing, or the withdrawal of an authorization granted under the same Regulation or under this Act.

4. Withdrawal of a certification or an injunction, for the relevant certification body's refusal to grant a certification or withdrawal of a certification granted.

5. With the exception of processing in the interests of State security or defense or processing operations covered by Title III of this Act when they are carried out on behalf of the State, a suspension of data flows to a recipient based in a third country or to an international organization.

6. Partial or full suspension of the decision to approve binding corporate rules.

7. With the exception of processing carried out by the State, an administrative fine up to EUR 10 million or, in the case of a business, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In the cases referred to in Article 83 (5) and (6) of Regulation (EU) 2016/679 of 27 April 2016, these limits are increased to EUR 20 million and 4% of turnover, respectively. The Restricted Committee will take account of the criteria specified in Article 83 to determine the amount of the fine.

The draft decision will, where applicable, be submitted to the other supervisory authorities concerned in accordance with the rules laid down in Article 60 of said Regulation.

Article 21

I. - In cases where failure to comply with the provisions of Regulation (EU) 2016/679 of 27 April 2016 or this Act leads to a violation of the rights and freedoms mentioned in Article 1 of this Act and where the Chair of the CNIL considers that there is an urgent need to act, the Chair will refer the matter to the Restricted Committee, which may, in the context of an adversarial emergency procedure defined by decree of the

Council of State, adopt one of the following measures:

1. A temporary suspension of processing operations, including data transfer outside the European Union, for a maximum period of three months, provided that the processing is not in the interests of State security or defense or processing covered by Title III when it is carried out on behalf of the State.
 2. A limitation on the processing of certain types of personal data for a maximum period of three months, provided that the processing is not in the interests of State security or defense or processing covered by Title III when it is carried out on behalf of the State.
 3. A temporary suspension of the certification issued to the controller or his processor.
 4. A temporary suspension of the accreditation issued to a certification body or a body entrusted with observing a code of conduct.
 5. A temporary suspension of the authorization issued on the basis of Article 66 (III) of this Act.
 6. An injunction to bring the processing into compliance with the obligations arising from Regulation (EU) 2016/679 of 27 April 2016 or this Act, or to comply with the data subject's requests to exercise his rights. A fine may also be imposed in the maximum amount of EUR 100,000 per day of delay from the date set by the Restricted Committee, except in cases where the processing is carried out by the State.
 7. A reminder.
 8. A notification to the Prime Minister to take the necessary measures to stop the violation, provided that the processing is not in the interests of State security or defense or processing covered by Title III when it is carried out on behalf of the State. The Prime Minister will then inform the Restricted Committee of the remedies taken within two weeks of receiving the notification.
- II.** - In the event of the exceptional circumstances provided for in Article 66 of Regulation (EU) 2016/679 of 27 April 2016, when the Restricted Committee adopts the provisional measures provided for in points 1 to 4 of I of this Article, it will immediately communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the European Data Protection Board referred to in Article 68 of said Regulation and to the European Commission.

When the Restricted Committee has taken such measures and it considers that final measures need to be adopted, it will implement the provisions of Article 66 (2) of Regulation (EU) 2016/679 of 27 April 2016.

III. - For processing operations covered by Regulation (EU) 2016/679 of 27 April 2016, where a supervisory authority authorized under said Regulation has not taken appropriate action in a situation where there is an urgent need to act in order to protect the rights and freedoms of the data subject, the Chair of the CNIL will refer the matter to the Restricted Committee, which may request an urgent opinion or an urgent binding decision from the European Data Protection Board, under the conditions and in accordance with the rules laid down in Article 66 (3) and (4) of that Regulation.

IV. - In case of serious and immediate infringement of the rights and freedoms referred to in Article 1 of this Act, the Chair of the CNIL may also request that the competent court, through summary proceedings, order, under penalty as applicable, any measures needed to safeguard these rights and freedoms.

Article 22

The measures provided for in Article 20 (III) and points 1 to 7 of Article 21 (I) of this Act will be adopted on the basis of a report prepared by a member of the CNIL, appointed by the Chair from among members who do not sit on the Restricted Committee. The controller or his processor will be notified of this report and may submit their remarks, and may be represented or assisted. The person who prepared the report may present remarks orally to the Restricted Committee but may not take part in its deliberations. The Restricted Committee may hear any person it believes might contribute useful information to its investigation, including the CNIL's operational staff.

The Restricted Committee may publish the sanctions issued. It may also arrange for them to be published in such journals, newspapers or other media it sees fit, at the expense of the sanctioned parties.

Without prejudice to the communication obligations incumbent upon the controller or his processor under Article 34 of Regulation (EU) 2016/679 of 27 April 2016, the Restricted Committee may request that the controller or his processor communicate, at their own cost, the violation of the provisions of this Act or of the aforementioned Regulation to each affected data subject individually, and any measures prescribed, if applicable.

Whenever the Restricted Committee issues a financial penalty that is final before the criminal court has definitively ruled on the same or related facts, the criminal court judge may order the financial penalty to be deducted from the administrative fine issued.

The penalty payment is calculated by the Restricted Committee, which sets the final amount.

The financial penalties and penalty payments will be collected as sums due to the Government other than taxes and property.

Article 23

Where a certification body or a body entrusted with observing a code of conduct has failed to fulfill its obligations or has not complied with the provisions of Regulation (EU) 2016/679 of 27 April 2016 or those of this Act, the Chair of the CNIL may, where appropriate after formal notice, refer the matter to the CNIL Restricted Committee, which may, under the same conditions as those laid down in Articles 20 to 22, order the withdrawal of the accreditation that was issued to that body.

NOTE: In accordance with Article 29 of Ordinance 2018-1125 of December 12, 2018, these provisions will enter into force at the same time as the decree amending Decree No. 2005-1309 of October 20, 2005 enacted for the application of Act No. 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties, as amended by this order, and no later than June 1, 2019.

Section 4: Cooperation

Article 24

Under the conditions laid down in Articles 60 to 67 of Regulation (EU) 2016/679 of 27 April 2016, the CNIL implements procedures to cooperate and mutually assist supervisory authorities from other EU Member States and conduct joint operations with those authorities.

The CNIL, the Chair, the Executive Committee, the Restricted Committee and CNIL staff will each implement the procedures referred to in the first paragraph of this Article.

The CNIL may make the Executive Committee responsible for:

1. Exercising its powers as the supervisory authority concerned, as per Article 4 of Regulation (EU) 2016/679 of 27 April 2016, and issuing a pertinent and reasoned objection to the draft decision of another supervisory authority.
2. When the CNIL adopts a draft decision as the lead supervisory authority or supervisory authority concerned, implementing the cooperation procedures to oversee the consistency and settlement of disputes provided for in Regulation (EU) 2016/679 of 27 April 2016 and adopting the decision on behalf of the CNIL.

Article 25

I. - For the purposes of Article 62 of Regulation (EU) 2016/679 of 27 April 2016, the CNIL will cooperate with the supervisory authorities of other EU Member States, under the conditions laid down in this Article.

II. - Whether acting as the supervisory authority concerned or the lead authority pursuant to Articles 4 and 56 of Regulation (EU) 2016/679 of 27 April 2016, the CNIL will be competent to handle a complaint lodged with it or possible infringement of the provisions of said Regulation affecting other Member States. The Chair of the CNIL will call on the other supervisory authorities concerned to participate in any joint supervisory operations it decides to conduct.

III. - Whenever a joint supervisory operation takes place on French territory, authorized members or staff of the CNIL, in their capacity as host supervisory authority, will be present alongside the members and staff of any other supervisory authorities taking part in the operation. At the request of the Member State supervisory authority, the Chair of the CNIL may, by special decision, authorize those members or staff of the supervisory authority concerned who present assurances comparable to those required from the CNIL's staff, in accordance with Article 10 of this Act, to exercise, under its authority, all or part of the audit and investigative powers held by the CNIL's members and staff.

IV. - When the CNIL is invited to take part in a joint supervisory operation decided by the supervisory authority of another Member State, the Chair of the CNIL will decide on the terms and conditions of participation, appoint the authorized members and staff and inform the requesting authority of this under the conditions laid down in Article 62 of Regulation (EU) 2016/679 of

27 April 2016.

Article 26

I. - Processing operations covered by Title III will be based on cooperation between the CNIL and the supervisory authorities of other EU Member States under the conditions laid down in this Article.

II. - The CNIL will provide the supervisory authorities of other Member States with relevant information and provide assistance in order to implement, at their request, supervisory measures, such as consultations, inspections and investigations.

The CNIL will reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request containing all the necessary information, including the purpose of and reasons for the request. It cannot refuse to comply with the request unless it is not competent for the subject-matter of the request or for the measures it is requested to execute, or if the request would infringe a provision of EU law or French law.

The CNIL will inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request.

The CNIL may, for the purpose of carrying out its tasks, seek the assistance of a supervisory authority from another EU Member State.

The CNIL will provide reasons for any refusal to comply with a request when it does not consider itself to be competent or considers that complying with the request would constitute an infringement of EU law or French law.

Article 27

When the CNIL acts as lead supervisory authority, pursuant to Article 56 of Regulation (EU) 2016/679 of 27 April 2016, for cross-border processing within the European Union, it will immediately notify the other relevant supervisory authorities of the report prepared by the draftsperson referred to in the first paragraph of Article 22 and of all relevant information from the procedure leading up to the report before the prospective hearing of the controller or his processor. The authorities concerned will be able to attend, by any appropriate means of transmission, the Restricted Committee's hearing of

the controller or his processor, or to be informed of the minutes drawn up following the hearing.

After deliberation, the Restricted Committee will submit its draft decision to the other supervisory authorities concerned in accordance with the procedure laid down in Article 60 of Regulation (EU) 2016/679 of 27 April 2016. In this respect, it will decide whether or not to follow any relevant and reasoned objections raised by these supervisory authorities and, if it decides to withdraw one of the objections, refer the matter to the European Data Protection Board in accordance with Article 65 of said Regulation.

The conditions for application for this Article are defined by decree of the Council of State following an opinion of the CNIL.

Article 28

When the CNIL acts as the supervisory authority concerned, as per Article 4 of Regulation (EU) 2016/679 of 27 April 2016, the Chair of the CNIL will consider the draft corrective measures submitted to the CNIL by a lead supervisory authority.

Where the purpose of such measures is the same as those defined in Article 20 (I) and (II) of this Act, the Chair will decide, where appropriate, to issue a relevant and reasoned objection, in accordance with the rules laid down in Article 60 of said Regulation.

Where the purpose of such measures is the same as those defined in Article 20 (III) of this Act, the Chair will take over the Restricted Committee. The Chair of the Restricted Committee or designated member of the Restricted Committee may, where appropriate, issue a relevant and reasoned objection according to the same rules.

Article 29

The CNIL may, at the request of an authority exercising similar powers to its own in a non-EU state, subject to appropriate personal data protection safeguards and other fundamental rights and freedoms, carry out audits under the same conditions as those laid down in Article 19, except where the processing referred to in Article 31 (I) or (II) is concerned. Subject to the same conditions, it may submit requests for the same purposes to a

supervisory authority exercising similar powers to its own.

The CNIL is authorized to share the information it obtains or holds, at their request, to supervisory authorities exercising similar powers in non-EU countries, subject to appropriate personal data protection safeguards and other fundamental rights and freedoms, except where the processing referred to in Article 31 (I) or (II) is concerned.

For the implementation of this Article, the CNIL will conclude an agreement in advance to set out its relations with the supervisory authority exercising similar powers to its own. This agreement will be published in the Official Journal.

Chapter III: Special Provisions on the Registration Number of Natural Persons in the RNIPP (*répertoire national d'identification des personnes physiques* – national register for identification of natural persons)

Article 30

A decree of the Council of State, passed following a reasoned and published opinion of the CNIL, determines the categories of controllers and the purposes of these processing operations, on the basis of which they may be carried out if they relate to data containing the RNIPP registration number. Processing will be carried out without prejudice to the obligations incumbent upon controllers or their processors under Section 3, Chapter IV of Regulation (EU) 2016/679 of 27 April 2016.

Certain processing operations that involve personal data containing the RNIPP registration number or that require consultation of this register do not fall within the scope of application of the first paragraph of this Article. These include:

1. Processing operations that are strictly for official statistical purposes, those that are carried out by the Official Statistical System (*service statistique public*) and those that do not contain any of the data mentioned in Article 6 (I) or Article 46.
2. Processing operations that are strictly intended for scientific or historical research purposes.
3. Processing operations that are carried out to provide users of public administration services with one or more online e-government services as

defined in Article 1 of Ordinance No. 2005-1516 of December 8, 2005 concerning electronic communication between users and administrative authorities pursuant to Article 1, and between the administrative authorities themselves.

The exemption provided for processing operations whose purposes are mentioned in paragraph 1 and 2 of this Article will apply only if the RNIPP registration number has already been encrypted and replaced with an unintelligible statistical code. This encryption will be renewed at a frequency defined by decree of the Council of State, passed following the reasoned and published opinion of the CNIL. Processing operations whose sole purpose is to perform this encryption are not subject to the first paragraph.

For processing operations whose purposes are mentioned in paragraph 1, the use of unintelligible statistical codes is only permitted within the Official Statistical System.

For processing operations whose purposes are mentioned in point 2, the encryption and, if applicable, the interconnection of two filing systems by assigning unintelligible statistical codes, may not be carried out by the same person or by the controller.

Notwithstanding the first paragraph, processing of personal data concerning health will be governed by Section 3 of Chapter III of Title II, with the exception of:

1. Processing operations mentioned in Article 67.
2. Processing operations containing the RNIPP registration number used as a medical identifier for individuals under Article L. 1111-8-1 of the Code of Public Health (*code de la santé publique*), except for processing operations carried out for research purposes.

Chapter IV: Formalities Prior to Commencing Data Processing.

Article 31

I. - An order of the competent minister(s), passed following the reasoned and published opinion of the CNIL, will authorize processing operations involving personal data carried out on behalf of the State, as well as:

1. Processing in the interests of State security, defense or public security.

2. Processing whose purpose is prevention, research, detection or prosecution of criminal offenses or the execution of criminal convictions or security measures.

The CNIL's opinion will be published together with the order authorizing the processing.

II. - Processing relating to the data mentioned in Article 6 (I) will be authorized by decree of the Council of State passed following the reasoned and published opinion of the CNIL. This opinion will be published with the decree authorizing the processing.

III. - Certain processing operations mentioned in I and II may be exempted, by decree of the Council of State, from the publication of the regulatory act authorizing them. For such processing operations, the notice issued by the CNIL will be published together with the decree authorizing the exemption from publication of the act.

IV. - For the purposes of this Article, processing operations that serve the same purpose, relate to identical categories of data and have the same recipients or categories of recipients may be authorized by a single regulatory act. In this case, each controller will send the CNIL a legal commitment stating that the processing complies with the description in the authorization.

Article 32

A decree of the Council of State, passed following the reasoned and published opinion of the CNIL, authorizes the processing of personal data carried out on behalf of the State, in the exercise of its public powers, in connection with genetic or biometric data necessary for the authentication or verification of individuals' identities.

Article 33

I. - Requests for opinions addressed to the CNIL, by virtue of this Act, will specify:

1. The identity and the address of the controller or, if he is not established in the national territory or in another EU Member State, that of the controller's representative and, where applicable, that of the person submitting the request.

2. The purpose(s) of the processing, and a general description of its functions for processing covered by Articles 31 and 32.
3. If applicable, any combination, alignment or any other forms of linking with other processing operations.
4. The personal data processed, their source and categories of data subjects to whom the processing relates.
5. The period for which the processed data will be stored.
6. The department(s) responsible for carrying out the processing and, for the processing operations covered by Articles 31 and 32, the categories of persons who, because of their duties or for the needs of the department, have direct access to the stored data.
7. The authorized recipients or categories of recipients to which data are disclosed.
8. The function of the person or department where the right of access provided for in Articles 49, 105 and 119 is exercised, as well as the measures relating to the exercise of that right.
9. The steps taken to ensure the security of processing and of data, and the safeguarding of legally confidential information and, where applicable, information about the use of a processor.
10. Where applicable, transfers of personal data intended for a non-EU state, in any form whatsoever.

Requests for opinions on processing in the interests of State security, defense or public security may not include all of the elements listed above. A decree of the Council of State, passed following an opinion of the CNIL, sets out a list of these processing operations and which information the requests for opinions on such processing must contain as a minimum.

II. - The controller, who has previously been authorized and may have been publicly notified under the conditions laid down in Article 36, will inform the CNIL immediately of:

1. Any changes affecting the information mentioned in I.
2. Any cessation of processing.

Article 34

I. - After referring the matter to the CNIL under Articles 31 or 32, the CNIL will make a decision within eight weeks of receipt of the request. However, this period may be extended by six weeks on the basis of a reasoned decision by the Chair.

II. - Any opinion requested from the CNIL about a processing operation that is not delivered by the end of the period provided for in I will be considered as favorable.

Article 35

The acts authorizing the creation of a processing operation, pursuant to Articles 31 and 32, will specify:

1. The purpose and, where applicable, the name of the processing operation.
2. The department where the right of access provided for in Articles 49, 105 and 119 is exercised.
3. The categories of personal data recorded.
4. The authorized recipients or categories of recipients to whom the data are disclosed.
5. Where applicable, exemptions from the communication obligation provided for in Article 116 (III).
6. Where appropriate, the limitations and restrictions on the rights of the data subjects provided for in Article 23 of Regulation (EU) 2016/679 of 27 April 2016 and in Article 107.
7. Where appropriate, the point of contact of the joint controllers for the data subjects.

Article 36

I. - The CNIL will publish, in an open and easily reusable format, a list of automated processing operations that have satisfied one of the formalities laid down in Articles 31 and 32, with the exception of those mentioned in Article 31 (III), and Section 3 of Chapter III of Title II.

For each processing operation, this list will specify:

1. The act containing the decision to create a data processing operation.
 2. The purpose and, where applicable, name of the processing operation.
 3. The identity and the address of the controller or, if he is not established in the national territory or in another EU Member State, those of the controller's representative.
 4. The function of the person or department where the right of access provided for in Articles 49, 105 and 119 is exercised.
 5. The categories of personal data being processed, as well as the authorized recipients and categories of recipients to whom the data are disclosed.
 6. Where applicable, transfers of personal data intended for a non-member state of the EU.
- II.** - The CNIL will publish its opinions, decisions or recommendations.

Chapter V: Obligations of Controllers and Rights of Individuals

Article 37

I. - Subject to this Article, Chapter I of Title V of Law No. 2016-1547 of November 18, 2016 on the modernization of justice in the twenty-first century and Chapter X of Title VII of Book VII of the Code of Administrative Justice (*code de justice administrative*) will apply to actions brought on the basis of this Article.

II. - Where several individuals in a similar situation suffer damage as a result of a similar type of failure of a personal data controller or processor to comply with the provisions of Regulation (EU) 2016/679 of 27 April 2016 or of this Act, a class action may be brought before the civil court or the competent administrative court on the basis of individual cases submitted by the claimant, who will inform the CNIL accordingly.

III. - This action may be brought either to stop the breach referred to in II or to hold the person who caused the damage liable in order to obtain reparation for the material or non-material harm suffered, or both.

However, the person who caused the damage may only be held liable if the event giving rise to the damage occurred after May 24, 2018.

IV. - The following parties may bring this action alone:

1. Associations that have complied with their disclosure requirements for at least five years and whose corporate purpose includes privacy protection or data protection.
2. Consumer protection associations representative at national level and approved under Article L. 811-1 of the Consumer Code, when the processing of personal data affects consumers.
3. Trade union organizations for employees or officials as defined in Articles L. 2122-1, L. 2122-5 or L. 2122-9 of the Labor Code (*code du travail*) or in Article 8 bis (III) of Law No. 83-634 of July 13, 1983 on the rights and obligations of officials or trade unions representing members of the judiciary, when the processing affects the interests of the people whom the bylaws of these organizations are designed to protect.

When an action is intended to claim reparation for damage suffered, it follows the individual reparation procedure laid down in Chapter I of Title V of Law No. 2016-1547 of November 18, 2016 on the modernization of justice for the twenty-first century and in Chapter X of Title VII of Book VII of the Code of Administrative Justice.

Article 38

Any person may instruct an association or organization referred to in Article 37 (IV), an association or an organization whose corporate purpose is associated with the protection of rights and freedoms where such rights and freedoms are disregarded in the personal data processing, or an association of which that person is a member and whose statutory purpose involves the defense of interests in relation to the purposes of the contentious processing, to exercise on its behalf the rights provided for in Articles 77 to 79 and 82 of Regulation (EU) 2016/679 of 27 April 2016. It may also instruct them to act before the CNIL, against it before a judge or against the controller or his processor before a court where a processing operation covered by Title III of this Act is involved.

NOTE: In accordance with Article 29 of Ordinance 2018-1125 of December 12, 2018, these provisions will enter into force at the same time as the decree amending Decree No. 2005-1309 of October 20, 2005 enacted for the application of Act No. 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties, as amended by this order, and no later than June 1, 2019.

Article 39

Where the CNIL has received a claim lodged against a controller or his processor, and considers the grounds for appeal as justified in connection with the protection of a person's rights and freedoms with regard to the processing of his personal data, or more generally, to ensure the protection of these rights and freedoms within its mandate, it may request that the Council of State orders, where appropriate under penalty, the suspension of a data transfer, an extension to the suspension of a transfer that it might have previously ordered. It will then state its conclusions in a reference for a preliminary ruling to the Court of Justice of the European Union in order to assess the validity of the Commission's adequacy decision taken on the basis of Article 45 of Regulation (EU) 2016/679 of 27 April 2016 and of all actions taken by the European Commission in respect of the appropriate safeguards for the transfers referred to in Article 46 of said Regulation.

Where the transfer of data in question did not result from a processing operation carried out by a court in the performance of its judicial function, the CNIL may, under the same conditions, refer to the Council of State for the purpose of ordering, either the suspension of the transfer of data based on a European Commission adequacy decision pursuant to Article 36 of Directive 2016/680 of the European Parliament and of the Council of 27 April 2016, or an extension to the suspension of this transfer, which it would have already ordered itself, pending the Court of Justice of the European Union's assessment of the validity of this adequacy decision.

Chapter VI: Criminal Provisions

Article 40

Infringements of the provisions of this Act are provided for in Section 5 of Chapter VI of Title II of Book II of the Penal Code.

Article 41

The public prosecutor will inform the Chair of the CNIL of any legal proceedings in connection with breaches of the provisions set forth in Section 5 of Chapter VI of Title II of Book II of the Penal Code and, where applicable, the decisions taken in respect of these breaches.

The public prosecutor will inform the Chair of the date and purpose of the judgment hearing sent by registered letter at least ten days before that date.

The court in charge of the investigation or of the judgment may ask the Chair of the CNIL or his representative to submit their comments or to present them orally before the court.

Title II: Processing Under the Data Protection Regime Provided For in Regulation (EU) 2016/679 of 27 April 2016

Chapter I: General Provisions

Article 42

I. -This Title will not apply to processing of personal data carried out:

1. In the course of an activity that does not fall within the scope of EU law, in particular the processing operations mentioned in Title IV.
2. In the course of activities falling within the scope of Chapter II of Title V of the Treaty on European Union.
3. By competent authorities for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
4. To temporary copies made in the course of technical operations for the transmission and provision of access to a digital network for automatic, intermediate and transient storage of data and for the sole purpose of allowing other recipients of the service to benefit from the best possible access to the transmitted information.

II. -This Title will apply without prejudice to Articles 32-3-3, 32-3-4 and 34-4 of the French Postal and Telecommunications Code (*code des postes et des télécommunications*) relating to the liability of intermediate service providers as amended by Article 9 of Law No. 2004-575 of June 21, 2004 on confidence in the digital economy and Article 10 of Law No. 2004-669 of July 9, 2004 on electronic communications and audiovisual communication services.

III. -This Title will apply without prejudice to the provisions of Article 6 of Law No 2004-575 of June 21, 2004 on confidence in the digital economy.

Article 43

The applicable principles, rules and conditions of lawfulness concerning the processing of personal data are those defined in Chapter II of Regulation (EU) 2016/679 of 27 April 2016 and Chapter I of Title I of this Act.

Article 44

Article 6 will neither apply if one of the conditions laid down in Article 9 (2) of Regulation (EU) No 2016/679 of 27 April 2016 is fulfilled, nor for:

1. Processing operations for the purposes of preventive medicine, medical diagnosis, the administration of care or treatment, or health services management carried out by a health professional, or by another person upon whom the obligation of professional secrecy is incumbent by reason of his duties, and any violation of which is punishable under Article 226-13 of the Penal Code.
2. Processing carried out by the National Institute for Statistics and Economic Studies (*Institut national de la statistique et des études économiques*) or one of the ministerial statistical services in accordance with Law No. 51-711 of June 7, 1951 on the obligation, coordination and secrecy of statistics, following an opinion of the National Council for Statistical Information (*Conseil national de l'information statistique*).
3. Processing of data concerning health which is in the public interest and in accordance with the provisions of Section 3 of Chapter III of this Title.
4. Processing, in accordance with the regulations referred to in point 2c of Article 8 (I), carried out by employers or administrations, which involve biometric data strictly required to verify access to the workplace and to the devices and applications used in the tasks entrusted to employees, officers, trainees or providers.
5. Processing relating to the re-use of public information contained in the decisions referred to in Article L. 10 of the Code of Administrative Justice and Article L. 111-13 of the Code of Judicial Organization (*code de l'organisation judiciaire*), provided that the purpose or effect of these processing operations

is not to allow the re-identification of data subjects.

6. Processing necessary for research in the public interest as defined by Article L. 112-1 of the Research Code (*code de la recherche*), provided that it is a matter of overriding public necessity, under the conditions laid down in point 2g of Article 9 of Regulation (EU) 2016/679 of 27 April 2016, following the reasoned and published opinion of the CNIL, in accordance with the rules laid down in Article 34 of this Act.

Article 45

Pursuant to Article 8 (1) of Regulation (EU) 2016/679 of 27 April 2016, if a child is 15 years or over, that child himself may consent to the processing of personal data in relation to the offer of information society services directly to him.

If the child is under 15 years of age, the processing will be lawful only if consent is given jointly by the child and the holder(s) of parental responsibility over that child.

The controller will ensure that all information and communication relating to the data subject is in such a clear and plain language that the child can easily understand.

Article 46

The processing of personal data relating to criminal convictions, offenses or related security measures may only be carried out by:

1. Courts, public authorities and legal persons managing a public service, acting within their legally assigned powers, as well as legal persons governed by private law working in the public justice system and belonging to categories contained in the list established by decree of the Council of State, passed following the reasoned and published opinion of the CNIL, to the extent strictly necessary for their mandate.
2. Court officers, strictly for the performance of duties entrusted to them by law.
3. Natural or legal persons, for the purpose of enabling them to prepare for and, if applicable, bring and pursue a lawsuit as a victim, accused party, or on behalf of the victim or accused party,

and to enforce the decision issued, for a period strictly proportionate to these purposes. Communication to a third party is then only possible under the same conditions and to the extent strictly necessary for the pursuit of these same purposes.

4. The legal persons mentioned in Articles L. 321-1 and L. 331-1 of the Code of Intellectual Property (*code de la propriété intellectuelle*), acting for the rights they manage or on behalf of victims of a violation of the rights provided for in Books I, II and III of said Code for the purpose of defending these rights.

5. Persons re-using public information contained in the decisions referred to in Article L. 10 of the Code of Administrative Justice and Article L. 111-13 of the Code of Judicial Organization, provided that the purpose or effect of the processing operations carried out is not to allow the re-identification of data subjects.

Article 47

The data subject will have the right not to be subject to a court decision involving an assessment of a person's behavior based on automated processing of personal data intended to evaluate certain personal aspects relating to him.

The data subject will have the right not to be subject to a decision based solely on automated processing of personal data, including profiling, which produces legal effects concerning him or significantly affects him, except:

1. In the cases referred to in points (a) and (c) of Article 22 (2) of Regulation (EU) 2016/679 of 27 April 2016, subject to the reservations mentioned in Article 22 (3), and provided that the rules defining the processing and the main characteristics of its implementation are notified, with the exception of legally protected secrets, by the controller to the data subject if he so requests.

2. Individual administrative decisions taken in accordance with Article L. 311-3-1 and Chapter I of Title I of Book IV of the Code of Relations (*code des relations*) between the public and the administration, provided that the processing does not involve the data referred to in Article 6 (I) of this Act. These decisions will contain the explicit reference provided in Article L. 311-3-1 of the Code of Relations between the public and the administration, failing which they will become invalid. For such decisions,

the controller will have expert knowledge of algorithmic processing and its developments so that he may explain, in detail and in an intelligible manner, to the data subject how the processing concerning him has been carried out.

Notwithstanding paragraph 2 of this Article, the data subject will have the right not to be subject to any decision, by which the administration rules on an administrative appeal referred to in Title I of Book IV of the Code of Relations between the public and the administration, taken based solely on automated processing.

Chapter II: Rights of the Data Subject

Article 48

The right to information will be exercised under the conditions laid down in Articles 12 to 14 of Regulation (EU) 2016/679 of 27 April 2016.

In particular, where personal data are collected from a child under the age of 15, the controller will convey the information referred to in Article 13 of that Regulation to the child in clear and easily accessible language.

The data subject from whom personal data concerning him is collected will also be informed, unless he has been previously informed, by the controller or his representative, of the right to specify what will happen to his personal data after his death, under the conditions laid down in Article 85.

Pursuant to Article 23 of the Regulation, the right to information will not apply to data collected under the conditions laid down in Article 14 of that Regulation and used in processing carried out on behalf of the State and in the interest of public security, to the extent that such restriction is necessary to comply with the purposes sought by the processing which are set forth in the act authorizing the processing.

The provisions of the preceding paragraph will apply when the processing is carried out by public authorities charged with official missions, such as tax and customs administration, or carrying out audits on the activity of natural or legal persons which may lead to the detection of an infringement or breach, and to administrative fines or penalties.

Article 49

The right of access will be exercised by the data subject under the conditions laid down in Article 15 of Regulation (EU) 2016/679 of 27 April 2016.

Where there is a risk of concealment or disappearance of personal data, the competent judge may order, by summary proceedings, any steps to prevent this concealment or disappearance.

The provisions of the first paragraph will not apply where the personal data are stored in a manner clearly avoiding any risk to the data subject's privacy and the protection of personal data, and for a period not exceeding that necessary for the sole purpose of creating statistics or carrying out scientific or historical research.

Article 50

The right to rectification will be exercised under the conditions laid down in Article 16 of Regulation (EU) 2016/679 of 27 April 2016.

Article 51

I.-The right to erasure will be exercised under the conditions laid down in Article 17 of Regulation (EU) 2016/679 of 27 April 2016.

II.-In particular, at the request of the data subject, the controller is obligated to erase personal data concerning the data subject without undue delay, which have been collected in relation to the offer of information society services if the data subject was a child at the time of collection. Where the controller has transmitted the data in question to a third party controller, the controller, taking account of available technology and the cost of implementation, will take reasonable steps, including technical measures, to inform the third party controller that the data subject has requested the erasure of any links to, or copy or replication of, those personal data.

In the event of a failure to erase personal data or in the absence of a response from the controller within one month of the request, the data subject may refer the matter to the CNIL, which will rule on the request within three weeks of receiving the complaint.

Article 52

Notwithstanding Articles 49 to 51, for processing carried out by public authorities and private persons charged with an official mission, such as tax and customs administration, the right of access, rectification and erasure will be exercised under the conditions laid down in Article 118, if such restrictions have been provided for in the act authorizing the processing.

The same provisions will be applied where the processing concerns public security, subject to application of the provisions in Title III.

Notwithstanding Articles 49 to 51, for any processing carried out by the financial jurisdictions, when acting in their non-judicial capacity provided for in the Code of Financial Jurisdictions (*code des juridictions financières*), in particular where their functions are likely to reveal irregularities calling for the initiation of legal proceedings, the right of access may be restricted under the conditions laid down in points (e) and (h) of Article 23 (1) of Regulation (EU) 2016/679 of 27 April 2016.

Article 53

The right to restriction of processing will be exercised under the conditions laid down in Article 18 of Regulation (EU) 2016/679 of 27 April 2016.

Article 54

The notification obligation regarding rectification or erasure of personal data or restriction of processing will be exercised under the conditions laid down in Article 19 of Regulation (EU) 2016/679 of 27 April 2016.

Article 55

The right to data portability will be exercised under the conditions laid down in Article 20 of Regulation (EU) 2016/679 of 27 April 2016.

Article 56

The right to object will be exercised under the conditions laid down in Article 21 of Regulation (EU) 2016/679 of 27 April 2016.

This right will not apply where the processing meets a legal obligation

or, under the conditions laid down in Article 23 of said Regulation, when the application of those provisions has been excluded by an express provision of the act authorizing the processing.

Chapter III: Obligations of the Controller and Processor

Section 1: General Obligations

Article 57

Pursuant to Article 24 of Regulation (EU) 2016/679 of 27 April 2016, the controller will implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with said Regulation and with this Act.

The controller and, where applicable, the controller's representative, will maintain a record of processing activities under the conditions laid down in Article 30 of that Regulation. They will designate a data protection officer under the conditions laid down in Section 4 of Chapter IV of the Regulation.

Article 58

I. -The controller will notify the CNIL and the data subject of any personal data breach pursuant to Articles 33 and 34 of Regulation (EU) 2016/679 of 27 April 2016.

II. -A decree of the Council of State, passed following an opinion of the CNIL, sets out the list of processing operations and categories of processing authorized as exempt from the right to communication of a personal data breach governed by Article 34 of said Regulation, where the communication of a disclosure or of unauthorized access to such data is likely to pose a risk to national security, national defense or public security.

The exemption provided for in this Article will apply only to the processing of personal data necessary for the fulfilment of a legal obligation which requires the processing of such data or for the exercise of a task in the public interest with which the controller is charged.

Article 59

Where two or more controllers jointly determine the purposes and means

of processing, their respective obligations will be exercised under the conditions laid down in Article 26 of Regulation (EU) 2016/679 of 27 April 2016 and in this Act.

Article 60

Acting in the capacity of processor will in no way exempt compliance with the applicable provisions of Regulation (EU) 2016/679 of 27 April 2016 and this Act.

Processing by a processor will be governed by a contract or other legal act that is binding on the processor with regard to the controller, in writing, including in electronic form, respecting the conditions laid down in Article 28 of the Regulation.

The processor and, where applicable, his representative will maintain the record referred to in Article 30 of said Regulation.

Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the processor will conclude with that other processor the contract referred to in the second paragraph. The third paragraph will also apply.

Article 61

In accordance with Article 29 of Regulation (EU) 2016/679 of 27 April 2016, the processor or any person acting under the authority of the controller or of the processor, who has access to personal data, is not permitted to process those data except on instructions from the controller, unless otherwise provided for by law or regulation.

Section 2: Obligations Where Processing Is Likely to Result In a High Risk to the Rights and Freedoms of Natural Persons

Article 62

The controller will, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data under the conditions laid down in Article 35 of Regulation (EU) 2016/679 of 27 April 2016.

Article 63

In accordance with Article 36 of Regulation (EU) 2016/679 of 27 April 2016, the controller will consult the CNIL prior to processing where the impact assessment referred to in Article 62 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Section 3: Processing of Personal Data Concerning Health

Article 64

Where the exercise of the right of access applies to personal data concerning health, such data may be communicated to the data subject, as he chooses, either directly or through a physician designated by him for that purpose, in compliance with the provisions of Article L. 1111-7 of the Code of Public Health.

Subsection 1: General Provisions

Article 65

Processing of personal data concerning health is subject, in addition to the provisions of Regulation (EU) 2016/679 of 27 April 2016, to the provisions of this Section, with the exception of the following categories of processing:

1. Processing falling within the scope of Article 44 (1) of this Act and of points (a) and (c) to (f) Article 9 (2) of Regulation (EU) 2016/679 of 27 April 2016.
2. Processing that allows studies to be carried out based on the data collected pursuant to Article 44 (1) of this Act if these studies are conducted by the staff responsible for the follow-up of patients and are intended for the exclusive use of the staff.
3. Processing carried out for the purposes of provision of benefits or monitoring by bodies responsible for managing basic health insurance plans as well as the provision of benefits by supplementary health insurance bodies.
4. Processing carried out within health institutions by physicians in charge of medical information, under the conditions laid

down in the second paragraph of Article L. 6113-7 of the Code of Public Health (*code de la santé publique*).

5. Processing carried out by regional health agencies, by the State and by the public entity designated by it under the first paragraph of Article L. 6113-8 of said Code, as defined by Article L. 6113-8 of said code.

Article 66

I. -Processing covered by this Section may only be carried out for the public interest purpose for which it is intended. Assuring high standards of quality and safety of health care and medicines or medical devices is considered a purpose in the public interest.

II. -Example standards and guidelines, within the meaning of points (b) and (c) of Section 2 of Article 8 (I), applying to processing under this Section, will be created by the CNIL in conjunction with the National Institute of Health Data (*Institut national des données de santé*) referred to in Article L. 1462-1 of the Code of Public Health and with public and private organizations representing the stakeholders concerned.

Processing that conforms to these standards may be carried out provided that their controllers send a declaration attesting to this conformity in advance to the CNIL.

These standards may also contain a description and procedural safeguards enabling them to be shared for the purpose of processing of health data sets that pose a low risk of impact to privacy.

III. -Any processing mentioned in I that does not conform to a standard referred to in II may only be carried out following authorization from the CNIL. Authorization will be requested as set out in Article 33.

IV. -The CNIL, with a single decision, may grant a same requester authorization for processing with the same purpose, relating to identical categories of data and with identical categories of recipients

V. -The CNIL will make a decision within two months of receipt of the request. However, this period may be extended once for the same period following a reasoned decision of its Chair or when the National Institute of Health Data has been called upon, as provided for in the second paragraph of Article 72.

The absence of a decision by the CNIL within this time limit is considered to be an acceptance. This provision will not, however,

apply if the authorization is the subject of prior opinion pursuant to subsection 2 of this Section and the opinion(s) delivered is/are not expressly favorable.

Article 67

By way of derogation from Article 66, the processing of personal data concerning health carried out by the organizations or departments entrusted with a public service task contained on a list established by decree of the ministers responsible for health and social security, passed following an opinion of the CNIL, whose sole purpose is to respond, in the event of an emergency, to a health alert and to manage the consequences, in accordance with Section 1 of Chapter III of Title I of Book IV of Part I of the Code of Public Health, is subject to the sole provisions of Section 3 of Chapter IV of Regulation (EU) 2016/679 of 27 April 2016.

The processing referred to in the first paragraph of this Article which contains the RNIPP registration number will be carried out under the conditions laid down in Article 30 of this Act.

The derogations governed by the first paragraph of this Article will end one year after the creation of the processing operation if the latter continues to be carried out beyond that time limit.

Article 68

Notwithstanding the rules on professional secrecy, members of health professions may transmit the personal data they hold to the controller authorized under Article 66.

Where such data may be used to identify someone, they must be transmitted under conditions which guarantee their confidentiality. The CNIL may adopt recommendations or standards on the technical processes to be implemented.

Where the result of data processing is made public, there must be no way to identify data subjects, either directly or indirectly.

Persons called upon to carry out data processing and those who have access to the data to which the processing relates are bound by an obligation of professional secrecy under the penalties provided for in Article 226-13 of the Penal Code.

Article 69

Persons from whom personal data are collected or about which such data are transmitted will be individually informed in accordance with the provisions of Regulation (EU) 2016/679 of 27 April 2016.

However, such information may not be provided if the data subject wanted to make use of the right recognized by Article L. 1111-2 of the Code of Public Health to be left in ignorance of a diagnosis or prognosis.

Article 70

Holders of parental responsibility over children or legal representatives for individuals under guardianship, family empowerment or a lasting power of attorney for protected persons of age whose condition does not allow them to make their own informed personal decision, will be recipients of the information and will exercise the rights of the data subject.

By way of derogation from the first paragraph of this Article, for the processing of personal data carried out for the research referred to in points 2 and 3 of Article L. 1121-1 of the Code of Public Health or for studies or evaluations in the health field, with a purpose that is in the public interest and involves children, the information may be obtained from one of the holders of parental responsibility if it is impossible to inform the other holder or if the other holder cannot be contacted within the time limits consistent with the methodological requirements for conducting the research, study or evaluation in relation to its purposes. This paragraph will not preclude each of the holders of parental responsibility from subsequently exercising the rights referred to in the first paragraph.

For this processing, where a child is at least 15 years of age, he may raise an objection to the holders of parental responsibility having access to the data collected during the research, study or evaluation. The child will then receive the information and he alone will exercise his rights.

For these processing operations, a child who is at least fifteen years of age may raise an objection to the holders of parental responsibility being notified of the data processing if being a data subject leads to information being revealed on preventive action, screening, diagnosis, treatment or intervention in respect of which the child is expressly opposed to the holders of parental responsibility being consulted pursuant to Articles L. 1111-5 and L. 1111-5-1

of the Code of Public Health, or if the family ties are broken and the child benefits personally from health and maternity insurance payments and supplementary coverage established by Law No. 99-641 of July 27, 1999 establishing universal health coverage. He alone will then exercise his rights.

Article 71

Information relating to the provisions of this subsection must be provided, particularly in any establishment or center where prevention, diagnosis and treatment activities are carried out which lead to the transmission of personal data for the processing referred to in this Title.

Subsection 2: Special Provisions on Processing for Medical Research, Study or Evaluation Purposes

Article 72

Automated processing of personal data whose purpose is or will be research or studies in the field of health and the assessment or analysis of treatment or prevention practices or activities will be subject to subsection 1 of this Section, in accordance with this subsection.

The National Institute of Health Data referred to in Article L. 1462-1 of the Code of Public Health may take on or be consulted on, under conditions defined by decree of the Council of State by the CNIL or the minister responsible for health, the matter in connection with the nature of the processing in the public interest referred to in the first paragraph of this Article.

Article 73

With regard to the standards referred to in Article 66 (II) of this Act, reference methodologies will be approved and published by the CNIL. They will be created in conjunction with the National Institute of Health Data referred to in Article L. 1462-1 of the Code of Public Health and public and private organizations representing the stakeholders concerned.

If the processing complies with a reference methodology, it may be carried out without the authorization referred to in Article 66 of this Act,

provided that the controller first sends a declaration attesting to this conformity to the CNIL.

Article 74

Every person has the right to object to personal data relating to him forming the object of the waiver of professional secrecy required due to the nature of the processing referred to in Article 65.

Article 75

In cases where research requires the examination of genetic characteristics, informed and express consent must be obtained from data subjects prior to the data processing being carried out. This Article will not apply to research carried out pursuant to Article L. 1131-1-1 of the Code of Public Health.

Article 76

Authorization for processing will be granted by the CNIL under the conditions laid down in Article 66, following an opinion of:

1. The competent committee for the protection of persons referred to in Article L. 1123-6 of the Code of Public Health, in relation to requests for authorization of research involving humans referred to in Article L. 1121-1 of said Code.
2. The expert committee for health research, studies and evaluations, in relation to requests for authorization of studies or evaluations and research not involving humans within the meaning of point 1 of this Article. A decree of the Council of State, passed following an opinion of the CNIL, establishes the composition of this committee and sets out its rules of operation. Members of the expert committee are subject to Article L. 1451-1 of the Code of Public Health.

The records presented under this Section, excluding research involving humans, will be stored within a single office secured by the National Institute of Health Data, which will ensure that they are forwarded to the competent bodies.

Article 77

In accordance with the tasks and powers of the CNIL and in order to

strengthen the proper application of the rules on security and data protection, an Audit Committee for the National System of Health Data (*système national des données de santé*) is hereby established. This Audit Committee defines an audit strategy and schedule, and notifies the CNIL of this. It carries out audits on all systems, gathering, organizing or making available all or part of the data from the national health data system for research, study or evaluation purposes and on systems that are part of the National System of Health Data.

The Audit Committee includes representatives from the government departments responsible for health, social security and solidarity, the National Health Insurance Fund (*Caisse nationale d'assurance maladie*) responsible for managing the National System of Health Data, other data producers from the National System of Health Data, the National Institute of Health Data as well as an individual representing private stakeholders in the field of health. Qualified specialists may be appointed to the Audit Committee. The Chair of the CNIL, or his representative, will attend the Audit Committee as an observer.

The scope of audits is defined by the Audit Committee and the audits are carried out by providers selected according to criteria and methods that are able to provide assurances as to their competence in auditing information systems and their independence from the audited entity.

The selected provider will submit to the Chair of the Audit Committee the list of people in charge of each audit and the information required to certify their competence and independence.

Audits are carried out as documentary and on-the-spot checks. The procedure followed includes an adversarial phase. Individual medical data may only be communicated under the authority and in the presence of a physician, in connection with information involved in processing required for preventive medicine, medical research, medical diagnosis, administration of care or treatment, or health services management.

For each audit, exchanges will take place, if necessary, between the persons in charge of the audits, the Chair of the Audit Committee, the controller referred to in Article L. 1461-1 of the Code of Public Health and the Chair of the CNIL.

If the Audit Committee becomes aware of information that could reveal serious deficiencies upstream, during an audit or in the event of an objection or impediment to the audit, a report will be sent without undue delay by the Chair of the Audit Committee to the Chair of the CNIL.

Following each audit, a report will be drawn up highlighting any anomalies found as well as any breaches of the rules applicable to the information systems audited.

If serious shortcomings are found during the audit, the Chair of the Audit Committee will be informed, who in turn will inform without delay the Chair of the CNIL and the controller referred to II of Article L. 1461-1 of the Code of Public Health.

In the event of an emergency, the managing director the National Health Insurance Fund may temporarily suspend access to the National System of Health Data prior to completion of the audit if it has sufficient elements for concern regarding serious breaches of the above rules. He will immediately inform the Chair of the Audit Committee and the Chair of the CNIL. Access may only be restored with agreement from the Chair of the CNIL with regard to the corrective measures taken by the audited entity. These provisions are without prejudice to the specific powers of the CNIL.

The final report of each task will be submitted to the Audit Committee, the Chair of the CNIL and the audited controller.

A decree of the Council of State, passed following an opinion of the CNIL, establishes the composition of the Committee and sets out its rules of operation and auditing methods.

Section 4: Processing for Archiving Purposes in the Public Interest, Scientific or Historical Research Purposes or Statistical Purposes

Article 78

Where the processing of personal data is carried out by public archiving services for archiving purposes in the public interest in accordance with Article L. 211-2 of the Heritage Code, the rights provided for in Articles 15, 16 and 18 to 21 of Regulation (EU) 2016/679 of 27 April 2016 do not apply insofar as these rights are likely to render it impossible or seriously impede the achievement of the objectives of that processing. The appropriate conditions and safeguards provided for in Article 89 of said Regulation will be determined by the Heritage Code and other legal provisions and regulations applicable to public archives. They are also ensured by the observance of standards in conformity with the state of the art in the field of electronic archiving.

A decree of the Council of State, passed following the reasoned and published opinion of the CNIL, determines under which conditions and subject to which safeguards derogations are provided, in whole or in part, with regard to the rights provided for in Articles 15, 16, 18 and 21 of said Regulation, concerning processing for scientific or historical research purposes or statistical purposes.

Article 79

Under the conditions of Article 14 (5) of Regulation (EU) 2016/679 of 27 April 2016, where personal data were initially collected for another purpose, the provisions of 1 to 4 of said Article 14 will not apply to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or to the reuse of such data for statistical purposes under the conditions of Article 7 bis of Law No. 51-711 of June 7 1951 on legal obligation, coordination and confidentiality in the field of statistics.

Section 5: Processing of Personal Data for the Purpose of Journalism and Literary and Artistic Expression

Article 80

By way of derogation, the provisions of Article 4 (5), Articles 6, 46, 48, 49, 50, 53, 118, 119 and Chapter V of Regulation (EU) 2016/679 of 27 April 2016 will not apply where such a derogation is needed to reconcile the right to the protection of personal data with the right to freedom of expression and information, in connection with processing carried out for the purposes of:

1. Academic, artistic or literary expression.
2. Journalism, in accordance with the ethical rules of this profession.

The provisions of the preceding paragraphs will not preclude the application of the provisions of the Civil Code (*code civile*), laws relating to print media or audiovisual press and the Penal Code, which stipulate the conditions for the exercise of the right of reply and which prevent, limit, compensate and, if applicable, sanction violations of privacy and attacks on the reputation of individuals.

Chapter IV: Rights and Obligations for Processing in the Electronic Communication Sector

Article 81

The rights and obligations mentioned in Chapters II and III will apply, subject to the special provisions of this Chapter.

Article 82

Any subscriber or user of an electronic communication service will be informed in a clear and comprehensive manner by the controller or his representative, except if previously notified, regarding:

1. The purpose of any action intended to provide access, electronically, to information previously stored in his electronic connection terminal device, or to record data on this device.
2. The means available to them to object to such action.

Such access or recording may only be carried out provided that the subscriber or user has explicitly expressed, after receiving said information, his consent, which may result from appropriate parameter settings on their connection device or any other system under their control.

These provisions will not apply if the access to data stored on the terminal device of the user or the recording of information on the terminal device of the user is:

1. Either exclusively intended to enable or facilitate communication by electronic means.
2. Or, is strictly necessary for the provision of an online communication service at the user's express request.

Article 83

I. - This Article applies to the processing of personal data carried out in connection with the provision of electronic communication services to the public on publicly available electronic communication networks, including those supporting data collection and identification devices.

For the purposes of this Article, "personal data breach" means a

breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed in connection with the provision of electronic communication services to the public.

II. - In the case of a personal data breach, the provider of electronic communication services to the public will notify the CNIL without undue delay.

When this breach is likely to infringe personal data security or the privacy of a subscriber or other natural person, the provider will also notify the data subject without undue delay.

Notification of a personal data breach to the data subject will not be required, however, if the CNIL has found that appropriate protection measures have been implemented by the provider in order to render the data unintelligible to any person who is not authorized to access it, and that those measures were applied to the personal data affected by the personal data breach.

Failing this, the CNIL may, after examining the gravity of the breach, give notice to the provider to inform the data subjects as well.

III. - Each electronic communication service provider will maintain a record of personal data breaches, listing in particular the conditions, effects and measures taken to remedy them, and will make it available to the CNIL.

Chapter V: Provisions Governing the Processing of Personal Data Relating to Deceased Persons

Article 84

The processing of personal data relating to deceased persons will be governed by the provisions of this Chapter.

The rights referred to in Chapter II will cease upon the data subject's death. However, they may be provisionally upheld under the conditions laid down in Article 85.

Article 85

I. - Any person may draw up instructions for the storage, erasure and communication of his personal data after his death. These instructions may be general or specific.

The general instructions concern all personal data relating to the data subject and may be recorded with a trusted digital third party certified by the CNIL.

The details of the general instructions and the trusted third party with which they are stored are entered in a single registry, the terms of and access to which are set by decree of the Council of State, passed following the reasoned and published opinion of the CNIL.

The specific instructions concern the processing of personal data mentioned in these instructions. They will be stored with the controllers concerned. They will require specific consent directly from the data subject and may not be provided from the data subject's mere approval of the general conditions of use.

The general and specific instructions define how the person intends to exercise the rights mentioned in Chapter II of this title after his death. Compliance with these instructions is without prejudice to the provisions applicable to public archives containing personal data.

Where the instructions provide for communication of data which also contain third party personal data, such communication will be carried out in accordance with this Act.

The data subject may change or revoke his instructions at any time.

The instructions referred to in the first paragraph of I may designate a person responsible for their execution. That person will then, upon the data subject's death, be authorized to read the instructions and request that the controllers concerned carry out these instructions. In the absence of a designation or, unless otherwise directed, in the event of the designated person's death, his heirs will be entitled to read the instructions on the death of their author and request that the controllers concerned carry out the instructions.

Any contractual clause in the general conditions of use for the processing of personal data which restricts the powers attributed to the person by virtue of this Article will be regarded as unwritten.

II. - In the absence of any instructions or unless otherwise directed in these instructions, the heirs of the data subject may, after his death, exercise the rights referred to in Chapter II of this Title II to the extent necessary:

1. For the arrangement and settlement of the deceased's estate. To this end, the heirs may access the processing of personal data which concern him in order to identify and obtain information on the administration and division of the estate.

They may also be entitled to access digital assets or data concerning family heirlooms, which are passed down to heirs.

2. When the controllers become aware of his death. To this end, the heirs may have the user accounts of the deceased closed, object to the continued processing of personal data concerning him or have the data updated.

If the heirs so request, the controller must justify, at no cost to the requester, that he has carried out the operations required under the preceding paragraph.

Disagreements between heirs over the exercise of rights provided for in II will be brought before the competent Regional Court.

III. - All providers of online communication services to the public will inform the user what will happen to the data concerning him on his death and will allow him to choose whether or not to share his data with a third party designated by him.

Article 86

Data concerning deceased persons, including those on death certificates, may be processed for research, study or evaluation purposes in the health field, unless the data subject has expressed, while living, his refusal in writing.

Title III: Provisions Applicable to Data Processing under Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 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, and Repealing Council Framework Decision 2008/977/JHA

Chapter I: General Provisions

Article 87

This Title will apply, without prejudice to Title I, to the processing of personal data for the purposes of the prevention,

investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, by any public competent authority or any other body or entity entrusted to exercise public authority and public powers, hereinafter referred to as competent authority.

In order to be lawful, such processing should be necessary for the performance of a task carried out, for one of the purposes set out in the first paragraph, by a competent authority within the meaning of this first paragraph and where the provisions of Articles 89 and 90 are observed. The processing will ensure, in particular, that the personal data will not be kept for longer than is necessary for the purpose of the file and the nature or gravity of the offenses concerned.

Article 88

The data referred to in Article 6 (I) should not be processed, unless in cases of absolute necessity, subject to appropriate safeguards for the rights and freedoms of the data subject, either laid down by a legislative or regulatory provision, or if it is necessary to protect the vital interests of a natural person or the processing relates to data which are manifestly made public by the data subject.

Article 89

I. - Processing carried out on behalf of the State for at least one of the purposes set out in the first paragraph of Article 87 will be subject to a legislative or regulatory provision passed under the conditions laid down in Article 31 (I) and Articles 33 to 36.

II. - Processing in relation to the data referred to in Article 6 (I) will be subject to a legislative or regulatory provision passed under the conditions laid down in Article 31 (I).

Article 90

Where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, in particular because they involve the data mentioned in Article 6 (I), the controller will carry out a data protection impact assessment.

Where processing is carried out on behalf of the State, this impact assessment will be sent to the CNIL with the request for an opinion provided for in Article 33.

In other cases, the controller or his processor will, prior to the implementation of personal data processing, consult the CNIL, which will also decide within the time limits provided for in Article 34:

1. When a data-protection impact assessment indicates that processing operations involve a high risk if the controller does not take measures to mitigate the risk.
2. When the type of processing, in particular because of the use of new mechanisms, technology or procedures, involves a high risk for the rights and freedoms of data subjects.

Article 91

Personal data collected by the competent authorities for the purposes set out in the first paragraph of Article 87 may not be processed for other purposes unless such processing is authorized by legislative or regulatory provisions or by EU law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 of 27 April 2016 will apply unless processing is carried out for an activity outside the scope of EU law.

Where the competent authorities are responsible for carrying out tasks other than those carried out for the purposes set out in the first paragraph of Article 87, Regulation (EU) 2016/679 of 27 April 2016 will apply to the processing carried out for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless processing is carried out for an activity outside the scope of EU law.

If the processing is subject to specific conditions, the competent authority transmitting the data will inform the recipient of such personal data of these conditions and of the obligation to observe them.

The competent authority transmitting the data will not apply, by virtue of the third paragraph of this Article, different conditions to those applicable to transfers of similar data within the Member State in which the competent authority transmitting the data functions, to recipients established in other EU Member States or to services, bodies and organizations established pursuant to Chapters 4 and 5 of Title V of the Treaty on the Functioning of the European Union.

Article 92

Processing carried out for one of the purposes set out in the first paragraph of Article 87 other than those for which data were collected will be authorized if they are necessary and proportionate for that purpose, subject to compliance with the provisions laid down in Chapter I of Title I and in this Title.

Such processing may include archiving in the public interest for scientific, statistical or historical research, for one of the purposes set out in the first paragraph of Article 87.

Article 93

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will be carried out under the conditions laid down in Article 4 (2) and (5), and processing referred to in Article 91, under Section 4 of Chapter III of Title II.

Article 94

Personal data based on facts will, as far as possible, be distinguished from personal data based on personal assessments.

Article 95

The data subject will have the right not to be subject to a court decision involving an assessment of a person's behavior based on automated processing of personal data intended to evaluate certain personal aspects relating to him.

The data subject will have the right not to be subject to any other decision based solely on automated processing, which produces legal effects concerning him or significantly affects him, or based on automated processing of data intended to use or evaluate certain personal aspects relating to him.

Profiling that results in discrimination against natural persons on the basis of the specific categories of personal data mentioned in Article 6 (I) will be prohibited.

Article 96

Personal data may only be processed by a processor under the conditions laid down in Article 28 (1), (2) and (10) and Article 29 of Regulation (EU) 2016/679 of 27 April 2016 and in this Article.

Processors must provide sufficient guarantees in the implementation of appropriate technical and organizational measures to ensure that the processing meets the requirements of this title and to ensure the protection of the rights of the data subject.

Processing by a processor will be governed by a contract or legal act that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller and the technical and organizational measures intended to ensure the security of processing, and stipulates that the processor acts only on instructions from the controller. The content of this contract or legal act will be specified by decree of the Council of State, passed following an opinion of the CNIL.

Chapter II: Obligations of the Competent Authorities, Controllers and Processors

Article 97

The competent authorities will take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are erased or rectified without delay or are not transmitted or made available. To this end, each competent authority will check, as far as possible, the quality of personal data before they are transmitted or made available.

As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date, will be added.

If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient will be notified without delay. In such a case, the personal data will be rectified or erased or processing will be restricted in accordance with Article 106.

Article 98

The controller, where applicable and as far as possible, will make a clear distinction between personal data of different categories of data subjects, such as:

1. Persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offense.
2. Persons convicted of a criminal offense.
3. Victims of a criminal offense or persons with regard to whom certain facts give rise to reasons for believing that they could be the victim of a criminal offense.
4. Other parties to a criminal offense, such as persons who might be called on to testify in investigations in connection with criminal offenses or subsequent criminal proceedings, persons who can provide information on criminal offenses, or contacts or associates of one of the persons referred to in points 1 and 2.

Article 99

I. - In order to demonstrate that processing is carried out in accordance with this Title, the controller and his processor will implement the measures provided for in points 1 and 2 of Articles 24 and 25 of Regulation (EU) 2016/679 of 27 April 2016 and appropriate measures to ensure a level of security appropriate to the risk, particularly with regard to the processing of particular categories of personal data mentioned in Article 6 of this Act.

II. - In respect of automated processing, the controller or processor, following an evaluation of the risks, will implement measures designed to:

1. Deny unauthorized persons access to processing equipment used for processing.
2. Prevent the unauthorized reading, copying, altering or removing of data media.
3. Prevent the unauthorized input of personal data and the unauthorized inspection, alteration or deletion of stored personal data.
4. Prevent the use of automated processing systems by unauthorized persons using data communication equipment.

5. Ensure that persons authorized to use an automated processing system have access only to the personal data covered by their access authorization.
6. Ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment.
7. Ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input.
8. Prevent the unauthorized reading, copying, altering or deleting of personal data during transfers of personal data or during transportation of data media.
9. Ensure that installed systems may, in the case of interruption, be restored.
10. Ensure that the functions of the system perform, that faults in the functioning are reported and that stored personal data cannot be corrupted by means of a system malfunction.

Article 100

The controller and his processor will maintain a record of processing activities under the conditions laid down in points 1 to 4 of Article 30 of Regulation (EU) 2016/679 of 27 April 2016. This record also contains a general description of the security measures aimed at ensuring a level of security appropriate to the risk, particularly with regard to the processing of particular categories of personal data mentioned in Article 6 (1) of this Act, an indication of the legal basis for the processing operation, including transfers, in which personal data are involved and, where appropriate, the use of profiling.

Article 101

The controller or his processor will keep a log for each automated processing operation involving the collection, alteration, consultation, disclosure including transfers, combination and erasure of such data.

The logs of consultation and disclosure operations will make it possible to establish the justification, date and time of such operations. They will also allow, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

This log will be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings. This log will be made available to the CNIL on request.

Article 102

Articles 31, 33 and 34 of Regulation (EU) 2016/679 of 27 April 2016 will apply to the processing of personal data under this Title.

If a personal data breach relates to personal data that has been transmitted by or to a controller established in another EU Member State, the controller established in France will also notify the controller in the other Member State of the breach without undue delay.

The communication of a personal data breach to the data subject may be delayed, restricted or omitted accordingly and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others.

Article 103

Except where the courts are acting in their judicial capacity, the controller will designate a data protection officer.

A single data protection officer may be designated for several competent authorities, taking account of their organizational structure and size.

The provisions of Articles 37 (5) and (7), 38 (1) and (2) and 39 (1) of Regulation (EU) 2016/679 of 27 April 2016, in connection with the controller, will apply to the processing of personal data falling within the scope of this Title.

Chapter III: Rights of the Data Subject

Article 104

I. - The controller will make the following information available to the data subject:

1. The identity and the contact details of the controller and those of his representative, where applicable.
2. The contact details of the data protection officer, where applicable.
3. The purposes of the processing for which the personal data are intended.
4. The right to lodge a complaint with the CNIL and the contact details of the CNIL.
5. The existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

II. - In addition to the information referred to in I, the controller will give to the data subject, in specific cases, the following additional information to enable him to exercise his rights:

1. The legal basis for the processing.
2. The period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period.
3. Where applicable, the categories of recipients of the personal data, including those established in non-EU countries or international organizations.
4. Where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

Article 105

The data subject will have the right to obtain from the controller confirmation as to whether or not personal data concerning him are being processed, and, where that is the case, access to the personal data and the following information:

1. The purposes of and legal basis for the processing.
2. The categories of personal data concerned.

3. The recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in non-EU countries or international organizations.
4. Where possible, the anticipated period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
5. The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject.
6. The right to lodge a complaint with the CNIL and the contact details of the CNIL.
7. Communication of the personal data undergoing processing and of any available information as to their origin.

Article 106

I. - The data subject has the right to request from the controller:

1. That inaccurate personal data relating to him is rectified without undue delay.
2. That incomplete personal data is completed, including by means of providing a supplementary statement.
3. That personal data concerning him is erased without undue delay where processing infringes the provisions of this Act, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.
4. That processing is restricted in the cases provided for in III of this Article.

II. - If the data subject so requests, the controller must justify that he has carried out the operations required under I.

III. - Instead of erasure, the controller will restrict processing where:

1. The accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained.
2. The personal data must be maintained for the purposes of evidence.

Where processing is restricted pursuant to point 1 of the present III, the controller will inform the data subject before lifting the restriction of processing.

IV. - The controller will inform the data subject of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal.

V. - The controller will communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

VI. - Where personal data has been rectified or erased or processing has been restricted pursuant to I and III, the controller will notify the recipients so that they may rectify or erase the personal data or restrict processing of the personal data under their responsibility.

Article 107

I. - The data subject's rights may be restricted as set forth in II of this Article, to the extent that, and for as long as such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

1. Avoid obstructing official or legal inquiries, investigations or procedures.
2. Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal penalties.
3. Protect public security.
4. Protect national security.
5. Protect the rights and freedoms of others.

These restrictions are provided for in the document establishing the processing.

II. - Where the conditions set out in I are met, the controller may:

1. Delay or restrict communication to the data subject of the information referred to in Article 104 (II) or not communicate this information.
- (2) Deny or restrict the data subject's right of access provided for in Article 105.
3. Not inform the person of any refusal of rectification or erasure of personal data or restriction of the processing of such data, or of the reasons for the refusal, by way of derogation from Article 106 (IV).

III. - In the cases mentioned in point 2 of II of this Article, the controller will inform the data subject, without undue delay, of any refusal or restriction of access and of the reasons for the refusal or restriction. Such information may be omitted where the communication thereof would undermine a purpose under I. The controller will document the factual or legal reasons on which the decision is based and make that information available to the CNIL.

IV. - In case of a restriction of the data subject's rights pursuant to paragraphs II or III, the controller will inform the data subject of the possibility, stipulated in Article 108, of exercising his rights through the CNIL. With the exception of the case provided for in point 1 of II, it will also inform the data subject of the possibility of seeking a judicial remedy.

Article 108

In case of a restriction of the data subject's rights pursuant to Article 107 (II) or (III), the data subject may refer the matter to the CNIL.

The CNIL will instruct one of its members who belongs to or has belonged to the Council of State, the Court of Cassation or the Court of Auditors to carry out the relevant investigations and make the necessary changes. The latter may be assisted by a CNIL member of staff. The CNIL will inform the data subject that all necessary verifications have taken place and of the right to seek a judicial remedy.

Where the CNIL finds, in agreement with the controller, that the disclosure of the data involved in the processing does not call into question its purposes, the security of the state, defense or public security, such data may be disclosed to the requester.

Article 109

I. -The information referred to in Articles 104 to 106 will be provided by the controller to the data subject by any appropriate means, including by electronic means, and, as a general rule, in the same form as the request.

II. -Any communication made or action taken, except where requests are manifestly unfounded or excessive, will be provided free of charge.

Where requests are manifestly unfounded or excessive, the controller may also refuse to act on the request.

In case of doubt, the controller to whom the requests are addressed will bear the burden of demonstrating the manifestly unfounded or excessive character of the requests.

Article 110

Each natural person will be entitled to object, for legitimate reasons, to the processing of personal data concerning him.

The provisions of the first paragraph will not apply where the processing meets a legal obligation or where the application of those provisions has been excluded by an express provision of the document establishing processing.

Article 111

The provisions of this Chapter will not apply where personal data are contained in a judicial decision or case file processed in the course of criminal proceedings. In such cases, access to such data and the conditions for rectification or erasure of such data may be governed only by the provisions of the Criminal Procedure Code.

Chapter IV: Transfers of Personal Data to Non-EU Countries or to Recipients Established Outside the European Union

Article 112

The controller may not transfer data or authorize the transfer of data already transmitted to a non-EU State unless the following conditions are met:

1. The transfer of this data is necessary for one of the purposes set out in the first paragraph of Article 87.
2. Personal data are transferred to a controller established in that non-EU State or to an international organization which is a competent authority entrusted with purposes under the first paragraph of Article 87 in France.
3. Where personal data come from another State, the transfer should take place only after the State from which the data were obtained has given its authorization to the transfer, pursuant to its national law.

However, if prior authorization cannot be obtained in good time,

the personal data may be transferred again without such prior authorization from the State that transferred the data when the new transfer is necessary for the prevention of an immediate and serious threat to public security of another State or to safeguard the essential interests of France. The authority responsible for giving prior authorization will be informed without delay.

4. The European Commission has adopted an adequacy decision pursuant to Article 36 of Directive 2016/680 of 27 April 2016 or, in the absence of such a decision, appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or, in the absence of such a decision and instrument, the controller has assessed all the circumstances surrounding the data transfer and considers that appropriate safeguards exist.

The appropriate safeguards provided in a binding legal instrument mentioned in point 4 may result either from the data protection safeguards mentioned in the agreements implemented with that non-EU state, or from legally binding provisions enforced during the exchange of data.

Where the controller other than a court carrying out a processing operation in the context of its judicial activities transfers personal data based solely on the existence of appropriate safeguards with regard to data protection, it will notify the CNIL of the categories of transfers that come under this framework.

In this case, the controller must document the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred. This information will be made available to the CNIL on request.

Where the European Commission has repealed, amended or suspended an adequacy decision adopted pursuant to Article 36 of Directive (EU) 2016/680 of 27 April 2016, the controller may nevertheless transfer personal data or authorize the transfer of data already transmitted to a non-EU State if appropriate safeguards with regard to the protection of personal data are provided in a legally binding instrument or where the controller, having assessed all the circumstances surrounding the data transfer, considers that appropriate safeguards with regard to the protection of personal data exist.

Article 113

By way of derogation from Article 112, in the absence of an adequacy decision or of appropriate safeguards, the controller of personal

data may transfer or authorize the transfer of data already transmitted to a non-EU State only on the condition that the transfer is necessary:

1. To protect the vital interests of the data subject or of another person.
2. To safeguard legitimate interests of the data subject, where French law so provides.
3. To prevent an immediate and serious threat to public security of another State.
4. In individual cases, for one of the purposes set out in the first paragraph of Article 87.
5. In an individual case, for the establishment, exercise or defense of legal claims relating to these purposes.

In the cases mentioned in point 4 and 5 of this Article, the controller of personal data will not transfer such data if he considers that the fundamental rights and freedoms of the data subject outweigh the public interest in the context of the proposed transfer.

Where a transfer is made for the purpose of protecting the legitimate interests of the data subject, the controller will document the date and time of the transfer, information about the receiving competent supervisory authority, the justification for the transfer and the personal data transferred. It will make this information available to the CNIL on request.

Article 114

The competent supervisory authorities referred to in the first paragraph of Article 87 may, in specific cases, transfer personal data directly to recipients established in a non-EU State only if the other provisions of this Act applicable to processing and pursuant to that same Article 87 are complied with and the following conditions are fulfilled:

1. The transfer is necessary for the performance of a task of the transferring competent authority for one of the purposes set out in Article 87.
2. The transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand.
3. The transferring competent authority considers that the transfer to the competent authority of the other State is ineffective or inappropriate,

in particular because the transfer cannot be achieved in good time.

4. The competent authority of the other State will be informed, without undue delay, unless this is ineffective or inappropriate.

5. The transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

The transferring competent authority will inform the CNIL of transfers which fulfill the conditions laid down in this Article.

The competent authority will document the date and time of the transfer, information about the recipient, the justification for the transfer and the personal data transferred.

Title IV: Provisions Applicable to Processing in the Interests of State Security and Defense

Article 115

This Title will apply, without prejudice to Title I, to the processing of personal data carried out on behalf of the State and which is of interest to State security or defense.

Chapter I: Rights of the Data Subject

Article 116

I. - Where personal data relating to a data subject are collected from the data subject, the controller or his representative will inform the data subject of the following, unless the data subject already has the information:

1. The identity of the controller and those of his representative, where applicable.
2. The purpose of the processing for which the personal data are intended.
3. Whether or not it is compulsory to provide such data.
4. Possible consequences of a failure to provide data.
5. The recipients or categories of recipients of the personal data.

6. Any rights it holds under the provisions of Articles 117 to 120.
7. Where applicable, transfers of personal data intended for a non-member State of the EU.
8. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

Where such data are collected by means of questionnaires, they will make reference to the requirements set out in points 1, 2, 3 and 6.

II. -Where personal data have not been obtained from the data subject, the controller or his representative must provide the data subject with the information listed in paragraph I upon registration of the data or, if the personal data is intended to be disclosed to third parties, at the latest when the personal data are first disclosed to the recipient.

Where personal data were initially collected for another purpose, the provisions of the preceding paragraph will not apply where the data subject has already been informed or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort.

III. - The provisions of I will not apply to data collected under the conditions laid down in II to the extent that such limitation is necessary to respect the purposes of the processing.

Article 117

Each natural person will be entitled to object, for legitimate reasons, to the processing of personal data concerning him.

The provisions of the first paragraph will not apply where the processing meets a legal obligation or where the application of those provisions has been excluded by an express provision of the document authorizing processing.

Article 118

I. - Requests to exercise the right of access, rectification and erasure will be addressed to the CNIL, which will instruct one of its members who belongs to or has belonged to the Council of State, the Court of Cassation or the Court of Auditors to carry out the relevant investigations and make the necessary changes. The latter may be assisted by a CNIL member of staff. The CNIL will inform the data subject that all necessary verifications have taken place

and of the right to seek a judicial remedy.

Where the CNIL finds, in agreement with the controller, that the disclosure of the data involved in the processing does not call into question its purposes, the security of the state, defense or public security, such data may be disclosed to the requester.

Article 119

I. - By way of derogation from Article 118, where the processing is likely to include information whose communication would not involve the purposes for which it was initially intended, the regulatory act authorizing the processing may provide that the rights of access, rectification and erasure may be exercised by the data subject through a direct request to the controller, under the conditions laid down in II to III of this Article.

II. - Upon proof of identity, the data subject has the right to obtain:

1. Confirmation as to whether or not personal data concerning him are being processed.
2. Information concerning the purposes of processing, the categories of personal data processed and the recipients or categories of recipients to whom the personal data have been disclosed.
3. Where applicable, information concerning transfers of personal data intended for a non-member State.
4. Communication of the personal data undergoing processing and of any available information as to their origin.
5. Information about the logic involved in the automatic processing and how to challenge it in the event of a decision taken based on the automated processing and which produces legal effects concerning the data subject.

Requests that are manifestly excessive in number, or where the data subject unreasonably and repetitiously requests information, may be rejected.

III. - Upon proof of identity, the data subject may also request that the controller, as applicable, rectify, complete, update, block or erase any personal data concerning him, which are inaccurate, incomplete, erroneous, outdated, or whose collection, use, disclosure or storage is prohibited.

If the data subject so requests, the controller must justify, at no cost to the requester, that he has carried out the required operations.

In the event of a dispute, the burden of proof will be on the controller through which the right of access is exercised, unless it is established that the contested data has been disclosed by the data subject or with his consent.

If data have been transmitted to a third party, the controller must make every reasonable effort to notify that third party of the operations he has carried out in accordance with the first paragraph of III.

Article 120

The data subject will have the right not to be subject to a court decision involving an assessment of a person's behavior based on automated processing of personal data intended to evaluate certain personal aspects relating to him.

No one will be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of personal data intended to use or evaluate certain personal aspects relating to the data subject.

Chapter II: Other Provisions

Section 1: Obligations of the Controller

Article 121

The controller, taking into account the nature of the data and the risks posed by the processing, will take all necessary precautions to maintain the security of the data and, in particular, to prevent it from being distorted, damaged or being accessed by unauthorized third parties.

Section 2: Obligations of the Processor

Article 122

Personal data may only be processed by a processor, a person acting under the authority of the controller or of the processor, upon the instruction of the controller.

The processor must provide sufficient guarantees to ensure

the implementation of the security and confidentiality measures referred to in Article 4 (6) and Article 121. This requirement does not exempt the controller from his obligation to ensure compliance with these measures.

The contract binding the processor to the controller will stipulate the obligations of the processor with regard to the data protection and confidentiality and that the processor may only act on instructions from the controller.

Section 3: Transfers of Personal Data To Non-EU Countries or to Recipients Established in Non-EU Countries

Article 123

The controller may only transfer personal data to a non-EU State if that State has a sufficient level of protection for the privacy and fundamental rights and freedoms of natural persons with regard to the processing of such data now or in the future.

The adequacy of the level of protection provided by a State will be assessed based on the provisions in force in that State, the security measures applied in it, the specific characteristics of the processing, such as its purposes and duration, and the nature, source and destination of the processed data.

Article 124

However, the controller may transfer personal data to a State that does not comply with the conditions of Article 123 if the person to whom the data relate has given explicit consent to their transfer or if the transfer is necessary under one of the following conditions:

1. To protect the life of that person.
2. To protect public interest.
3. To comply with obligations necessary for the establishment, exercise or defense of legal claims.
4. To consult, under regular conditions, a public register established by legislative or regulatory provisions, that is intended for consultation by the public or persons having a legitimate interest.

5. For the performance of a contract between the controller and the data subject, or in order to take steps at the request of the data subject prior to entering into a contract.

6. At the conclusion or execution of a contract concluded or to be concluded, in the interest of the data subject, between the controller and a third party.

An exception may also be made to the prohibition provided for in Article 123 if such a transfer is authorized by decree, passed following the reasoned opinion of the CNIL, where the processing guarantees a sufficient level of protection for the privacy and fundamental rights and freedoms of natural persons, in particular by virtue of the contractual clauses or internal rules to which it is subject. Where the transferred data is derived from processing created by a regulatory act exempt from publication under Article 31 (III), the decree authorizing the transfer will itself be exempt from publication.

The CNIL will make a decision within two months of receipt of the request for an opinion. However, this period may be renewed once on the basis of a reasoned decision by the Chair. Where the CNIL has not given its decision within these time limits, the opinion requested from the CNIL on the transfer will be deemed favorable.

Title V: Provisions Relating to Overseas France

Article 125

This Act is applicable in New Caledonia, French Polynesia, Wallis and Futuna and the French Southern and Antarctic Lands, as amended by Ordinance No. 2018-1125 of December 12, 2018 pursuant to Article 32 of Law No. 2018-493 of June 20, 2018 on the protection of personal data and amending Act No. 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties and various provisions concerning the protection of personal data.

Article 126

For the purposes of this Act in Saint-Barthélemy, Saint-Pierre and Miquelon, New Caledonia, French Polynesia, Wallis and Futuna and the French Southern and Antarctic Lands, the reference to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data will be replaced by the reference to the regulations in force in mainland France under Regulation (EU) 2016/679 of 27 April 2016.

Article 127

Article 37 of this Act is not applicable in New Caledonia and French Polynesia insofar as it concerns class action before the judiciary courts.

Article 128

I. - For the purposes of Article 37 of this Act in Wallis and Futuna, the wording: "Articles L. 2122-1, L. 2122-5 or L. 2122-9 of the Labor Code (*code du travail*)" is replaced by: "order passed pursuant to Article 73 of Law No 52-1322 of December 15, 1952, establishing a Labor Code for the territories and associated territories within the competence of the Ministry of the Overseas (France) (*ministère de la France d'outre-mer*)."

II. - For the purposes of Articles 65 to 77 of this Act in New Caledonia, French Polynesia, Wallis and Futuna and the French Southern and Antarctic Lands, references to Articles L. 1451-1, L. 1461-1, L. 1462-1, L. 6113-7 and L. 6113-8 of the Code of Public Health are replaced by locally applicable provisions having the same purpose.

III. - For the purposes of Article 67 of this Act in New Caledonia and French Polynesia, the reference to Section 1 of Chapter III of Title I of Book IV of Part I of the Code of Public Health is replaced by locally applicable provisions having the same purpose.

This translation is provided for reference purposes only and without any warranty or representation regarding its accuracy or completeness. Reliance on this translation is at your own risk. If you would like to report a translation error or inaccuracy, we encourage you to please contact us.