kaksikäyttötuotteiden vientivalvonnasta) regulates the export controls of dual use items. The Ministry of Foreign Affairs is the national supervisory and licensing authority for the export of dual use technology. The EU Regulation (EC) No 428/2009 for the control of exports, transfer, brokering and transit of dual-use items is obviously also applicable in Finland.

10 France

Olivia Tambou (Paris-Dauphine University), Maitena Poelemans (CDRE, Universidad de Pau et des pauys de l'Adour)

10.1 Informed consent

10.1.1 General Regulatory Framework

Regulation	Type of regulation (hard law, soft law…)	Brief description and scope
Loi n°78-17 du 6 janvier 1978, (hereinafter LIL)	Main hard French Law on data protection which was modified by the loi n° 2018-493, 20 June 2018 and rewritten by the Ordonnance n°2018-1125 adopted on 12 December 2018 which came into effect on the 1st of June 2019.	**Art. 5 LIL** recalls that the consent is one of the legal grounds for lawful processing and refers to art. 4 §11 and 7 of GDPR. **Art. 45 LIL** is about the conditions applicable to the child's consent in application to art. 8 GDPR. (See section 3) **Art. 75 LIL** is the need in certain cases of an informed and "express" consent for health processing for scientific research purpose when the examination of genetics featured are necessary. Curiously, the GDPR term of explicit consent has not been used in French, which maintains the former used concept of "express consent" without a definition of it. **Art. 82** LIL transposed the consent of the e-privacy Directive. **Art. 85** LIL provides a specific consent of the data subject for the digital will. (See Section 4)
Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatiqu	Administrative Act considered as hard law The decree complete the LIL and also came into force on the 1st of June 2019	**Art. 114** lays down that the explicit consent according to art. 75 of the LIL must be written. When this is impossible, a third party, independent of the data controller must certify the express consent.

e, aux fichiers et aux libertés		
Art. L 103 du code des postes et télécommunications	Hard law, modified by the Ordonnance n°2018-1125	The article aligns the conditions of the consent provided by the GDPR for the delivery of safe on-line services. (Obligation of the provider of the service to have such consent of the user.)
CNIL, Délibération no 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs)	Usually guidelines are considered as soft law in French Law. Faced with the development of the adoption of guidelines by independent administrative authority, the Conseil d'Etat (French Administrative Supreme) Court recognised that it could be seized in order to obtain the annulment of some guidelines adopted in order to concretise European obligations, which have a general and imperative character and therefore affect the behaviours of actors. This is the case of these guidelines of the CNIL, (French SA) based on article 8 LIL, which implements art. 82 LIL on Cookies and other tracking devices. See CE 16 October 2019, n°433069 These new Guidelines repeal the 2013 recommendation, which was not compatible with the new provisions of the GDPR. Thus, these Guidelines update the applicable law, without waiting for the future ePrivacy regulation. These Guidelines are under consultation (with professional, civil society).	These Guidelines are the national transcription of the EDPB Guidelines on consent and its Opinion 5/2019 on the interplay between the e-Privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. The Guidelines refer to art. 82 GDPR and contains 6 articles on its scope, the collection of consent, the setting of the terminal, the specific case of the tracking devices The main novelties are twofold. - "the scrolling down or swiping through a website or application can no longer be viewed as a valid expression of consent to the implementation of cookies. - stakeholders who operate tracking devices must be able to prove that they have obtained the consent." **A period of adaptation**, ending six months after the publication of the future recommendation, is given to the stakeholders in order to allow them to implement the new rules. However, the CNIL announced that it would be able to control the compliance of the data controller and processor to rules regarding consent during the adaptation period. As the CNIL said on its website, "*operators must not read or write any data in the terminal of the users before obtaining consent. They must also leave the possibility for users to access the service even in case of refusal to consent, and they must provide the possibility to withdraw consent in an easily accessible and usable manner*." https://www.cnil.fr/en/cookies-and-other-tracking-devices-cnil-publishes-new-guidelines

	The final recommendation should be published in the first quarter of 2020. Further sectorial recommendations are foreseen, with more practical details on the collection of consent.	The Conseil d'Etat seized by La Quadrature du Net considered that this period of adaptation is part of the margin of manoeuvre of the regulation powers of the CNIL. The Conseil d'Etat considered that there is no violation of the art. 8 of the Charter of Fundamental Rights, nor the art. 7 of the European Convention of Human Rights because the CNIL clearly did not renounced to use its correctives power in case of significant violations. See CE 16 October 2019, n°433069

Main regulatory tools addressing data protection issues and informed consent in France

(i) The GDRP does not apply to purely personal or household activity. Is there any provision under national law for the protection of these data categories?

Art. 2 LIL is a copy/paste of art. 2§2 c) GDPR. It provides that the LIL does not apply to processing of natural person in for the exercise of purely personal or household activity. There is no further provision in French Law for the protection of these data categories. defence

1.C. The GDPR does not apply to national security. Is there any national regulation covering this topic (in terms of data protection issues)?

Art. L.1111-1 of the French defence code defines the strategy of national security in broad terms, which includes the identification and the answers of the public authorities, "of all the threats and risks likely to affect the life of the Nation in particular regarding the population, the territorial integrity, and the permanence of the institutions of the Republic"… Thus, "all the public policies contribute to the National Security", in particular, State security, intelligence, and the fight against terrorism.

Firstly, **art. 31-1 LIL** maintains prior formalities for the processing related to State security and defence, or public security. This implies that a decree of the government or the Minister concerned adopted after the opinion of the CNIL is necessary. The opinion of the CNIL only consultative but it has to be made public.

Secondly, **the title IV LIL** is devoted to the processing related to the State security and defence. It provides an adaptation of the right of the data subject, on the one hand, and of the obligations of the controller and processor for that processing, on the other hand. Furthermore, some provisions provide rules in case of a transfer of data to third countries.

Art. 121 LIL details the right of information of the data subject. **Art. 117** provides a right to object only when the processing is not based on a Law, which excludes such right to object. **Art. 119 LIL** introduces an indirect right to access, to delete and to rectification. The data subject has to address its request to the CNIL, which will be delegated to one of its members who need to be a judge. The Commissioner of the CNIL will check whether the communication of the data put at risk the purposes of the processing, the safety of the State, defence, etc. Finally, **art. 120 LIL** provides a strict prohibition of judicial decision based on automated individual decision-making including profiling and other decisions, which produce legal effects based solely on automated processing.

Thirdly, **art. 58-1 LIL** excludes the communication of a data breach to the data subject "*when it is likely to present a risk to national security, national defence, or public security*".

Beyond the LIL, other rules on data protection related to national security can be found in the internal security code and the code of defence. (See for instance, **art. L222-1** of the internal security code relative to the access of administrative databases and to data held by private operators, or art. **L-223-1 to L-223-8** related to the video surveillance)

To be noticed in France likewise in other Members States there is some discussion on the application of the Tele2Sverige Case. See the French Conseil d'Etat request for a preliminary ruling lodged on 3 August 2018 C-511/18. In its questions the French Conseil d'Etat invites the ECJ to recognize the utility of a general and indiscriminate retention obligation on providers, in the background of serious and persistent threats to national security, and in particular the terrorist threat.

Name of Authority	Is this an independent body?	Number of employees	Level of activity (according to your appreciation)?	Response to requirements, questions, etc. made by the public
Commission Nationale Informatiques et Libertés	Yes, it is an independent administration authority in French Law but without juridical personality	215 Not enough for ensuring all of its tasks See Evolution of the number of employees since 1990 https://www.data.gouv.fr/fr/datasets/effectifs-de-la-cnil/	The CNIL is considered as an active supervisory authority (hereinafter SA) as its website and its annual report 2018 could illustrate. **Important consulting activity** : 120 opinions issued mainly for the government, participation to thirty parliamentary hearings. However, the opinion of the CNIL is not always followed by the politician. See Alicem case. **Important information activity:** several guidance, fact sheets published for the implementation of the GDPR for various public (Smes, the local authorities, the physicians, etc.) several check lists, model, and a DPIA tool, etc. Awareness of general public (data protection literacy regarding data protection security, partnership with the National Education Ministry, etc.), information about the challenges of new technologies	The functioning of the CNIL is not very transparent. Its interne regulation after the GDPR need still to be updated. According to the 2018 Annual report There is no available statistics of the delay for the response of the public. Some actors complain

			and data protection, blockchain, AI, etc. **A patchy regulation activity** including adoption of few recommendations, sectorial tool kits for conformity elaborate with the stakeholders (Smart Grids, social housing, connected cars, etc. See here), referential, certification (recently for the accreditation of DPO), authorisation for some Health processing, etc.) **A pedagogical control activity :** - 11 077 complaints in 2018 (Increase of 20%) see complaints number since 1990 https://www.data.gouv.fr/fr/datasets/plaintes-recues-par-la-cnil/ - 310 investigations See list of the controls of the CNIL since 1990 https://www.data.gouv.fr/fr/datasets/controles-realises-par-la-cnil/ Only 3 sanctions post RGPD (63 sanctions since 2006 see https://www.legifrance.gouv.fr/rechExpCnil.do?reprise=true&fastReqId=154954635&page=1 Most of the sanctions are now made public.	about the lack of consistency or clarity in the answers of the agents of the CNIL.

Information regarding Data Protection Authority, France

(ii) Does your national legislation introduce a specific definition of "data processing for research purposes"? Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

There is no legal definition in France of data processing for research purposes. The LIL introduces a dual regime of data processing for research purposes:

- **A common regime: See art. 78, 79 LIL**, which is related, likewise art. 89 GDPR, to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A public consultation on the legal regime of the data processing for research purposes launched by the CNIL in July 2019 is ongoing. This consultation could help to have a soft law definition

of research in public interest. Two criteria could be taken into account to grasp this blur concept of research in public interest. The nature, the status of the data controller and the purpose of the processing.

- **A sectorial regime in the area of Health**. **See art. 72-77 de la LIL**. According art. 72 LIL, the public interest of the research concerned can be evaluated by the Institut National des Données de Santé (INDS). This entity can launch this evaluation on its own. The CNIL or the Health Minister can also seize it. A committee of Expert on the public interest (Comité d'expertise sur l'intérêt public), attached to the INDS is in charge to give recommendation to the INDS. The French law called My Health 2022 adopted in July 2019 provides the future transformation of the INDS in a Health Data Hub (HDH). Due to this change, the evaluation of the public interest of the research will be made in the future by the Comité d'Expertise pour les Recherches, les Études, les Évaluations dans le domaine de la santé (CEREES).

In both cases, there is no legal definition of the concept of research in public interest, but much more a series of criteria, indices used to define this concept, which could imply a balance between private interest and public interest. It is a functional concept, which has not an exhaustive materiel definition. (See etude de Simmons and Simmans done for the INDS 2017)

Article L112-1 of the French research code gives only a definition of the term of public research. This definition is based on six purposes, such as:

- the promotion and progress of knowledge,
- the valorisation of the results of the research for the benefit of the society through innovation and technology transfers,
- the knowledge sharing focused on free access,
- the development of a capacity of expertise and support for associations and foundations recognised for its public utility and for the public policies aiming at facing the societal challenges, economic and social needs, and sustainable development,
- the training and by the research,
- the organisation of the open access to scientific data.

Art. L. 112-3 of the research code adds a kind of institutional definition of public research, which is mainly set up on public research establishments (Etablissements publics de recherche) and establishements of higher Education (établissements d'enseignement supérieur) such as the universities.

However, it is clear that not all the processing of these establishments are processing for research in public interest.

(iii) Does your national legislation implement Article 89 of the GDPR, introducing in particular some specific safeguards to adopt in case of data processing for research purposes?

Art. 78 §2 LIL provides that the specific safeguards to adopt will be laid down by a decree. Those specific safeguards have been included in **art. 116** of the Décret no 2019-

536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Firstly, **art. 116 of this decree** clarifies that the derogations to the rights of the data subject (right to access, right to rectification, right to restriction of the processing, and right to object) only apply when those rights make it impossible to fulfil or impedes seriously the specific purposes of the processing or when those derogations are necessary for the purposes specified.

Secondly, only authorised people should have access to and be able to modify the data.

Thirdly, these authorised people have to comply with the rules of deontology of their activity sector.

Fourthly, the authorisations given by the controller or the processor to these people need to respect the specified purposes and the below-mentioned safeguards.

Fifthly, the data has to be anonymised for their dissemination except when an interest in a third party for the communication prevailed in the interest or the rights and fundamental liberties of the data subject. The communication of data needs to be necessary to the presentation of the results of the research. The data released have to be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. (Recall of the principle of minimisation).

Furthermore, **art. 30 LIL** provides the possibility of using the national identification number (NIR) for processing which is exclusively for research and historical purposes. The safeguard required for the application of this derogation are that that processing has to be encrypted by applying a statistical code no significant and that the interconnection between the two files cannot be assumed by the same person or the same controller.

In addition, **art 2 LIL** introduces an additional condition for further processing for scientific or historical research purposes as well as for statistical purposes and archiving purposes in the public interest. Those processing cannot be used for taking a decision on data subjects.

Beyond these common specific safeguards, the LIL introduces some additional measures for the **processing for Health research**.

That processing needs in principle a prior formality. This could be an authorisation of the CNIL after the opinion of the "Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé" or a declaration of conformity to a statement ("referentiel)" of the CNIL, which has to be addressed to the CNIL. Currently they are three "referentiels" of the CNIL for Health research stricto sensu :

- Two apply to Health Research involving a human being. (MR-001 : impliquant la personne humaine pour des recherches interventionnelles, MR-003 : impliquant la personne humaine pour des recherches non interventionnelles.) In addition, processing of Health Research involving a human being needs to have the opinion of the Comité des personnes according to **Article L1123-7 of the code of public Health**.
- The MR-004 : for Hearth Research which is not involving a human being. (studies, evaluation)

Two other referentiels address the access of the Health data for actors (hospitals for the purposes of epidemiological and medico-economic studies (M 005) and industrials for (M006 for post-market surveillance studies for instance).

The INDS (or in the future the HDH) keeps public records of the Health research declared conform to a "referential".

(iv) Does your national legislation provide specific cases and safeguards for processing sensitive data beyond article 9 of the GDPR? Which cases? Which safeguards?

Art. 6 LIL is a copy paste of art. 9 GDPR. It was necessary to clarify that there are under French law only one race therefore, art. 6 LIL departs from the letter of art. 9 GDPR by using the word "presumed racial origin". Beyond, the exceptions provided by art. 9§2 GPDR, **art. 6 III LIL** includes the possibility to proceed sensitive data for two kinds of processing when there is a public interest and when that processing is implemented on behalf of the State:

- processing concerning the State Security (Sûreté de l'Etat), defence, and public security or processing of personal data relating to the prevention, investigation, detection and prosecution of criminal convictions, offences or security measure according to art. 31 LIL.

- Processing implemented for the exercise of public authority dealing with genetic data or biometric data necessary for the authentication or the identity controls of individuals according to art. 32 LIL.

In both cases, that processing needs as prior formality an authorisation in a form of a decree adopted after the opinion of the CNIL, which is made public.

Art. 44 of the LIL adds six other possibilities of processing of sensitive data:

1. Processing necessary for preventive medicine, medical diagnosis, and delivery of medical care or treatments, healthcare management. In this case, the safeguard is that the processing must be implemented by a member of a regulated health profession or a person who has an professional secrecy obligation.

2. Statistics processing realised by the Institut national de la statistique et des études économiques or one of the Ministerial Statistical Services covered by the Law n°51-711 adopted the 7 June 1951. The safeguard is that the Conseil national de l'information statistique has to deliver an opinion prior the implementation of this processing.

3. Processing in the area of Health justified by a public interest as mentioned before

4. Processing implemented by administrations or employers with biometric data strictly necessary for the control to workplaces or devices or applications given in their missions to the employees, agents, trainees or providers. The safeguard is that that processing has to comply with a "règlement type" adopted by the CNIL in conjunction with the representatives of the stakeholders. The CNIL adopted this "règlement type" in March 2019. The administration or the employer has to demonstrate why the processing of biometric data is necessary and why an alternative technique cannot be used. The "règlement type" lists the categories of data that can be collected. Therefore, the use of biological sampling is prohibited (saliva, blood). The choice of a particular biometric data has to be justified. Other safeguards measures are provided such as the need for a DPIA, the clarification

of the person who can proceed to these biometric data, the limitation of the retention, modalities for the security of the data, etc.

5. Processing on the reuse of public information given by judicial decisions. This exception covers the actors of the Legaltech sector. The safeguard measure is this reuse is only possible if there is no risk of re-identification of the person.

The processing is necessary to the public research as defined in the code of research. The safeguard measures are that this derogation can only be used when the processing is necessary for important public interest. Furthermore, the CNIL has to give a prior opinion on the processing, which will be made public.

(v) Do you have a national (or some regional) Code(s) of Conducts or national Code of Ethics for data processing in research? Could you please summarize the content of such codes (specifying scope, suggested measures to protect individuals, prohibitions, exemptions, etc.)?

As far as I know, there is not really a code of conduct in the sense of the RGPD regarding the Ethics for data processing in research. This matter is usually addressed through guidelines of stakeholders. For instance, the CNRS (Centre national de la Recherche Scientifique) published guidelines on the application of the GDPR, with some ethical concerns. Furthermore, the CNRS and have a strong ethics policy, which is not only based on data processing and partially inspired by the Ethics requirements of Horizon 2020. Thus, the CNRS Ethics is clearly focused on the sharing of scientific data based on the FAIR (Findable, Accessible, Interoperable, Reusable,) principles. The CNRS has Committee on Ethics (Comité d'éthique called COMETs), which was created in 1994. The ANR,(Agence Nationale de la Recherche) adopted a policy on Ethics and scientific integrity, and imposed a Data Management Plan for all the projects selected. The Comets gives opinion on Research Ethics, which are made public. The Comets gave an opinion on the ethical challenges of the sharing of scientific data in 2015. The first national code of conduct could be the one currently negotiated on data Health with the CNIL and public hospitals and establishments for dependent elderly people. It should include in some ethical concerns but not focus on research due to the actors involved.

(vi) Does your national legislation give specific definitions of data processing for "statistical purposes"? Are there specific rules that apply to such data processing?

There is no general definition of data processing for statistical purposes in the LIL. The LIL sometimes only refers to public statistical purposes. This concept should be interpreted at the light of the Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. Art. 1 of this law provides a definition of public statistics. "The public statistics regroups all the productions issued by:

- statistical survey listed every year by the ministry for economic affairs
- the processing, for general information purposes, of data collected by public administrations and bodies or private entities fulfilling a public service role."

The law of 1951 has been amended and updated several times. It provides the creation of the National Council for Statistical Information (CNIS), which is a forum for consultation between producers and users of official statistics and is responsible for monitoring statistical studies. In 2009, this Act established the Official Statistics Authority (ASP), responsible for ensuring the professional independence of official statisticians. The public statistical system comprises **INSEE and the Ministerial**

Statistical Departments (SSM), which conduct statistical operations in their area of expertise. INSEE and the SSMs, under the Institute's coordination, decide which methods, standards and procedures to apply in preparing and publishing statistics.

LIL refers to public statistics mainly in two articles:

- **Art. 30 1°) LIL** admits a derogation at the interdiction of the processing of the NIR. In that situation the data need to be encrypted data and use of a statistical code no significant specially authorized by the public service of statistics.
- **Art. 44 LIL** mentioned before which enable the processing of sensitive data with safeguard measures.

Art. 78 and 79 LIL concretise article 89 GDPR and clarify the possible derogations for the processing for statistical purposes. **Art. 119 of the decree 2019** provides safeguard measures. Mainly the specific rules regarding processing for statistical purposes are the same as the rules explained before for research purposes.

(vii) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

The French list of the processing, which requires a compulsory DPIA do not explicitly refer to processing for research purposes, but much more to processing of sensitive data and on vulnerable individuals. Obviously, some processing for research purposes will need a prior DPIA in particular in the Health sector. France did not use the possibility to impose DPO beyond the obligations introduced in the GDPR. All the universities and research establishments for instance need to have a DPO under the GPDR conditions because there mostly are public entities.

10.1.2 Rights of data subjects and data processing

(i) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

The chapter II of the title II of the LIL is dedicated to the rights of the data subject. The LIL mainly refers to the correspondent article of the GDPR for the rights of the data subject. This is the case for the right to rectification, the right to limitation, and the right to portability. For the other rights, the LIL provides some clarifications or additional safeguards.

Firstly, regarding **the right to information art. 48 LIL**:

- clarifies that the information of the minor under 15 years of age needs to be given to him in a clear and accessible language. The third sentence of art. 45 LIL clarifies that the information has to be easily understandable by the minor himself.
- includes the obligation to inform the data subject on his right to give guidelines regarding the processing of his data after his death. (More information on Section 4.)
- provides two exceptions for the right to information based on art. 23 GDPR. (Theses exceptions will be explained later one.)

Art. 69 LIL provides a **right to the data subject not be informed** about a diagnostic or prognosis. This rule is based on art**. L-1111-2 of the public Health code**.

Secondly, regarding **the right to access, art. 49 LIL** provides effective judicial protection of this right. The judge can take an injunction in order to avoid the data disappears, including with an interim procedure. **Art. 49 LIL** provides that this right to access does not apply to processing for statistical purposes or for scientific or historical purposes. This derogation can only apply:

- when the data are stored in a manner that avoids any risk of adversely affecting the rights and freedoms of the data subject
- during the time necessary for the purposes of the processing.

Thirdly, regarding **the right to erasure, art 51 II** provides two clarifications.

- The article includes an obligation for the controller to delete personal data collected in relation to information society services when the individual was a minor. This specific right to erasure applies at the request of the individual, who can make this request at his adulthood. This exception should apply to minor in the normal legal definition i.e. under 18 years of age in France, in the lack of explicit reference to art. 8 GDPR. This specific obligation to erasure is complemented by a further obligation for the controller to inform the third-party controller to which he had transmitted the data. The letter of art 22§2 GDPR inspires the modalities of this second obligation. Thus, it is expected that the controller takes reasonable steps including technical measures to inform the other controllers taking into account the available technology and the cost of implementation.
- The last sentence of article 51 II LIL, aims at facilitating the enforcement of these rights. It recalls that in case of a lack of action of the controller one month after the request, the data subject can lodge a complaint with the CNIL, which will have three months to deliberate on this matter.

In addition, French legislator uses in moderation the possibilities of restrictions of data subject rights laid down in Article 23 GDPR.

- **Exception to the right not to be subjected to a decision based solely on automated processing, including profiling (art. 22 GDPR see art. 47 LIL)**

  Firstly, art. 47 LIL harmonises measures to safeguard the data subject's rights when a controller can adopt automated individual decision-making, including profiling. Art. 22 GDPR §3 imposed on the controller justifying of an explicit consent of the data subject or of a contract necessity "at least" to give to the data subject the right to obtain human intervention, to express his or her point of view and contest the decision. Art. 47 LIL 1°) adds the obligation to give to the data subject at his request the rules of the processing and the main features of their implementation, excepted when there is a protected secrecy. This seems to go further than the simply requirement of "the information on the logic involved as well as the significance and the envisaged consequences of such processing for the data subject", made by art. 12§2 f) GDPR. Art. 47 LIL 1°) clearly contains a right of post explanation and not only a right of prior information.

Secondly, **art. 47 2°) LIL** contains a legal ground for a systematic use of administrative individual decisions solely based on automated processing. The purpose is to legalise the generalisation of the use of algorithms by the public administration with adding safeguard measures. The data subject shall be prior informed about the use and the logic of the algorithms in an intelligible way. The data subject shall have a right to appeal against such administrative decisions. The use of automated decisions for the processing of sensitive data is excluded. Controllers have an obligation to control the algorithm and its development. The Conseil Constitutionnel (The French Constitutional Court) in its Decision no. 2018-765 DC of 12 June 2018 gave some useful interpretation of this provision. The French constitutional judge considers that "… *when the principles of the functioning of an algorithm cannot be communicated without infringing on one of the secrets or interests…, no individual decision shall be made on the exclusive basis of this algorithm*" (point 70.) "*Lastly, the data processor must ensure managing the algorithmic processing and its changes in order to be able to explain, in detail and in an intelligible format, to the person in question how the data processing has been implemented to him/her. It results that, as an exclusive basis for an individual administrative decision, algorithms likely to revise by themselves the rules to which they apply cannot be used, without the oversight and validation of the data processor*", (point 71). In other words, the Conseil Constitutionnel warns the administration of not using Machine Learning and not open-source algorithms in order to take individual administrative decisions solely based on automated processing. This is a consequence of the existence of a real right of explanation of algorithmic decision for the data subject. (See the decision, which is available in English here.)

- **The right to information does not apply** (see art. 48 LIL, third sentence):
    - To the indirect collected data (situation of Art. 14 GDPR) made on behalf of the State for public security interest and
    - to the processing made by the public administrations in their mission of control or the enforcement of taxes, or their mission of investigation or finding of an infringement, which could lead to impose administrative fines or penalties.

Art. 51 LIL provides the legal basis for the processing of the financial courts in their mission of control, which can imply a limitation of the right to access justified on art. 23 e) or h) GDPR.

Art. 56 LIL recalls that the right to object cannot apply when there is a legal obligation covering the processing or an exception provided by art. 23 GPDR.

Art. 58 II LIL provides a legal basis for no communication of data breaches to the data subject. However, this could occur only when the processing is covered by a legal obligation, and when it is necessary for the exercise of a mission of public interest and if there is a risk for national security, national defence or public security. Art. 85 of the decree n° 2019-536 clarifies which are the processing covered by this exception.

(ii) Are there any special requirements regarding informed consent at the national level?

There are a few special requirements regarding informed consent at national level. Beyond the mentioned provisions on the consent of the minors, which concretised art. 8

GDPR, some specific requirements exist regarding Health Data of the minors, which will be detailed in the section 3.B.

Art. 75 LIL provides that the informed and explicit consent of the data subject is required when research imposed genetics analysis. This explicit consent shall not apply when:

- the analysis is made from collected data by the concerned body for other purposes and that the data subject informed about the research project did not object to the processing.
- The person cannot be found. In this case a committee (Comité des personnes) needs to assess whether the data subject did not object to the processing of his genetics data and of the scientific interest of the research. (See art. Article L1131-1-1 of the Public Health Code, which does not apply when the anonymity of the data subject is not respected).

Art. 85 LIL provides the need of a specific consent regarding the will of a data subject for the processing of his data after his death. This means that the genuine approbation of the terms of use are not considering as a valid consent of the data subject. (To be detailed below in Section 4).

(iii) Are there any special requirements regarding data processing at the national level?

The LIL provides two kinds of clarification regarding the application of the GDPR in France.

Firstly, **art. 42§4 LIL** maintains the former exception regarding the temporary copies. (Caching). These temporary copies are made in the framework of technical activities of transmission and provision of access to a digital network, for the purposes of automatic, intermediate and temporary storage and performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service. The conformity of this exception introduced in France at the time of the transposition of the Directive 95/46 has been discussed especially because it was not part of the Directive. It is also most likely that this exception is not compliant with the GDPR.

Secondly, **art. 3§2 LIL** adds a provision regarding the law applicable in cross-border cases in the exercise of the national margin of manoeuvre. This provision aims at resolving potential horizontal conflicts between national laws regarding the implementation of opening clauses. The LIL uses the residence criteria in order to protect the fundamental rights of the data subject. The LIL provides an exception for processing carried out for journalistic purposes. In this situation, the establishment criterion will apply.

(iv) Are there any special requirements to exercise data subject's rights (right of access, correction, deletion of personal data)?

Art. 52 LIL provides a special requirement for the right to access, to rectification and to erasure for the processing implemented by public or private authorities in charge of a public mission of control and enforcement of taxes. These special requirements are detailed in **art. 118 LIL**. A member of the CNIL who belongs or was part of the Conseil d'Etat, the Cour de cassation or the Cour des comptes needs to be designed by the CNIL for investigations. On this basis, the CNIL should assess whether the data subject can

access to his data without jeopardising the public security, the defence or State security. Art. 141-145 of the decree n° 2019-536 sets out the modalities of theses indirect rights.

Art. 64 LIL provides the right to the data subject to choose to have direct access to his Health processing or an indirect access through a physician.

10.1.3 Minors, sensitive data and other additional categories of data

(i) Are there additional rules beyond the ones enforced by the GDPR for processing special categories of personal data (e.g. sensitive data or data of legal persons/entities)?

As mentioned before, the LIL contains several provisions regarding the processing of sensitive data (Art. 6 LIL). In addition, **art. 30 LIL** sets out how the national identification number can be processed. **Art. 46 LIL** details the authorities and entities, which can process personal data relating to criminal convictions and offences. This provision contains two novelties beyond the former authorised bodies such as the jurisdictions, auxiliary of justice, entities in charge of the defence of intellectual-property rights. **46 §4 LIL** introduces the possibility of legal or natural persons to process these data in order to prepare or exercise a judicial action as a victim and to enforce a decision. Two safeguards are mentioned. Firstly, the duration of the processing has to be limited to the purposes. Secondly, the communication to third party is only authorised under the same conditions. **Art. 46§5** adds the re-users of public information such as the judicial decisions. It aims at securing the activities of the Legaltech.

There is currently a strong debate in France on the need for developing **facial recognition processing**. The use of facial recognition processing is experimented by cities (such as Nice during its carnival in 2019). Recently, the French Minister of the Interior launched an experimentation of app called Alicem, which imposes a processing of facial recognition as unique authentication in line for several administrative services. La Quadrature du Net considers that this is inconsistent with the GDPR in particular to the requirement of a free consent. The concern is that there is no alternative to another authentication technique than the facial recognition if the data subject wants to use this app (see. Bloomberg article 3 octobre 2019). The Conseil d'Etat has been seized in order to address this issue. Several actors (the CNIL, Ministers, Parliamentarian) call on the need of a national debate on the use of facial recognition. Cedric O, the French State Minister in charge of the Digital proposed firstly to submit the experimentations of facial recognition to a committee comprising administrations, regulators, researchers and citizens for an evaluation

(ii) Are there any special rules when processing personal data of children? At what age can a minor provide consent according to your regulation?

Beyond the rules, regarding the rights mentioned above in section 2.A., **Art. 45 LIL** reduces the threshold of consent for a minor to **15 years old**. French law also adds some specific rules regarding the modalities of this consent. Art. 45 LIL introduces an obligation of **dual consent** (consent from the minor under 13 years to 15 years of age and the consent of the holder of the parental responsibility of the child). The French government has justified this additional condition on the letter of art. 8 RGPD. The Conseil constitutionnel considers that this interpretation was in conformity with the RGPD. The Conseil Constitutionnel declares that "*It follows that the use of the terms "granted or authorized" that the Regulation allows Member States to establish that either consent must be given related to the minor by their parental authority, or that the*

minor is authorized to consent by the parental authority, which therefore implies that dual consent is established in the contested text. The contested provisions are thus not manifestly incompatible with the Regulation for which they have adapted national law." (Point 63 decision n° 2018-765 DC on 12 June 2018, which is available in English here.)

Art. 70 LIL introduces some specific rules regarding the health data of the minors. Firstly, the information needs to be given to the holders of the parental authority. The possibility to give the information to one of the holders of the parental authority is limited to the situation where it is impossible to inform the other parent or when the information cannot be done in time. The minor less than 15 years age have the right to object to the transmission of this information to the holders of the parental authority. In this situation, the minor will exercise his right himself.

Furthermore, art. 8 LIL charges the CNIL to promote the elaboration of a code of conduct regarding the processing of minors. The recommendation was made that the French Ministry of Education elaborates such a code of conduct (see this report made in 2018 p. 11). The Cnil announced in April 2019 that one topic of its strategic plan of control will be on the data of the minors.

(iii) Are there other vulnerable individuals identified in your national legislation?

e LIL contains elements on incapable adults regarding who can be the recipients of information regarding their Health Data. (See **art. 70 LIL**), or who can give an explicit consent to processing of genetic data (See art. L. Article L1131-1-1 of Public Health Code).

The CNIL made some old recommendations on the geolocation of the elderly or disabled people.

Furthermore, 8 categories of processing involving vulnerable individuals are included in the list of processing which required a DPIA (see section 5).

10.1.4 Deceased individuals and personal data

(i) As recital 27 clarifies, the GDPR does not apply to deceased individuals. However, some countries provide people with the right to have all their personal data deleted once they pass away. Some others empower their close relatives to do the same. In some others, these data cannot be used at all without an explicit judicial mandate. What is the situation in your country?

Article 85 LIL provides a digital will regarding the use of the personal data of the data subject after his death. This provision was introduced in 2016 in French law before the GDPR.

Art. 85 LIL offers two options. The data subject can give general guidelines for the storage of all his personal data to a third person certified by the CNIL. The data subject can also give some particular guidelines to the specific controller regarding the processing of his personal data after his death. In this second situation, a specific consent is required. When there are no guidelines, the heirs can exercise the rights of the data subject, when it is necessary:

- for the organisation and the settlement of the inheritance rights
- for the controller to take into account the death of the data subject. The heirs can close the user accounts of the data subject, object to further processing or ask for an update of it.

Art. 86 LIL also provides that the information relating to deceased persons including causes of death can be processed for research, studies and evaluation, in the area of Health except if the data subject opposes to it during his life.

10.1.5 Accountability and Data Protection Impact Assessment

(i) Does your national regulation introduce further provisions related to general accountability? Any particular requirements? Any specific procedures?

(ii) Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research?

The CNIL adopted a list of 14 categories of processing for which a DPIA is compulsory which has been adapted after the opinion of the EDPB. The final list of the CNIL includes:

- processing of Health Data implemented by Health establishments (Hospitals, clinic) or medical and social establishments (establishment for elderly people, Communities Centre for Social Action in municipalities, etc.) for patients care
- processing relating to genetic data of vulnerable persons (such as patients, employees and children)
- processing including profiling for human resources management purposes
- processing for systematic monitoring of the activities of employees purposes
- processing for the management of warnings and reports in the social sector and healthcare.
- processing for the management of warnings and reports at work
- processing of Health Data necessary for the constitution of a register or data repositories
- processing involving profiling of individuals, which could result in an exclusion of a benefit or of a contract, the suspension or the breach of the contact.
- processing of contractual breaches which might lead to a decision of exclusion or the suspension of a contract (automated decision which produces legal effect or similarly significantly affect the data subject)
- Profiling based on data delivered by a third person (such as data brokers)
- Processing of biometric data for the identification of persons including vulnerable persons (the elderly, patients, students, asylum seekers)
- Processing for the requests and the management of social housing
- Processing for social or medico-social support of individuals
- Processing of data localization at large scale, which includes one of the following items at least: collect of sensitive data, systematic monitoring, vulnerable persons, the implementation of new technologies.

The CNIL submitted a list of categories of processing for which a DPIA is not required. The EDPB adopted in July 2019 an opinion on it. The final list published recently includes:

- Processing implemented under the conditions laid down by the applicable texts, solely for human resources purposes by employers with fewer than 250 people, except when profiling is used.
- Some processing relating to breathalyser tests implemented in the framework of transport activities. (Restricted to the situation where those tests are mandatory by law, for the sole purpose of preventing drivers from operating vehicles while under the influence of alcohol or narcotics.)
- Some processing carried out solely for the purpose of managing access controls and schedules excluding any biometric device and excepted processing of sensitive data or data considered as highly personal. ("données à caractère hautement personnel" in French is a subjective approach of personal data.)
- Processing implemented by lawyer, notaries, registrars of the Commercial Court, in the exercise of their profession
- Processing of municipalities for the purposes of the management of the schools, nurseries and extracurricular activities, or for the management of the electoral register.
- Processing for the management of the relation with the providers, or the activities of the Staff Committees,
- Processing implemented by charities for the management of their members and their donors in their habitual activities and only when sensitive data are not at stake
- Processing of individual Health Data necessary for the patient care by physicians in their offices, by a pharmacy or a biological laboratory.

10.2 Commercialization of data

10.2.1 General Regulatory Framework

Regulation	Type of regulation	Brief description and scope
Loi n°78-17 du 6 janvier 1978, (hereinafter LIL)	Hard law	The LIL does not explicitly refer to Data commercialization. Nevertheless, when such commercialisation involves personal data, it needs to comply with the GDPR and the LIL. In particular, **art. 4 of the LIL** copy-paste **art. 5 GDPR** by recalling that personal data need to be processed lawfully, fairly, and in a transparent manner, collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Beside the informed consent, one of the main issues of the commercialisation of personal data is to assess whether the processing can be based on a compatible change of purpose or on other legal grounds such as the legitimate interest of

		the controller, a legal obligation, or the performance of a contract. (**art. 5 LIL** copy-paste **art. 6 GDPR**). Those principles apply in particular to the social scraping (automatic web scraping tools that extracts data from social media channels), which can lead to commercialisation of data. Recently, the CNIL expressed strong reluctance against the use of social web scraping regarding data protection and respect of private life. This opinion was not about social scraping for commercialisation of personal data but for monitoring taxpayers to combat tax fraud.
Protection of the Maker of Databases	Hard law introduced in the art. L-341 to L-343.7 of the Code la propriété intellectuelle (hereinafter CDI)	These provisions adopted by the Loi 98-536 transposed the Directive 96/9 EC. These provisions introduced in French law the *sui generis* right for the maker of a database. Thus, commercialisation of data i.e. subscription to databases, utilisation of the databases can be based on a licence agreement or terms of Use. In French Law, the extraction of a database can also be protected by an action for unfair competition (art. 1240 and 1241 civil code) and parasitism.
Protection of the author	CDI	This protection can apply both to the author of the database and to some content (data) of the database.
Loi n°2016-1321 called Loi République numérique (LRN)	Hard law introduced in the code des relations entre le public et les administrations (CRPA), art.L-321-1 to L-327-1	These provisions created a public service of data in charge of the Open Data policy in particular of master data, which are listed in art. L-321-4 and art LR 321-5 CRPA. Furthermore, French administrations are obliged to communicate all their public data and to facilitate the reuse of these data. There is no protection of the maker of databases or copyright for the administrations. See Conseil d'Etat 8 févr. 2017, n° 389806, NotreFamille.com (Sté). In principle, this reuse is free in an open standard easily useable and readable by an automated system. A fee can be imposed under certain conditions see art. **L-6324-1 and et seq. CRPA** (i.e. to cover the cost of the extraction of data, the digitalisation of collection of libraries, museums or archives) but this implies the use of licences. **Art. D-324-5-1 CRPA** lists a different geographical, meteorological and marine data, which are submitted to a fee. Data of general interest, which are produced by private companies in charge of a public service, are also submitted to the same principles.
Transmission des données à des partenaires à des fins de	Soft law	The main elements of these guidelines are: • The need for a prior consent • The need of indication of the partners

prospection électronique : quels sont les principes à respecter ? CNIL December 2018		• The notification of changes to the list of partners • Limit to further sharing without consent • Notification by the partner at the time of the first communication to the individual
CNIL, Délibération no 2019-093 du 4 juillet 2019 on cookies		Mentioned before in the first Table see Part 1 section 1.

Main regulatory tools addressing data commercialization in France.

10.2.2 Practice

(i) In practice, does your country allow contracts based on exchange of personal data for services (for instance, to gain access to an app)?

There is no general prohibition of such contract, much more element to take into account for such use. In the past, the CNIL gave some advice for the insurance contract pay as you drive. (prior informed consent, limitation of the collection of data to the purpose of the processing, modalities of storage etc.)

The Directive 2019/770 also seems to admit that data can be the counterpart to a service.

(ii) Do you know if these practices are routinely performed?

It is still common for people in France to consider that free access to services or product are the counterpart of giving their personal data. According to a recent study 40% of the French are ready to sales their localisation or their browsing history.

The way other round, the idea that the best way to avoid the commercialisation of his data is to pay for the service is spreading. Recently, the newspaper Liberation made public that it will delete the commercial tracker only for its subscribers.

(iii) Does your country have any specific regulation on the remuneration of data subjects if profit is made out of their data?

More than regulation there are some experimentations, projects, or demands regarding this issue. Some actors such as Generation libre clearly appeal to a legal clarification and campaign for a real property right on personal data. Other actors such as Privacy Tech promote self-data policies by creating tools that the data subject can use in order to clarify the use and conditions of their data. Privacy Tech is for instance working on Privacy Icons inspired by the licence Creative Commons.

The French Apps WeWard, proposed to monetise the data location of the data subject. Apparently, if you walk 75000 or 10 000 steps by the day, which is recommended by the World Health Organisation, you will receive 100 €. The idea is to be paid for receiving adds.

(iv) Do you have any particular national regulation on the secondary use of data?

As mentioned in the above table, national regulation of secondary use of data concerned mainly public data or data of public interest introduced by the LRN. These provisions explicitly refer to the obligation to comply with the LIL and the GDPR.

Secondary uses of data based on abusive Term of Uses can be prohibited. Thus, the French consumer protection can be usefully invoked. The French Association Que Choisir? obtained the annulation of Twitter, Google and Facebook Term of Uses which allowed the social networks to sell the data of its users.

(v) Do you have any specific protection for metadata or non-personal data in your country?

The protection for metadata or non-personal data is mainly based on national texts, which transpose or implement EU Law. Beyond the above-mentioned texts in the table, the Regulation of 2016/679 can be quoted.

10.2.3 Nature of Data

(i) How does your country classify data? Is it a product/commodity/good or service? Do you have an additional construct for data?

French Law does not attribute a general legal status to the data. There is more academic and political debate on this issue. The majority of actors are claiming the affirmation of data as a Good. This is clearly the position of actors who support the idea of a right of property on personal data. This is also the position of actors who support the idea that data are res nullius or should be seen as a new kind of Common, like air, space. Some authors also refer to data as an essential facility, which seems to be more a conception as the data as a service. There is also a recent approach of the data as a tool for the regulation and the regulators. See the recent report of seven French regulators on this topic. The idea is to consider that regulators should animate networks with the users and stakeholders in order to reduce the information asymmetries. In other words, the use of the Big Data is at the core of the improvement of supervisory and regulatory missions. The central issue is not any more the property of the data, but much more the access to the data, and how to share data.

(ii) Except for the Sui Generis Right on the protection of databases, do you have a legislation protecting data in your country (e.g. like copyright)? Are you aware of any mechanisms to determine the value of data?

As mentioned in the above table copyright can be used to protect a database and the content of its.

10.3 Security and cybersecurity

10.3.1 General Regulatory Framework

Regulation	Type of regulation	Brief description and scope
LIL **Art. 4, art. 8 I-2°) c), art. 33, art. 77** **art. 83 LIL and** **Art. 99, 100, 101, 121 and 122 LIL**	Hard law	The LIL contains several provisions on security of the processing. **Art. 4 6° LIL** copy-paste **art. 5f) RGPD**. It includes in addition a specification on the need for a protection against the access from no authorised person to the data by using technical and organisational measures. **Art. 8 I- 2°) c) LIL** provides the CNIL with power to establish "Model Regulation"

(transposition of the directive Police)		(règlement type) with stakeholders that ensure the security of the systems of processing with biometric, genetic and health data. The CNIL can include in those Model Regulation additional technical or organisational measures based on art. 9§4 RGPD. **Art.8 I 4°) f) LIL** provides that the CNIL has to promote the development of Privacy Enhanced Technologies, in particular encryption technologies. **Art.77 LIL** creates an Audit committee of the National Health Data System (Système National des données de Santé) **Art. 83 LIL** introduces in the LIL the obligation of notification of data breaches
Décret n°2019-536	Hard law	**Art. 101** et seq of this Decree provides elements on the composition and the functions of the Audit committee of the National Health Data System.
Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail	Hard law The « Model Regulation », règlement type are administrative act under French law. Thus it is compulsory for the actors.	**Art. 10** of the deliberation imposed security measures regarding the personal data, regarding the organisation, the materials, the software, and informatics channel. **Art. 11** recalls that the DPIA is required for this kind of processing.
CNIL Guide sur la sécurité des données personnelles	Soft law	This guide describes in 17 sheets the main steps for ensuring the security of personal data. The CNIL recommends a four-step procedure: a mapping of the processing, a risk-based analysis of each processing, The implementation of the safeguards measures and the performance on a regular basis of audit on security.

Decree n° 2009-834 du 7 juillet 2009	Hard law	In 2008, the White Paper on Defence and National Security referred to the need to introduce cyber security measures to protect national Security. Therefore the decree n° 2009-834 created a national Cyber security Agency called Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). In July 2010, the President of the French Republic decided to make the Agency responsible for the defence of information systems in addition to its security role. Therefore, the ANSSI made public Information systems defence and security strategy. This strategy is based on four objectives. 1. Becoming a world power in cyber defence 2. Safeguard France's ability to make decisions through the protection of information related to its sovereignty 3. Strengthen the cyber security of critical national infrastructure 4. Ensuring security in cyberspace Gradually, the role of the ANSSI has been enlarged to foster a coordinated, ambitious, pro-active response to cyber security issues in France, for administrations, individuals, businesses.
Loi n° 2013-1168 de programmation militaire	Hard law	**Art. 21 to 23** of the law includes provisions relating to the protection of vital infrastructure against cyber-attacks, which are part of the French code of defence. (**art. L. 1332-1, L. 1332-2, L. 1332-6-1 et seq**)
French national digital security strategy, 2015	Soft law	The French National Digital Security provides five objectives: 1. Ensuring France's freedom of expression and action as well as the security of its critical infrastructure in case of a major cyber attack 2. Protecting the digital lives of citizens and businesses and combat cyber-crime 3. Ensuring the education and training required for digital security

		4. Contributing to the development of an environment that is conducive to trust in digital technology 5. Promoting the cooperation between Member States of the (EU) in a manner favourable to the emergence of a European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of our values.
Loi n° 2018-133 26 February 2018, which transposed the NIS Directive	Hard law	The law opted for a restricted scope limited to the operators of essential services and to digital service providers, but not the operators of vital infrastructure of the above-mentioned law of 2013. (See **art. 5§2** of the 2018 law, which refers to art. L. 1332-1, L. 1332-2, of the code of defence). Stricter obligations than those mentioned in the Directive NIS are still provided for those operators. This seems to conform to article 3 of the NIS directive, which recognizes that the directive provides a minimal harmonisation. Like the NIS directive, the Law recognised only three kinds of digital service providers: the online market place, the online browser, and the cloud services. (**See art. 10**) The law provides for an obligation of notification of the incident to the ASSNI for the operators of essential services (**art. 7)** and for the digital service providers (**art. 13**). The notification is compulsory when the incident has a significant impact on the continuity of services for the operators of essential services, and on the provision of the service for the digital service providers. The significant impact is appreciated regarding the number of users concerned, the duration, the geographical scope. In case of digital service providers, the criteria are the gravity of the disruption of the functioning of the service and the impact on economic and societal activities. These obligations of notification apply to digital service providers established in the EU having their social headquarters or main establishment in France. Digital service providers established outside of the EU offering services in France need to have a representative in France when it

		has not registered such a representative in another Member State. Digital service providers, which employ lest than 50 employees and with annual revenue of less than 10 million euros are excluded from these obligations of notification. (See **art. 11** of the Law). The ANSSI is the national competent authority and contact point as well as the French representative of the Computer security incident response teams under art. 8 and 9 of the NIS directive.
Decree n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique	Hard law	The decree concretises the former law. It lists in its annexe the operators of essential services.
Kit on security and RGPD proposed by the ANSSI	Soft law	This is a package including videos; MOOC, recommendations, guides, sheets on security specially for the administrations, SME's in order to understand, to protect themselves, to raise public awareness among the worker, to choose solutions and trusted experts and to act in case of an incident.

Main regulatory tools addressing security and cybersecurity in France

10.3.2 Implementation of EU Law

(i) Are any particular procedures described in your national regulation?

One of the main particular procedures is the introduction in the LIL and the decree n°2019-536 of **an Audit committee of the National Health Data System**. A senior official of the Ministry of Social Welfare is the chair of the Audit Committee. The other members are presidents of different Heath and public social organisms, a qualified person and a representative of the private actors in the area of Health. The president of the CNIL is also a member of this committee, but with an observatory status. The Audit Committee mainly decides each year on an audit program of processing of the national Health system. **Art. 102 et seq** of the decree provides details on the organisation of the audit. Independent providers deliver the audit. The audit is submitted to classical procedural rules (notification to the entity that will be submitted to an audit, right to oppose to the audit, powers of the auditors, access of the auditors from 8 AM to 8 PM to the premises of the

audited entity, requirement of the physician when the audit implies access to individual personal data, elaboration of the report of the audit with transmission to the submitted entities, etc.) A monitoring of the recommendations issued by the report is foreseen. The annual report of the activities of the Audit Committee including recommendation is transmitted to the Ministry of Social Health care.

(ii) What is the status of the implementation of the NIS directive in your country towards data protection/security of data?

The NIS directive is transposed in France by the Law n ° 2018-133 and the Decree n ° 2018-384. As mentioned in the table, French law contained security obligations for vital infrastructure, which are maintained out of the scope of the Law, which transposed the NIS directive. Likewise, France maintained is former national cyber security adopted in 2015 before the NIS Directive. Based in this strategy, a national system was established in 2017 to provide assistance for victims of cyber malevolence. See the website https://www.cybermalveillance.gouv.fr/

The security measures to apply are fixed by the Prime Minister services with the support of the ANSSI for the operators of essential services. (See **art. 6 of the Law n ° 2018-133,** and **art. 10 of the Decree n ° 2018-384**). The ANSSI or a qualified provider can control these security measures by order of the Prime Minister (art. 8 of the Law n ° 2018-133 the operators of essential services). Art. 14 of the same law provides equivalent control possibilities for Digital service providers. The modalities of control are detailed in art. **13 to 15 of the Decree n ° 2018-384** for the operators of essential services, and art. 22 to 24 for the same Decree for the digital service providers.

(iii) The GDPR stipulates that appropriate technical and organisational measures to protect personal data must be implemented. Is this prevention reflected in your national regulation?

Yes. Art. 57 LIL contains a general obligation to provide appropriate technical and organisational measures to protect personal data, which is concretised in several specific texts, in particular Délibération n° 2019-001 du 10 janvier 2019 and in the **CNIL Guide sur la sécurité des données personnelles**). Beyond these provisions, **art. 33 LIL** provides in case of prior formalities obligations, that the organism submits in its request the technical and organisational measures it intends to implement to protect personal data.

YES Germany: The requirement to have appropriate technical and organizational measures in place are part of the German data protection legislations at both, federal and state level, as well as part of several sector-specific laws.

10.3.3 Personal Data Breach Notification

(i) What requirements in relation to data breach notifications exist in your national regulation? Is this issue regulated in the national implementation of the NIS Directive?

Two kinds of notifications exist in case of personal data breach. The first one is based on **art. 58 LIL** or **art. 83 LIL**. These notifications have to be done before the CNIL. In practice, it has been noticed that the number of personal Data Breach notifications in France is lower than in other comparable European Member States, which is suspicious. (2044 in the first year of application of the GDPR in contrast to 14 072 UK notifications, 5818 in Ireland for the same period.)

The second ones are based on the NIS Directive transposition. (See **art. 7 and art. 13 of the Law n °2018-133**). In this situation, the notification has to be made before the ANSSI.

Coordination between the CNIL and the ANSSI has been foreseen.

10.3.4 Supervision of cybersecurity

(i) Does a supervisory body in a narrow sense with enforcement powers exist in your country?

(ii) Is in your country an institution like the German BSI (*Bundesamt für Sicherheit in der Informationstechnik*) established. The Federal Office for Information Security is the national cyber security authority of Germany. It shapes information security in digitisation through prevention, detection and reaction for government, business and society. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) or something similar established? If yes, what are the competences and responsibilities?

In France, the National agency for Information Systems Security (ANSSI) has been designated to fulfils the dual role of :

- defining a national security strategy

- ensuring the proper transposition of the NIS Directive, and national computer incident response teams (https://www.ssi.gouv.fr)

The ANSSI, created by decree n° 2009-834 of July 7, 2009, is the authority for the defence and security of information systems. It reports to the Secretary General of Defence and National Security (SGDSN), the authority responsible for assisting the Prime Minister in the exercise of his responsibilities in the area of defence and national security. At the end of 2017, it had 600 agents and its number should eventually reach 750 agents.

Missions: It is the national authority for information systems security. As such, it is responsible for proposing the rules to be applied for the protection of the State's information systems and for verifying the application of the measures adopted.

In the field of information systems defence, it provides a monitoring, detection, alert and reaction service to computer attacks, especially on State networks.

The ANSSI provides expertise and technical assistance to administrations and companies, with a reinforced mission for operators of vital importance (OIV). Its work with the various publics includes monitoring and reaction, development of products for civil society, information and advice, training, as well as the labelling of trusted products and service providers.

In concrete terms, it is responsible for

- propose to the Prime Minister measures to respond to crises affecting or threatening the security of information systems of public authorities and operators of vital importance;

- coordinate government action within the framework of the guidelines set by the Prime Minister in terms of information systems defence

- to propose measures for the protection of information systems;

- carry out inspections of the systems of government departments and operators of vital importance;

- participate in international negotiations and liaise with its foreign counterparts.

Finally, it acts as a response and processing centre for security incidents (CSIRT).

The ANSSI has been tasked with piloting the transposition of Directive 2016/1148 of July 6, 2018 into French law, and for this purpose has announced the existence of 122 essential service operators (ESOs) whose list will be updated annually.

(iii) How can damages caused by lack of cybersecurity be claimed (and compensated)? Are such issues sufficiently regulated in your country?

First of all, such damages can be claimed under general rules of the responsibility regime (art. 1240 et 1241 et seq. of the civil code). Secondly, **art. 37 et seq of LIL** introduce a possibility of collective action including for receiving compensation from the controller or the processor for material or non-material damages suffered. This implies a judgment on the responsibility of the controller or the processor before the civil or administrative judges and then an individual procedure for the compensation of the damage before the controller or the processor. The compensation can also be made at any time by meditation between the victims and the controller or processor. The LIL introduces this collective action both for association or not-for-profit mandated by the data subject and for some associations or not-for-profit entities independently of a data subject's mandate (Thus, French law goes beyond the situation of **art. 80§2 GDPR**).

10.4 Enforcement: fines and sanctions

(i) Is a crime related to data protection or cybersecurity punished by a fine or imprisonment?

Penalties for data protection are provided by art. **L226-16 to 226-24 of the French penal code**. Criminal offence is punishable with up € 300 000 fines and 5 years of imprisonment. Those penalties, which mainly were anterior to the GDPR, have been almost never used in France.

(ii) Are there administrative fines related to data protection issues?

Under French law there are administrative fines related to data protection issues except for State administrations. By contrast, fines can be imposed to local authorities such as municipalities and regions for instance. **Art. 20 LIL** provides the corrective measures and sanctions that the CNIL can impose. Beyond the administrative fines provided by the GDPR, **art. 20 III 2°) LIL** gives the CNIL the possibility to join a **periodic penalty** (with a maximum limit of €100,000 per day) to the administrative fines.

(iii) Do data protection offences constitute an official offence or are only prosecuted by the injured party's request

As offenses incorporated into the Penal Code, they constitute "official" offenses.

10.5 Governance

(i) At least in the biomedical sciences research involving human participants usually is subject to ethical review by research ethics committees or similar bodies. Data protection, however, not only affects the biomedical sciences, but potentially all fields of research. Are you aware of any committees (e.g. research ethics

committees, ethical review boards) or agencies (e.g. national research funding agencies, national security agencies) in your country that review data protection issues in research projects? If yes, are reviews mandatory and governed by specific guidelines or regulations? Do you know which aspects of data protection review bodies focus on? Are reviews only conducted before the actual research starts or is the research process monitored as well?

Beyond the elements given in the first section -General framework question (v)-, there is in France a National Consultative Ethics Committee for health and life sciences (hereinafter CCNE for "Comité consultatif national d'éthique pour les sciences de la vie et de la santé"). The main tasks of this CCNE are to highlight the evolution of science and technology, to raise new issues challenging society and to observe changes from the perspective of ethics. The CCNE was created in 1983. As a strictly consultative body, it can be seized by the President of the Republic, the Presidents of the Houses of Parliament, members of government, universities and other institutions of higher education, public institutions, a recognised public interest foundation working mainly in the field of research, technological development or health promotion and protection. The CCNE can also decide itself to take on questions asked by a private individual or a CCNE member. Since its creation, the CCNE has published 118 opinions. Beyond its contribution to the ongoing debate around the adoption of the new French Law on bioethics, the CCNE gave two opinions on Big Data Health (2019) and Ethics challenges regarding the Health and Digital (2018). The first opinion includes 12 recommendations articulated around three ethical principles such as:

- Ensuring the autonomy of the individual in order to give him the opportunity to choose its decisions
- Respecting individual liberty without jeopardizing solidarity and collective interests
- Ensuring the acquisition of new knowledge in the area of research for the benefit of everyone Health, without giving into potential drift

(ii) What instruments (e.g. ethics self-assessments at the proposal stage), if any, do research funding agencies and other research supporting bodies in your country use to promote data protection in ICT R&I? Do they facilitate the use of these instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

See answer given in the first section -General framework question (v)-.

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

A French Agency for innovation was created in 2018 at the Ministry of Defence. Innovation is focus in 12 areas such as autonomous vehicles; control of connected objects in particular drones, collects and processing of data, captors, man-machine interface, and telemedicine. In addition, there is currently a debate on the ethics of the IA in the sector of defence. In September 2019 a report to the Minister proposed a roadmap for the Ministry. It includes the creation of ethics and robust legal framework for the French Ministry of Armed Forces. The mentioned questions on defence technology might be addressed in the

future in a specific Ethic Committee for the application of AI in the defence area. This should also affect the private partners and the researchers involved in such AI projects.

Mainly, the ANSSI with its cyber defence centre can support the victims of industrial espionage. DFIR ORC is for instance an open-source modular framework to collect forensic artefacts on machines running a Microsoft Windows operating system created in 2011 to address operational needs of incident responders. The ANSSI also provides to the actors a list of recommended software, they might use for protection against industrial espionage and other confidentiality breaches. Finally, the ANSSI develops research projects on its own or with partners and is equipped with a Scientific Committee. It might be able to elaborate technical tools required.

11 Germany

Harald Zwingelberg (ULD)

11.1 Informed consent

11.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
General Data Protection Regulation (GDPR)	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679	EU regulation, hard law	Harmonized European data protection law
Federal Data Protection Act (Bundesdatenschutz-gesetz, BDSG)	https://www.gesetze-im-internet.de/englisch_bdsg/	hard Law	
State Data Protection Acts (Landesdatenschutz-gesetze, LDSG[83])	Overview page with links: https://dswiki.tu-ilmenau.de/liste_der_landesdatenschutzgesetze	hard Law	
Gesetz zur Regelung des Datenschutzes und des Schutzes der	https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_	hard law as of December 1st 2021	Summarizing data protection related laws currently spread in

[83] Links to the state data protection acts have been collected here including links to the central parliamentary documents motivating the law and usually containing some core considerations on each of the articles. https://dswiki.tu-ilmenau.de/liste_der_landesdatenschutzgesetze.