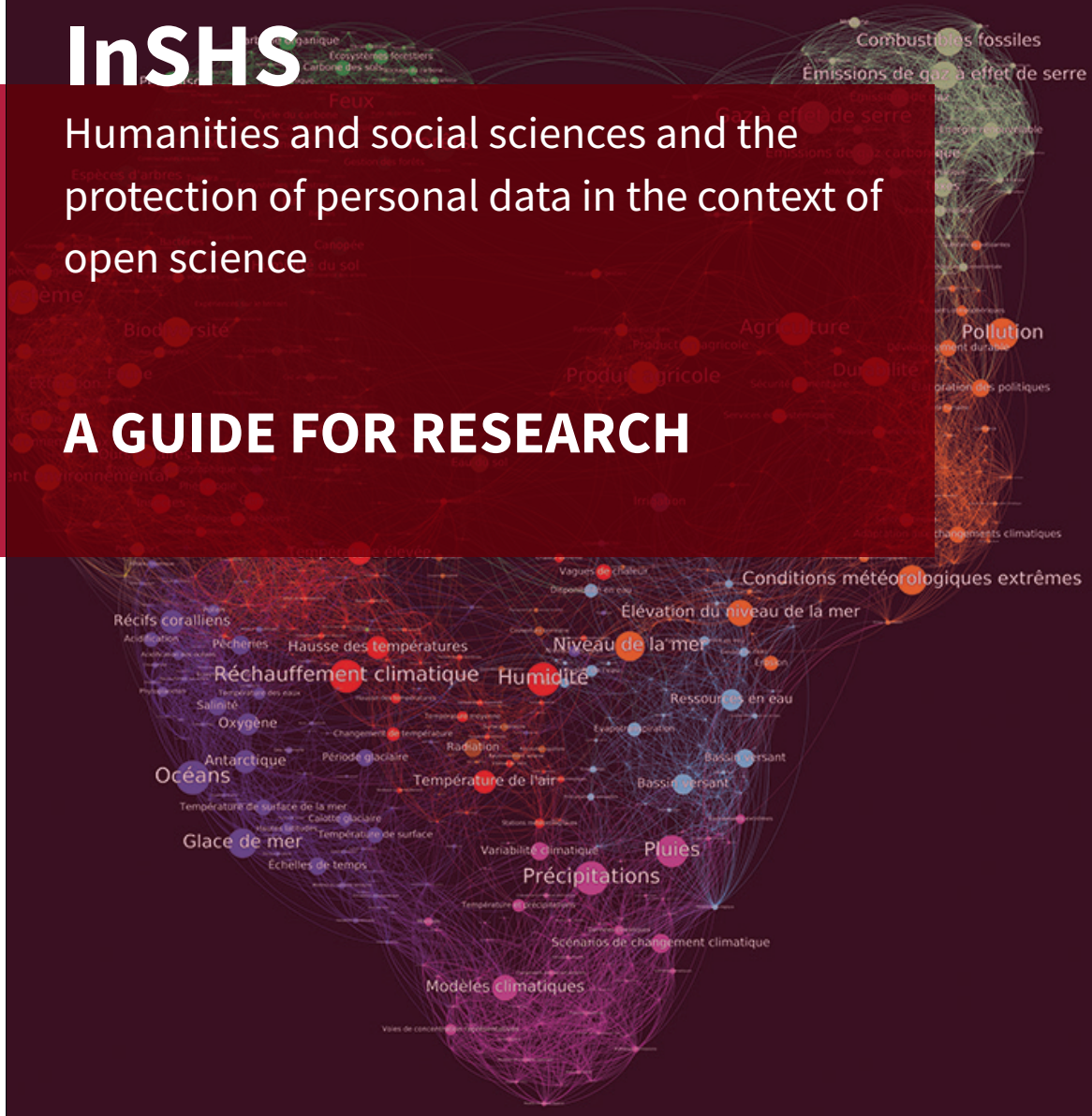
InSHS

Humanities and social sciences and the protection of personal data in the context of open science

A GUIDE FOR RESEARCH



CONTENTS

Editorial

"Information technology should be at the service of every citizen. [...] It shall not violate human identity, human rights, privacy, or individual or public liberties"

In 1978, France passed its legislation on Information Technology, Data Files and Civil Liberties, aka Data Protection Act, whose wording, taken from its first article, reflects its humanist inspiration. Forty years later, it is the same spirit that drives the General Data Protection Regulation (GDPR) that came into force on 25 May 2018.

This text makes the European Union the area in the world where personal data are most strongly protected, at a time when some excesses of the digital revolution made it necessary to return to fundamental values centred on respect for the human person.

In connection with the many issues addressed by the GDPR, scientific research has a crucial status and the European legislature used a balanced approach in this respect. While the main principles of personal data protection apply to research activities, the text also recognises their legitimacy and seeks to produce a specific regime offering researchers a specific flexibility. The GDPR thus provides for the compatibility between the protection of fundamental rights and the conduct of research activities, without antagonising one against the other.

The purpose of this Guide is to provide the research communities in the Humanities and Social Sciences with resources to appropriate this new personal data protection legal background. Written with researchers for researchers, it outlines the rules to be used at each stage of the data life cycle and identifies good practices to be implemented based on practical examples.

The humanities and social sciences use materials (statistics, surveys, interviews, archives, etc.) that frequently contain personal data requiring special precautions more than any other scientific disciplines. This is why Ms Gaëlle Bujan, the CNRS Data Protection Officer wanted to work with the INSHS first and foremost to produce this guide. We would like to thank her and all those who participated in its development.

This document shows in particular that researchers are not alone in facing the imperative of data protection. Many infrastructures like Huma-Num, Progedo, CASD (Centre d'Accès Sécurisé aux Données) or CINES (Centre Informatique National de l'Enseignement Supérieur) already provide researchers with data management solutions. These are valuable resources in which the CNRS is involved, with the conviction that sharing is a priority.

The CNRS Institute for Humanities and Social Sciences is set to support research units in this transition period because data protection and privacy are a major issue for the 21st century. The GDPR relies on a principle of accountability of those involved, and it is above all our common responsibility to build the services of the CNRS Data Protection Officer, through close collaboration between individual researchers, unit directors, research infrastructures, and all the professionals committed to this endeavour.

This guide demonstrates that acting in accordance with the GDPR is not only a matter of compliance with the legislation, although this dimension is essential. The good practices it implies in the collection, processing, storage and dissemination of data also have an epistemological dimension, their appropriation is possible in each discipline, and can contribute to the advancement of Science in itself.

François-Joseph Ruggiu Director of the InSHS of the CNRS

THIS GUIDE WAS DEVELOPED BY:

Isabelle André-Poyaud and Sandrine Astor, Pact Engineers, Social Sciences Laboratory

Olivier Baude, Director of the very large infrastructure TGIR Huma-Num

Fabrice Boudjaaba, CNRS InSHS Scientific Assistant Director Gaëlle Bujan, Data Protection Officer of the CNRS Béatrice Collignon, Director of the Passages Research Unit

Frédéric Dubois, research engineer, Laboratory of ethnology and comparative sociology

Emmanuel Kessous, interdisciplinary laboratory, sciences, innovations, companies Lionel Maurel, CNRS InSHS Scientific Assistant Director

Muriel Roger, University Professor, Centre d'Economie de la Sorbonne

June 2019.

INTRODUCTION

The European Regulation on the protection of personal data, which came into force in May 2018, raises questions among the scientific community, particularly in the humanities and social sciences, about the compatibility of research work with this regulation.

It is very protective and provides every person free control over his or her personal data, under certain conditions. This is a fundamental right, the laws, statutes and regulations apply to everyone (see Article 8 of Chapter II "Freedoms" of the Charter of Fundamental Rights of the European Union).

Failure to comply with the laws and regulations on the protection of personal data is a criminal offence.

The scientific community in the humanities and social sciences only uses personal data for research purposes. Those who made this regulation have understood this and it takes into account the specificities of scientific activity, i.e. possible reuse of data for research purposes, processing of sensitive data (e.g. health data, data on trade union membership, ethnic origins) for research purposes by taking appropriate precautions, possible derogations under certain conditions from the obligation to inform individuals, etc. (See Article 89 of the GDPR).

The objective of this guide is to help humanities and social sciences researchers understand the legal mechanisms that impact their research and to provide them with the right habits and tools when they are led to process personal data.

It aims to be a tool to support legitimate questions during the construction, implementation of a research program, the publication of results and the potential reuse of data.

The various topics covered in this guide refer to the General Data Protection Regulation, its application to research in the humanities and social sciences and provide examples from situations encountered in laboratories.

The information and examples in this guide focus on research data.

The Guide is not intended to address issues of personal data protection and privacy related to the operation or administration of research in laboratories. For these types of data, the texts fall under European and French laws and regulations without there being any specific derogations for higher education and research.

As far as possible, this guide will be updated at least once a year by a committee of experts similar to the one that developed this initial version.

BACKGROUND INFORMATION

In today's digital environment, the broad possibilities for the dissemination of information and data, including personal data, the daily use of social networks, and the vanishing boundaries between the public and private spheres make it crucial for the scientific community to maintain the trust of the individual citizens in the research activities and programmes being launched. Importantly, the quality of research and adhered-to research ethics combine to shape the simple principles that are part of the advancement of knowledge

The Research Environment

Digital technology opens up new opportunities, access to mass and potentially reusable data, new techniques for storing, hosting and transferring information, which are all crucial resources for research whose reliability must be preserved.

Increasingly, progress in knowledge, scientific advances and innovation are partly based on data use/reuse and sharing. Open science, i.e. the unhindered dissemination of research publications and data, is now a "new paradigm" in which every researcher should work (Speech delivered by Frédérique Vidal, Minister of Higher Education, Research and Innovation, on 4 July 2018 to launch the French National Open Science Plan).

Open science relies on the opportunities to develop access to all publications and research data through digital technologies and it contributes to research efficiency, opens up opportunities to be part of international competition, and fosters citizens' trust through transparent research. This development impacts all scientific disciplines. The National Open Science Plan is in line with France's international commitments to transparent public action. It also meets the EU's Amsterdam Call for Action on Open Science to make research results accessible, without delay and without payment, to citizens, companies and research stakeholders.

The plan, with a budget of €5.4 million, is divided into three areas:

- Generalising access to open science: automatically publish in open access for any project financed by public funds; simplify the deposit of publications by researchers;
- Structuring and opening up research data: develop the open dissemination of publicly funded research data output; create the conditions and promote the openness of research data;
- Engaging in a sustainable European and international dynamic: develop skills in open science; encourage research operating organisations to adopt an open science policy; contribute to European structuring within the European Open Science Cloud.

The increasing development of regulations and statutes in all areas of civil life also affects scientific work. Thus, in the fields of personal data protection, many other legislations apply to the processing of data: the law on digital trust, the public health code, the law on research on persons (aka *Jardé law*), as amended, and its implementing decrees, the heritage code, the intellectual property code, etc.

The principles of Research

Research quality, ethics and scientific integrity result from the practices and behaviours that contribute to civil trust and that of research stakeholders.

These principles must be complied with for all research, including that involving personal data.

Identifying the data adapted to the project, their relevance, volume, updating, stability over time, transparency as to how they are constructed are all part of science work reliability, and of the reproducibility of the results.

For any project, it is important to collect, use and analyse the data in connection with the research scope. An objective approach, respect for the data collected and shared research results are in line with the principles of ethics and scientific integrity which are to be followed.

Each higher education and research institution and many research funding institutions require these practices to be observed and make sure that they are complied with.

→ The CNRS has set up an ethics committee and has entered into discussions on general ethical issues raised by the practice of research and related to the social and moral consequences of knowledge advances, the principles

that should drive individual behaviour, and the making of science.

→ In June 2014, the ANR adopted a policy on ethics and scientific integrity that sets out the fundamental principles to be complied with by all research stakeholders and the rights and duties of those who evaluate and support scientific activity. Since 2019, the ANR has required the implementation of a Data Management Plan (DMP) for all funded projects (see page 9 of the ANR action plan).

→ The European Union in its H2020 programme requires research data management to be implemented. Research data must be "searchable, accessible, interoperable and reusable" (aka FAIR principles). Partners in EU-funded projects must build a data management plan.

CHAPTER 1:

THE MAIN DEFINITIONS AND THEIR APPLICATION TO RESEARCH IN THE HUMANITIES AND SOCIAL SCIENCES

In this first part, the main concepts will be described and illustrated as much as much possible with examples in the different disciplines of the humanities and social sciences.

Personal data are involved daily in humanities and social sciences research projects, and protecting the information about people involved in scientific projects has to be a prominent concern.

1.1. PERSONAL DATA

Personal data means any information that makes it possible to identify a person directly or indirectly (Article 4 of the GDPR):

- Directly identifying data: surname, forename, address, photo, voice, etc.
- Indirectly identifying data: a telephone number, or cross-referencing information such as the son of the research director, who lives on the island of Batz, etc.

Example: A research project is to develop a business travel plan in which the surnames and forenames of individuals are not collected (this information is not necessary) while data on the movements of individuals, their employers, their socio-professional categories and their place of residence allow the specific identification of these natural persons. This information is therefore personal data.

Note

- Irreversibly anonymised data, whereby a person can no longer be re-identified, are not subject to the laws and regulations on the protection of personal data.

- Pseudonymised data are personal data that can no longer be directly attributed to the data subject. However, the use of additional information, such as a correspondence table, can be used to re-identify the person. In this case, the General Data Protection Regulation shall apply.

Among personal data, several are **"sensitive" data** under the Regulation: data disclosing alleged racial or ethnic origin, political opinions, philosophical or religious beliefs, trade union membership, sexual orientation, health data, biometric data allowing a person to be identified, genetic data.

Processing of such sensitive data is prohibited (Article 9 of the GDPR) unless explicitly listed in the Regulation (for example, with the consent of the person concerned, data manifestly made public by the data subject, substantial public interest, safety of human life). The use of this sensitive data is possible for public research purposes and during the preparation of the project, it is necessary to seek the prior opinion of the CNIL in certain cases, and to organise the securement of the data.

Other data are subject to specific requirements:

- The French social security number (aka NIR) is a directly identifying piece of data and its use is strictly regulated by law. This data may be used if the processing has an exclusively scientific purpose and provided that it has been encrypted prior to data processing.
- Data on offences or convictions can only be processed by the courts and a number of bodies specifically listed in the law. However, as part of an agreement with the Ministry of Justice, public research institutions and associated

laboratories may sometimes be required, under certain strictly controlled conditions, to process these data, and in particular if, and only if, the purpose or result of the processing is not to re-identify a person

1.2. STAKEHOLDERS AND ROLES

The EU regulation on the protection of personal data changed the concept of accountability for data processing.

First, the obligations of stakeholders, such as subcontractors, have been extended. Second, the controller must implement appropriate technical and organisational actions to ensure that the processing operation complies with the regulation.

For research projects, several parties are involved in achieving compliance.

- **Researchers** who conduct and lead any research project, whether funded or not, involving several partners or not, shall take the necessary steps to make sure that the project/processing complies with the regulation.

- **Doctoral students** shall carry out the required steps as an integral part of their research project. For a CNRS joint research unit under the authority of CNRS InSHS, the unit director shall be the controller accountable for the processing of data related to a project. Doctoral students shall carry out the steps for compliance with the regulation under the supervision of their thesis director.
- **The controller** is the person, public authority or body that determines the purpose and means of the processing operation. (Article 4 of the GDPR)

At the CNRS

For joint research units, the unit director is responsible for processing (controller). He/she must therefore make sure that the RGPD is complied with and appoint a Data Protection Officer. To this end, he/she relies on the scientific managers of the projects operated in the unit.

In most cases, when the unit director is a CNRS member of staff, he/she appoints the CNRS Data Protection Officer.

Each controller is required to document the processing of personal data and maintain up-to-date **records of processing operations**, keeping track in particular of:

- The purposes of the processing operation
- The categories of data subjects and related data
- The recipients of the data
- Information on the use of data, their storage and the rights of the data subjects
- The names and contact details of the controller and the Data Protection Officer

At the CNRS

The records of each controller (i.e. each unit) are maintained by the Data Protection Officer (DPO) on behalf of the controllers.

Formally, this task is carried out by the project's scientific manager on behalf of the DPO, who in turn provides counselling, and monitors and validates the registration of the data processing.

At their request and at least once a year, the DPO shall forward to the unit directors their unit's updated list of processing operations.

The procedures for registering processing operations were previously carried out and filed with the CNIL or the "Correspondents Informatique et Liberté". These are now to be carried out as a whole with the Unit's Data Protection Officer.

Remember, however, that the prior opinion of the CNIL is required before any processing operation that could create exceedingly significant risks for the data subjects, as highlighted by a privacy impact assessment (see page 16) and that the researcher cannot reduce without impacting his or her research.

Authorisation from the CNIL may also be required for health research (see the CNIL website and page 21).)

In any case, it is advisable to contact the Data Protection Officer for a joint referral to the CNIL.

→**The processor** is "a natural or legal person, public authority, agency [or other body] which processes personal data on behalf of [on instructions from and under the authority of a] the controller " (Article 4 of the GDPR). The processor must provide appropriate safeguards to protect the security and confidentiality of the data, specified in particular in the binding contract between the controller and the processor. This contract shall also specify their respective commitments for data processing.

Examples of subcontractors:

Huma-Num TGIR data hosting service
A polling company when contracting a survey to such a firm. The processor is in charge of collecting the information from the data subjects, the researcher takes and uses the information thus obtained. In some cases the data may be pseudonymised by the processor.

→ The Data Protection Officer

Each public institution must have a Data Protection Officer to advise and make controllers aware of their obligations for the application of personal data protection regulations and rules (see Articles 37 to 38 of the GDPR). The Data Protection Officer advises on compliance with the regulations, cooperates with the supervisory authority, and ensures compliance with the regulation on the protection of natural persons.

Each unit director must appoint a Data Protection Officer. The appointed Data Protection Officer should be designated to the CNIL.

CNRS special note:

For unit directors who choose the DPO of the CNRS, the procedure is as follows: the unit director informs the DPO of his choice. The DPO contacts the CNIL for formalisation and designation.

In all cases, a registration receipt is sent by the CNIL to the unit director with a copy to the designated DPO. This document must be kept by the unit and is integrated into the unit's corpus of documents relating to the protection of personal data.

→ **The Commission nationale Informatique et Libertés (CNIL)** is the supervisory and advisory authority in France responsible for monitoring, informing and supporting the application of the European regulation and French regulations on the protection of personal data (see article 51 of the GDPR) and chapter 2 of the ordinance 2018-1125 of 12 December 2018 on the protection of personal data (amending the Data Protection Act of 6 January 1978).

1.3. THE TERRITORIAL SCOPE OF THE REGULATION

The European Regulation applies to data processing operations in the context of activities carried out by an establishment located on EU territories.
It also applies to processing operations carried out by a controller or processor established outside the European Union but involving individuals who are located in the territory of the European Union (see Article 3 of the GDPR).

Example: French researchers carried out a study on the genetic and linguistic diversity of the Cape Verdean population. European legislation is intended to apply because the controller is located on European territory, regardless of whether the data collection takes place in Cape Verde.

The protection of personal data is carried out in different ways in different countries. Outside the European Union, several countries adopted legislations recognised by the European Commission as providing an adequate level of protection under the GDPR; in other countries, there is no protection. The CNIL keeps up-to-date records on the state of legislation in each country: the protection of personal data worldwide.
The transfer of data outside the European Union is possible provided that a sufficient and appropriate level of protection is provided. These transfers must be supervised using different legal mechanisms (see CNIL website).

It is advisable to contact the unit's **Data Protection Officer**.

For an international research laboratory (UMI or UMIFRE) whose partners apply different laws and regulations, the applicable law must be subject to a thorough analysis.
A clause on the protection of personal data must be included in the relevant international cooperation contract. It is advisable to contact the Unit's Data Protection Officer.

1.4. DATA PROCESSING

A data processing operation is any operation involving personal data, whatever the process, the medium used, regardless of whether it is computerised. The data are used to meet objectives/purposes. The processing of data in the sense of "protection of personal data" goes beyond the analysis or exploitation of the data, it also covers the collection, analysis, reuse of data, archiving, etc. (Article 4 of the GDPR).

Example:

Data hosting by Huma-Num and archiving by CINES are personal data processing operations.

The purpose of the processing is one of the essential principles of the Regulation. All data processing is carried out for a specific, explicit and legitimate purpose. The data may not be processed in a way that is incompatible with the defined purpose.

However, the data may subsequently be used for research purposes by providing safeguards to protect the privacy of the data subjects by the data collected (see Article 5 of the GDPR and Article 89 of the GDPR).

For social science research, the research scope is often the purpose of data processing.
Example: A sociolinguistic study of the variation of the language used on Twitter is the purpose for collected data that are the personal details, economic data, and geolocation.

1.5. PRINCIPLES UNDERLYING DATA PROCESSING

Before starting one's research project and when it contains personal data, the person in charge of the scientific project shall undertake the analysis addressing:

- The lawfulness of the processing, which is the basis of the processing (a)
- The purpose of the processing operation (b)
- The relevance and proportionality of data (c))
- Data security and protection (d)
- Limited data storage (e)
- Transparency of information about the use of data (f)

In addition to the basis of the processing, it is necessary to ensure compliance with the principles of personal data protection in conducting the research.

(a) The leader of the project or the controller verifies whether the project is lawful, i.e. whether it complies with one of the following conditions: (Article 6 of the GDPR)

(a) The person has consented to the processing of his or her data
(b) The processing relies on a legal basis
(c) The processing is linked to the execution of a contract
(d) The processing is necessary to safeguard the vital interests of the data subject
(e) The processing is necessary for the performance of a task to be carried out in the public interest
(f) The processing is in accordance with a legitimate interest for the controller

In the humanities and social sciences, the basis most often involves consent, a task of public interest or a legitimate interest.

Examples:
(g) *Field surveys in metropolitan France are often carried out on the basis of a consent given to the investigator.*
(h) *Sociological research with the collection of messages exchanged on Twitter can be based on a task of public interest.*

(b) The purpose of the processing corresponds to the objective pursued.
The purpose must match the missions of the institution or entity.

Example:
Study on the evolution of territorial inequalities over the past 30 years in urban areas and the emergence of "urban traps" with the use of personal geolocation data using INSEE databases.

(c) Relevance and proportionality of data
Data must be commensurate with purpose.

Example: In a research project on people's leisure activities, it may be relevant to collect a number of complementary data such as religion. This may have an impact on the choice of leisure activities based on the days of practice of these leisure activities. The collection of this information is appropriate because it has an impact on research results.

(d) Data security and protection
The controller is required to take all measures to protect the data and prevent them from being diverted, reused for purposes not intended, to safeguard the integrity and confidentiality of the data. Security mechanisms should be provided at all stages of the project, regardless of the nature of the data (see page 24).

(e) Limited data storage

The data may only be stored for a predefined and limited period. The length of the period of storage should be commensurate to the purpose of the processing. At the end of the processing operation, the data shall be either anonymised or stored for subsequent reuse for scientific research purposes only.
For research purposes, data can be archived according to specific provisions presented in Chapter 2, page 26.

(f) Transparency of data processing

Information relating to the purpose of the processing operation, the name and contact details of the controller, the name and contact details of the Data Protection Officer and the storage periods shall be communicated in a transparent manner to the data subjects by the data controller.

See examples of information references on the CNIL website
See Appendix 2 for a sample information note developed by the Pacte joint research unit

1.6. PRIVACY IMPACT ASSESSMENT

Its aim is to anticipate the risks of processing data for the privacy of the data subjects. This analysis is carried out by the controller (and by delegation, the scientific manager of the project) in conjunction with the Data Protection Officer and the Information Systems Security Officer.

It is mandatory where the processing is likely to generate high risks and in particular must be carried out if the processing includes at least two of the following criteria:

- Automated monitoring,
- Sensitive data,
- Large-scale processing,
- Data cross-referencing,
- Vulnerable persons (patients, elderly, children, etc.),
- Evaluation/scoring (including profiling),
- Automated decision making with a legal outcome,
- Innovative use or NICT use,
- Exclusion from a right or a contract.

The CNIL has published the list of processing operations for which a data protection impact assessment (DPIA) is mandatory. This list is not exhaustive.

1.7. THE RIGHTS OF INDIVIDUALS

The GDPR has extended the rights of individuals.

→ **Precise information on the processing, purpose, use of the data, storage period must be provided to the data subjects. This information must be transparent and easily accessible** (Article 12 of the GDPR). It must be transmitted directly to the data subjects. Where the provision of such information is impossible or would require disproportionate effort, or where such information would be likely to render impossible the purposes of the processing or seriously impair their achievement, it is possible, by way of derogation, not to do so with the data subjects but to take appropriate measures to protect the rights and freedom of individuals, including by making the information publicly available (Article 14.5 of the GDPR).

→ **Right of access to one's data** (see Article 15)

→ **Right to be informed of a data breach when there is a significant risk for the data subjects.**

→ **Right to objection** (see Article 21): a person may object, on legitimate grounds, to the use of his or her personal data unless the processing complies with a legal obligation. A derogation makes it possible to reject such a request where the processing is based on the performance of a task of public interest.

→ **Right of rectification** (see Article 16): a person may ask to modify his/her data.

→ **Right to erasure** (see Article 17): a person may request access to his/her data and request erasure. The request may not be granted, if exercising this right is likely to make impossible or seriously impair the achievement of the processing objectives

→ **Right to portability** (see Article 20): a person may ask to receive his/her data in a structured and machine-readable format and to transmit them to another controller. This right shall not apply to processing necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller.

→ **Right to a restricted use of one's data** (see Article 23)

Today, any individual can easily exercise his or her rights as soon as he or she knows the names and contact details of the controller and the Data Protection Officer, which are mandatory information that should be given to data subjects. The regulations provide for response times: as from the receipt of a request for access to the data, the data must be transmitted within one month.

At the CNRS, the exercise of rights is handled by the Data Protection Officer (DPO) and the controller.

Case 1: When a request is made to the controller or the scientific manager
The request should be forwarded to the DPO who advises him/her. A reply is sent to the person and a copy forwarded to the DPO

Case 2: Request to the DPO
The controller or scientific leader is asked to draft the reply and send it with a copy forwarded to the DPO.

The request for the exercise of rights and the copy of the reply shall be entered in the records of the controller kept by the DPO.

One of the main changes in the GDPR covers the obligation for the controller (and the processor) to set out and organise measures to demonstrate compliance with the regulations at any time.

This accountability of stakeholders requires a thorough analysis of the data and their processing. During the development and implementation of research projects, this analysis is central and even imposed by the funders.

CHAPTER 2

RESEARCH PROJECTS, DATA LIFE CYCLE AND THE PROTECTION OF PERSONAL DATA

This second part focuses on a tangible description of data analysis methods, the issues related to personal data protection legislation that may arise all along the path of data life during research projects, from data collection to dissemination, or potential reuse.

In the interest of compliance with the principles of ethical research, the reliability and quality of research and data require a structured approach prior to the establishment of any research project. This guides you through an early reflection about all stages of the project and helps you make appropriate decisions at the right time, thus facilitating the implementation of the project: for example, identification of the security measures to be taken, request for pre-project authorisations (filming, use of health data, sensitive data in certain cases, etc.), anticipation of final data storage issues at the end of the project and reflection on their availability at the end of the project.

Further reading: Huma-Num document on the main stages of a research project in the digital age.

All projects now require prior reflection on research data. The aim is to identify data and describe the collection, storage and archiving methods, and thus to consider a data management plan.

Project grant applications are also facilitated or even automatically imply a prior clarification about the nature of the data the project is to use and the means. Therefore, a scientific project must formalise and explain all stages of data exploitation and processing. This is why research funding practices are gradually changing and funders increasingly tend to require **DMPs**.

Since 2007 and 2019 respectively, in an effort to achieve quality and open access to research, the European Union and the ANR have required a DMP to be drafted for every project funding application.

DMPs: What is a DMP? Why a DMP?

A DMP is a structured document explaining how data are obtained and processed throughout their life cycle, from collection stage to archiving.
It must indicate:

- how research data are handled before, during and after the end of the project,
- the data that will be collected, processed and/or generated,
- whether the data are shared, made accessible, and how they will be organised and stored (including after the end of a project).

A DMP:

- Ensures the quality of research
- Contributes to making data "findable, accessible, identifiable, reproducible", or FAIR (for H2020 projects)

- In our digital age, is a tool for reliability and knowledge for a potential reuse of Open Access data
- Meets the requirements of research funders like the European Union, ANR, etc. The associated costs are entitled to be included in project eligible expenses.

The elements relating to the protection of personal data are only a part of the information to be included in a DMP, even if compliance with the Regulation is to be observed during all stages of a DMP.

.

Several institutions provide approaches and templates to create data management plans:

DMP templates can be found at the Inist: see OPIDOR website.

The University of Paris Diderot makes a methodology available for the production of DMPs.

USR PROGEDO and its network of university data platforms (PUD) provides national support for the implementation of DMPs.

INRA makes a guide to DMPs available.

2.1. CREATING DATA (DATA COLLECTION)

2. 1. 1. Data categories

The regulation makes a distinction between the method used for collecting personal data and the method of producing research data in the humanities and social sciences.

Reminder: the GDPR makes a distinction between:

Data collected directly from the data subjects. These individuals must be informed precisely about the data collected, their use, the purpose of their processing, their storage period, and the procedures for exercising the relevant rights, the names of the controller and the Data Protection Officer.

Data indirectly collected are also subject to information on data processing as above. For this type of collection, it is also necessary to inform the data subjects about the categories of data collected and the source of the data (stating in particular whether they come from publicly available sources).
See **Articles 13 and 14** of the GDPR

A - Data generated for research purposes directly by the researcher

Example:

Data from a sociological survey, an ethnological survey, a field survey, oral archives, questionnaires, forms, interviews, and data extracted from the web, etc.

If you contract to a service provider, a contract should set out the obligations and commitments of each party. The controller must communicate all information on the processing of data to the processor and comply with the principles of the data protection regulations. The obligations of each party shall be governed by a contract (Article 28 of the GDPR).

Note

The processor has crucial responsibilities for the protection of personal data. Thus, the processor must:

- Take into account the security, confidentiality and documentation aspects of the activities carried out on behalf of the controller
- Assist the controller in the implementation of his obligations (privacy impact assessment, data breach notification, security)
- Maintain a register of processing operations carried out on behalf of the data controllers
- Appoint a DPO under the same conditions as a controller.

In research projects involving contracted personal data processing, it is recommended to refer to the Partnership and Technology Transfer ("Partenariats et Valorisation") and/or Financial ("Département financier")/Purchase department ("Département Achats") of the supervisory authority institution that manages the project expenses in order to adapt the contract to the necessary protection of personal data.

Similarly, when the laboratory processes data as part of its services, it is recommended to contact the Partnership and Technology Transfer Department of the contract managing authority.

For surveys conducted by **one or more students**: provide a confidentiality commitment and ensure the security of the information systems used. Students will comply with the terms of the processing operation registered with the DPO of the unit in which the research is being carried out.

B - Data initially produced for non-research purposes and subsequently used for research purposes

Example:

Data from official statistics, surveys of polling agencies, government bodies, data from administrative files

In the case of data not directly collected from the data subjects but from a third party, which has collected the data lawfully, the GDPR provides that the pursuit of a research purpose is compatible with the original purpose of data collection. In this case, the regulations on the protection of personal data apply to the new processing operation.

In the case of data from official statistics, researchers can access different data files containing detailed and individual information on individuals or enterprises (household composition or income, business profits, location, etc.). There may be three types of files available, which may even come from the same resource. They differ in their accuracy and the risks involved in identifying individuals or companies. A distinction has to be made between:

- Confidential files giving specific information about the respondents that could be used to identify them. Access to this data is possible for researchers in a secure environment, on a project basis, after approval by the Committee on Statistical Secrecy. This is possible - against a fee - via the Secure Data Access Centre (https://www.casd.eu/en/ - CASD)
- Production and Research files. These files are pseudonymised. The data made available to researchers are not directly personal but are considered to be indirectly identifiable (see definition on page 8). These files are produced specifically for research purposes. They are accessible to the scientific community via Quetelet Progedo Diffusion (http://quetelet.progedo.fr/)
- Standard files for which all the necessary processing has been carried out in order to make them anonymous (example: merging of professions and socio-professional categories with geographical areas of residence for households). They are accessible as open data.

2. 1. 2. Types of personal data

Depending on their level of sensitivity, personal data may be subject to specific provisions in order to protect privacy. For processing for research purposes, the data may:

1. have no specific level of sensitivity;
2. involve so-called sensitive information (see page 11).

The processing of sensitive data is generally prohibited unless provided for by legislation: e.g. express consent or for research purposes. In this case, compliance with the regulations is of special importance (see page 11).

Example:

Comparative study of the eating habits of high school students residing in France, the United States, Senegal and Brazil with a follow-up of children aged 15 to 16 for 3 years comprising data on gender, socio-professional category of parents, religious beliefs, etc.

3. target vulnerable groups of individuals: minors, elderly individuals, employees being subjects of surveys, prisoners, asylum seekers. There is no definition provided for the concept of a vulnerable population in the legislation. However, specific provisions must be complied with: e.g. obtain the individuals' consent and guarantee the security and confidentiality of information. For research involving minors, the information must be adapted and it is recommended to also inform parents accurately (or the person having parental authority).

Example:

A study aimed at specifying changes in the interactions between patients and caregivers interactions, these interactions can cause new social vulnerable situations or, on the contrary, contribute to the reduction of social inequalities in health.

4. cover research in the field of health

Health data are broadly defined as data relating to past, present or future physical or emotional health that gives an indication of the person's health status.

Example:

Monitoring the daily lives of men under 30 with autism with a collection of data on the condition and its course, and on the persons and their living habits

Required steps for research involving health data:

→ **Situation 1:** The research involves health data (pregnancy, disability, chronic disease, etc.) but is not health research: the procedure is identical to that involving so-called sensitive data (see page 11).

→ **Situation 2:** Health research involving human subjects:

- Request an opinion from a Committee for the Protection of Persons (Comité de protection des personnes physiques - CPP)

If the processing is compliant with a baseline methodology (Méthodologie de référence - MR) required by the CNIL: The controller should carry out a privacy impact assessment and signs a commitment to comply with the MR with the CNIL.

This compliance commitment shall be registered in the records. The processing operations carried out under the baseline methodology should be listed in the records by the controller

- MR-001: involving human subjects for interventional research. MR-001 requires the express and informed consent of the patient or his or her legal representatives.
- MR-003: involving human subjects for non-interventional research. This methodology does not imply patient consent, but informing the patient is mandatory.

If the prior approval of the CNIL is required, a privacy impact assessment must also be carried out:

→ **Situation 3:** Research in the field of health not involving human subjects

- The processing complies with MR-004: a research not involving human subjects connected to studies, evaluations in the field of health (**a privacy impact study is to be carried out and a compliance commitment filed at the CNIL.** This compliance commitment should be saved in the records, and the processing operations carried out under the baseline methodology should be listed in the records by the controller.) The processing is also included in the public register made available by the National Institute of Health Data (Institut national des Données de Santé - INDS); or,

- The processing does not comply with the baseline methodology and it is necessary to request an opinion from CEREES via the INDS (the national institute for health data), a privacy impact study should be carried out and then an approval application should be submitted to the CNIL.

In all cases, it is advisable to conduct the privacy impact study and all steps in conjunction with the Unit's DPO.
In all cases, the processing operation will be registered in the processing records and documented with the privacy impact assessment, the compliance commitment and/or approval by the CNIL and any other relevant documents.

5. Particular attention, including a data protection impact assessment, must be given to research involving data relating to criminal convictions and offences or related security measures.

2.1.3. The legitimate basis of the processing associated with data collection

As stated in Chapter 1, the regulation provides six bases, three of which are often used in research: consent, public interest, and legitimate interest.

In the context of research activities, processing should preferably be carried out on the basis of consent (compliance with the principle of informational self-determination), but may also be grounded on the performance of a task carried out in the public interest.

The choice always rests with the controller who analyses the nature of the data, the data subject population involved. This option's arguments should be detailed and the DPO should provide advice to determine the grounds for processing.

FOCUS on consent

Written or oral Consent may be given in different forms. In all cases, it is important to ensure the traceability of the collection of consent. It must include the information necessary for consent to be free, specific, informed and unambiguous.

You are advised to visit the CNIL website, on how to obtain the consent of individuals:
https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes

Once given, one should be able to withdraw their consent as simply as when giving it. In the case of such an occurrence, the associated data can no longer be processed in the project.

The controller is required to keep proof that consent has been given to him/her to carry out a processing operation.

See Appendix 1: Sample consent form by the Pacte joint research unit.

2. 1. 4. Purpose

Article 5 of the GDPR sets out that personal data may only be collected for a "specified, explicit and legitimate purpose" which in principle should be identified prior to processing and brought to the attention of the data subjects.

However, Recital 33 of the GDPR also accepts a degree of uncertainty of purposes for processing carried out for research:

> *"It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose." (Recital 33 GDPR).*

Even when the purpose is not fully determined, the processing of personal data is possible. The information provided to individuals must be adapted to the purposes known at the beginning of the research.

2. 1. 5. Proportional data

The question is whether the data collected are relevant and necessary for the processing operation.

Example:

A research project requires to collect the age of individuals, but this does not mean recording the day and month of birth. For the residence, is it necessary to collect the full address or only the city? For the occupational activity, is it necessary to know only the occupational category or the fact that the person works in a particular profession, in a particular company, etc.?

Similarly, personal data might be collected unintentionally.
For example, such data may result from an interview while not being related to a data processing purpose.

In this case, the researcher must decide whether the data should be saved for his initial investigation or erased, or reused subsequently (the same applies to so-called sensitive data).

2.2 DATA STORAGE

Preserving the security of data access, storage and hosting is crucial to protect personal data. The controller should use the tools provided by his supervisory institutions to comply with and/or enforce compliance with the institution's internal policies.

The basic rules (non-exhaustive list) for securing information systems, the use of digital tools, data exchanges and data storage are in line with the information systems security policy of the unit's and researchers' supervising institutions:

- Authentication should be provided for users of digital tools: digital certificates, passwords;
- Authorisation management: restricted access to sites and data should be granted only to persons approved by the controller or research project manager;
- Security of tools: computers and smartphones should be encrypted;
- Internal computer networks should be protected;
- Exchanges between organisations, units and researchers should be protected by a secured system;
- Secure tools should be used for videoconferences (at CNRS: use of Skype Enterprise).

Accessible tools
The CNRS digital services
CNIL publication: security of personal data, 2018 edition

FOCUS: Examples of bad practices:

Use of unsecured email messaging for information exchange
Private and professional email interactions
Use on-line survey tools hosted abroad (such as Google Forms). Save files on one's personal workstations when they are only accessible on secure workstations
Exchange files containing so-called sensitive personal data by email without message encryption

FOCUS: Retrieval advice by government authorities under the digital security programme:

Manage your passwords
Security of mobile devices
Separate professional and private use

(source: GIP Action contre la Cybermalveillance (public interest group on cyber-threat control))

Several entities offer solutions for data storage. Whatever the medium, it is important to anticipate the volume of data, the duration of storage and to estimate its cost (this can sometimes be taken into account in the eligible expenses of research project applications).

See Huma-Num services

2. 3. DATA PROCESSING

In this section, data processing is to be understood as the stage of data analysis, consolidation and work on data that helps to provide insight on the issue investigated.

The data may match different statuses.

1 – identifying data used on a small number of people and needed for qualitative analyses (common in ethnology, social or cultural geography, sociology).
It is important to remove the identifying character at the publication stage and/or at the end of the research project. Depending on the situation, anonymisation or pseudonymisation is required.

2 – anonymised data

This irreversibly removes the link with personal data.
If the identification of a person is not possible in any way, the GPDR does not apply. In qualitative surveys, anonymisation will generally not be possible, as there is a proven need to identify individuals.
When the research objectives requires the identity of the interviewees (personality, expert, etc.) to be cited, they should be informed that identifying data will be published and that they will be guaranteed access to the interview transcript.

For quantitative studies, anonymisation should be carried out further to the principle of proportionality, from the very moment of data collection.

3 –Pseudonymising data consists in separating directly identifying data (e.g. surname and forename) from other non-identifying data (for example, by assigning numbers to persons thus avoiding disclosing their surname, but by keeping a correspondence table to trace the identity of the person).

FOCUS on anonymisation
The anonymisation of data requires that the identification of persons becomes impossible, either directly or indirectly, an operation that follows a specific process.
Whatever the technique used, anonymisation must lead to compliance with three criteria:
- Total inability to single out an individual
- Total inability to link records relating to two individuals together
- Impossibility to deduce information about an individual
-

Examples of anonymisation techniques (Article 29 DPWP opinion):

- *Adding noise: altering the accuracy of the information by adding randomness*
- *Switching: Mixing attribute values within the dataset*
- *Generalisation: Change the granularity of the values to form groups*
  - *k-anonymity: at least k people have the same profile*
  - *L-diversity: at least l values have the same attribute*

Big Data and Artificial Intelligence

The use of innovative data processing technologies such as Big Data or Artificial Intelligence (AI), requires special care, given the characteristics of these technologies.

Because it involves the processing - and often the cross-referencing - of large amounts of data, Big Data carries a higher risk of indirect identification of individuals, even when it is based on initially anonymous data.

The creation of a database from several sources requires special precautions. It must be ensured that the consent of the data subjects has been obtained or - in cases where processing is carried out on another basis - that the right to information of the data subject is respected.

The implementation of technologies such as Big Data or Artificial Intelligence will often require a privacy impact assessment (PIA. See page 16). An impact study is necessary when faced with several criteria, including character profiling, data cross-referencing, automatic decisions or use of cutting-edge technologies.

With regard to Artificial Intelligence and Machine Learning, it should be remembered that profiling operations (in the sense of processing personal data for the purpose of analysing and predicting behaviour), as well as fully automated decisions that may result from them, are subject to special supervision under the GDPR.

In particular, persons may assert rights to transparency and the intervention of a human person, when such decisions have legal effect.

2.4. DATA ARCHIVING

In principle, the processing of personal data must have a fixed period of time, in relation to the fulfilment of the purpose for which they were collected. The GDPR states that this data storage period is set at the "strict minimum", at the end of which normally the data must be archived in accordance with the regulations on public archives.
Nevertheless, the GDPR also sets out that data may be kept for longer periods of time when they are processed "for archiving purposes in the public interest, for scientific or historical research, or statistical purposes" (see Article 5 of the GDPR and information on the CNIL website).
Data storage according to the regulations on archive provides for a three-stage cycle.

Phase 1: storage in the active database
It corresponds to the current use of data, i.e. the timespan of the research project.

Phase 2: Intermediate archiving
Under certain conditions, personal data may be stored after the data have been processed but with restricted access. Personal data for research purposes are often archived in a so-called intermediate format, provided that the rights of individuals and the associated information are maintained.

At the CNRS, the intermediate archiving period is often two years after the last publication of the research results.

Phase 3: final archiving
Personal data that is not destroyed may be archived in accordance with the provisions of Book 2 of the Heritage Code (Code du Patrimoine). Final archiving cannot be carried out in the laboratory. It is carried out with the Departmental or National Archives in conjunction with the supervisory institutions of the laboratory.
Once archived, research data containing personal information may be retrieved in accordance with the general rules governing the communication of archives laid down by the Heritage Code (deadlines for communication, possible exemptions for researchers, etc.).

Conservation periods must be set out and explicitly laid out when registering processing operations. This information must also be transparent to any subject data involved in a data procession operation. The conservation periods can be changed during processing operations.

Data archiving services are available at CINES and TGIR Huma-Num (in collaboration with CINES and the National Archives).

2. 5. DATA SHARING IN PARTNERSHIP RESEARCH

Research activities are sometimes conducted in partnerships involving several entities, under different supervision, sometimes involving public and private partners.

In these cases, it is imperative to anticipate and lay out within a partnership agreement (such as a consortium agreement), the capacities the partners in the project will have, within the meaning of the GDPR, as controller, joint controller or subcontractor. These partnership agreements must make it possible to identify the roles and obligations of each party, particularly regarding data security.

The scientific leader of the project is the person best suited to become the controller of the processing operation under the supervision of his/her unit director.

When a research project is to be conducted by several specific partners, the scope of authorisations for data access and manipulation must be set up in anticipation when drafting partnership agreements.

In any case, for the research purpose of the project, funders will not have the status of data controllers, in particular insofar as they are not the recipients of raw data in most situations, but only of the finalised research output.

2. 6. DATA DISSEMINATION AND PUBLICATION

Several potential situations are to be taken into account:

- Dissemination of anonymised data (always possible when the data is truly irreversibly anonymised);
- Transmission of unanonymised data to other researchers;
- Publication of unanonymised data in research papers;
- Dissemination of unanonymised data with prior consent of the data subjects.

As for the transmission of non-anonymised data to other researchers, this is made possible with the authorisation of the controller pursuant to the decree of 1 August 2018 which provides (art. 100-1):

> *"The data resulting from these processing operations and stored by the controller or his processor may only be accessed or modified by authorised persons. These persons shall comply with the rules of ethics applicable to their sectors of activity."*
>
> *The authorisations granted to these persons by the controllers are strictly regulated, they must be in line with the specific purposes and safeguards provided for by the above-mentioned decree.*

Research is based on public personal data collected online or via social network services. The laws and regulations apply if the data are not anonymous.

- define the legal basis: generally, consent or performance of a task in the public interest
- state the purpose of the processing and the relevance of the data collected
- provide for the information of individuals (e.g. on laboratories' websites, in the press) and in particular about the procedures for exercising their rights
- use anonymisation of data as early as possible
- set up data storage periods according to the purposes of the processing and the project stage

Pay attention to the way data are collected, such as secure storage, sharing, etc.

Further reading: see the CNIL's decision of 3 May 2018 authorising the University of Lorraine to implement automated processing of personal data for the purpose of research on the impact on privacy of publications of information openly accessible on social networks.

2. 7. REUSING DATA

The reuse of data makes it possible to share "personal data" resources with other researchers, particularly in the context of open science.

Since 2016, legislation (Digital Republic Act, Valter Act) have enshrined a general principle of openness and free reuse of public information (Open Data by default). In principle research data are such public information. See: Guide d'ouverture des données de recherche du CoSo (a guide to research data openness by CoSO, or open science committee).

Nevertheless, the law links these obligations of openness to the protection of personal data, providing that when including personal data, public sector information may only be made public "*after having been processed in such a way as to make it impossible to identify such persons*" (anonymisation) or with the consent of data subjects.
Data may be reused for research purposes when they have been anonymised. They may also be reused under the persons' consent or if reuse had already been provided for in the initial processing.

Except where the data have been anonymised, re-use does not exempt the researcher from procedures to update compliance with the GDPR: lawfulness of the processing, explicit, legitimate purpose, proportionality of the data, security of the data, information to individuals, etc.
See: Practical guide of the CNIL and CADA (Guide pratique de la CNIL et de la CADA) on the online publication and reuse of public data (Open data)

Example: Quetelet Progedo Diffusion and CASD provide access to data that can be reused for research projects.

The data can be reused for a commercial purpose, for example in research and technology transfer situations. In all cases, further processing will have to be set up and the personal data anonymised. Overall, except in research and technology transfer situations under the control of the laboratories' supervising entities, the purpose of the data processing operations must not be commercial. Precautions must be taken and counselling by the DPO and Technology Transfer Departments should be sought.

APPENDIX 1: SAMPLE CONSENT FORM

Proposed by the Pacte joint research unit, Social Sciences Laboratory (CNRS, Grenoble Alpes University, Institut d'Etudes Politiques de Grenoble)

CONSENT FORM FOR THE COLLECTION OF PERSONAL DATA

(*To be completed on laboratory letterheaded paper, in duplicate to be signed by the respondent. The investigator will provide one copy to the respondent and the other to the project manager).*

This form is intended to collect your consent for the collection of data/information about you, as part of the XXX project led by *"specify team / laboratory"*.

By signing this consent form, you certify that:

- you have read and understood the information provided in the information sheet;
- you are satisfied with the answers given to your questions;
- you have been informed that you are free to withdraw your consent or withdraw from this research at any time, without prejudice.

Information about the participant:
Surname: Forename: Address:

To be filled by the participant: *(to be adapted accordingly)*

- I have read and understood the information provided in the information sheet and I freely agree to participate in this research:
  ☐YES ☐NO

In the situation of an interview investigation:

- I agree that my comments may be recorded and used by the XXX project team:
  ☐YES ☐ NO
- - I agree that my image and comments may be filmed and used by the XXX project team:
  ☐YES ☐NO
- I accept that my image and my comments may be disseminated during scientific conferences, seminars or any form of promotion of the XXX project:
  ☐YES ☐ NO

In the situation of a questionnaire survey:

- I agree that my answers to the questions asked may be used by the XXX project team:
  ☐YES ☐NO

Special cases:

- I agree to the use of an embedded system [or connected object] to collect data [geolocations, practices, etc.] and that these data [geolocations, practices] be used by the XXX project team:
  ☐YES ☐ NO
- I agree that "sensitive data" of the type (list the data concerned here) will be collected, stored and used by the XXX project team:
  ☐YES ☐NO
- I agree that my personal data may be used for research projects with the same purposes as the XXX project:
  ☐YES ☐NO

Surname, forename - Date - Signature

A copy of this document is given to you, another copy is kept in our records.

APPENDIX 2: SAMPLE INFORMATION NOTICE

Proposed by the Pacte joint research unit, Social Sciences Laboratory (CNRS, Grenoble Alpes University, Institut d'Etudes Politiques de Grenoble)

PERSONAL DATA COLLECTION INFORMATION SHEET

(to be given to the participant on a laboratory letter headed sheet).

(Language should be adapted to the target audience: for example, information sheets for children should be written in clear language with words used by children)

(Data controller)

The information collected *[about you] (if direct collection)* will be processed as part of the project XXX managed by *"Surname, forename, title and institutional affiliation of the project manager, postal address and e-mail"*.

(In case of indirect data collection, e. g. web data, designate the data subjects)

The persons involved by the data processing operations will be:

(Purpose of the project)

The purpose of the processing operation is: *"specify the main goal of the research and, where applicable, specify sub-objectives"*.

Specify what is expected of the person....

For Example:

For an interview investigation

We expect you to participate in an interview during which we will ask you questions about

(write a brief description of the purpose of the project). .... The interview will last ***"specify duration"***.

Specify the collection method:

Option 1: The interview will not be recorded.

Option 2: The information collected during this interview is recorded.

Option 3: The information collected during this interview is videotaped / photographed.

Option 4: In case of commented routes with satellite navigation system (SATNAV) data collection: The routes we will follow will be recorded by GPS/GSM sensor.

For a questionnaire survey

We expect you to participate in a questionnaire survey during which we will ask you questions about *"write a reminder of the project purposes"*. The questionnaire will last *"specify administering timespan"*. *In case of a longitudinal survey, specify the duration of participation and collection periods.*

Additional collections (e.g. logbook, SATNAV tracking, use of connected objects, etc.):

Adapt accordingly:

We would also like you to fill a logbook to learn about your practices of *"specify types of practices"* for a period of *"specify timespan"*.

We also want to use a SATNAV sensor *(or other connected object)* to understand your practices of *"Specify type of practice"* in *"specify territory"* for a duration of *"specify timespan"*. You may *"turn off the GPS/deactivate the connected object"* at any time.

(Type of the data collected)

Only the data strictly necessary for the performance of our research will be collected and processed: List the types of personal data collected, for example:

Identification

Personal life (lifestyle, family situation)

Data on professional life (CV, education, training, distinctions, publications, etc.)

Economic and financial information (income, financial situation)

Internet connection (IP, logs, etc.)

Geo-location (GSM, SATNAV data, etc.)
Sensitive data (religious or philosophical beliefs, trade union or political affiliation, sexual orientation or life, offences or convictions, social security numbers, health, biometric or genetic data)
Data source (in case of indirect collection)
This information is collected from (source to be specified and indicate whether it comes from publicly available/unavailable sources) between (specify collection period).

(Legal basis of the processing operation)
The legal basis of the processing operation is based on:
Adapt accordingly:
- the execution of a public research tasks => if projects financed with public funds only
- participants' consent => mandatory in case of sensitive data, joint consent of the child and holder of parental authority if the respondents are minors under 15 years of age.

(Voluntary participation)
Your participation in "specify project name" project is on an entirely free and voluntary basis.

(Withdrawal of consent)
You are free to withdraw or terminate your participation in this project at any time. This withdrawal will have no consequences.
[If you work with students, you can specify that the withdrawal will have no impact on the rest of their education].
Longitudinal data collection case: In the case of data collection over several periods, the withdrawal of consent will be effective from the date it was received by the controller.

(Pseudonymisation/ confidentiality)
For an interview investigation
The project *"specify the name of the project"* makes the following commitments:
- Your identity will be obliterated using a random number in all writings produced on the basis of your comments (interview reports, observation notes, analysis notes exchanged between researchers, publications...).
- No other information will be kept that could reveal your identity: interview notes, interview reports, observation notes, analysis notes and publications will be completely anonymous.

For a questionnaire survey
- Your identity will be obliterated using a random number for all types of information collected (list to be adapted according to the project: questionnaires, SATNAV data, logbook, etc.).
- Only the project manager holds the correspondence table that allows you to link your identity to the random number assigned in the different files (list to be adapted according to the project questionnaires, SATNAV data, logbook, etc.).

(Recipients of personal data)
The recipient or categories of recipients of this data are: "indicate who needs to access or receive it according to the stated purposes; specify the names of organisations, partners, entities, etc. ».

(Data transfers)
Option 1: All data will be kept in France;
Option 2: The data collected will be transferred / stored by one of the project partners in a European Union country, which is subject to the same privacy rules as France.
Option 3: The data collected will be transferred / stored by one of the project partners in a country outside the European Union. The transfer is based on standard contractual clauses of the European Commission or governed by approved specific contractual clauses, a code of conduct, certification, etc.

(Storage period)
Your personal data are kept in an active database until/for "specify date or duration".
Option 1: After this date/period, your data will be permanently archived (if of significant scientific, statistical or historical interest)
Option 2: After this date/period, they will be permanently archived anonymously (if there is no interest in keeping the personal data).

(Security)
In order to guarantee the confidentiality of your data and avoid their disclosure, the following measures have been put in place:

- The only entity(-ies) which will have authorised access to the data will be the following: "specify entity(-ies)".
- (If applicable) The external service provider "specify its role" is subject to contractual guarantees protecting your data.
- The following safety measures (hardware and software) have been secured : (e.g., fire protection, backup copies, antivirus software, regular change of minimum 8-character alphanumeric passwords, computer encryption)

(Dissemination)
The results of this research will be disseminated anonymously in professional and scientific conferences, reports to authorities, professional and academic journals and general public information (list to be adapted according to the project).

(Rights of persons)
You are entitled to ask questions about this project at any time by contacting the project manager by e-mail: *"specify address"*.
You have the right to access and require a copy of your personal data, object to the processing of your personal data, have them rectified or deleted. You also have a right to limit the processing of your data. You can exercise these rights by contacting: *"indicate the contact details of the department or person responsible for the right of access - postal address and email"*.
You can also contact the Pact Laboratory Data Protection Officer at the following address: DPD - 17 rue Notre Dame des Pauvres - 54519 - Vandoeuvre lès Nancy Cedex - dpd.demandes@cnrs.fr

After contacting us, if you believe that your Data Protection rights are not respected, you may file a claim online with the CNIL or by post. CNIL, 3 Place de Fontenoy, TSA 80715 - 75334 Paris Cedex 07 (https://www.cnil.fr)

APPENDIX 3

Key issues to achieve compliance with legislation on the protection of personal data

Situation 1:

The data used for your research will be (irreversibly non-identifying) anonymous data.	The laws and regulations on personal data protection need not apply

Situation 2:

The data used for research are personal data: application of the GDPR with adjustments when the processing operations are for research purposes

		See page(s)
Who is responsible?	• The data controller • The processor (subcontractor) • Partners, processing joint controllers	12, 27
What kind of data?	• Non-sensitive data • Sensitive data • Social security number • Data on offences and convictions • Data on vulnerable populations	11, 21
How are the data collected, who are the recipients?	• Direct collection • Indirect collection	19
What is the purpose of the processing?		23
Do the data correspond to the purpose and are they sufficient for the project?	Principles relating to data processing	15, 23
How long are the data to be stored?		26
How are people informed? What rights do they have?		16
What provisions are required to ensure data confidentiality and security?	• Data hosting • Storage • File/folder sharing	24, 27
Is a privacy impact assessment necessary?	• The CNIL's open source PIA software	16

What steps should be taken? Who should they be carried out with?	• Registration in the processing records • The Data Protection Officer • The CNIL	12 13
Are there any mechanisms, methodological aids, services available for the scientific community?	Anonymisation and pseudonomysation techniques Data hosting and archiving services	25, 26
What data can I publish?		27
Can the data be reused?		28

APPENDIX 4

LIST OF ACRONYMS

ANR: Agence Nationale de la Recherche (French national research agency)

CASD: Centre d'Accès Sécurisé aux Données (national secured data access centre)

CEREES: Comité d'Expertises pour les Recherches, les Etudes et les Evaluations dans le domaine de la Santé (national expert committee for health research, studies and evaluations)

CINES: Centre Informatique National de l'Enseignement Supérieur (national computer centre for higher education)

CNIL: Commission Nationale de l'Informatique et des Libertés (National Commission on Informatics and Liberty)

CPP: Comité de Protection des Personnes (ethical research committees)

CNRS : Centre National de la Recherche Scientifique (national centre for scientific research)

DPD : Délégué à la Protection des Données (Data Protection Officer, DPO in this document)

INDS: Institut National des Données de Santé (national institute for health data)

INIST: Institut de l'Information Scientifique et Technique (institute for scientific and technical information)

INRA : Institut National de la Recherche Agronomique (national institute for agricultural research)

MR: Research Methodology

OPIDOR: Optimisation du Partage et de l'Interopérabilité des Données de la Recherche (a support portal set up and hosted by the CNRS Inist for research data sharing optimisation and interoperability)

H2020: Horizon 2020 research framework programme (EU)

PUD: Plateformes universitaires des Données (university data plaforms)

TGIR: Très Grande Infrastructure de Recherche (very large research infrastructure)

TGIR Huma-Num: TGIR des Humanités Numériques (very large research infrastructure for digital humanities)

TGIR Progedo: TGIR Production et Gestion des Données en Sciences Sociales (very large research infrastructure for social science date production and management)

EU: European Union

Cover photo: Interactive visualisation of climate change topic clusters generated by the Climate Tweetoscope.
© David CHAVALARIAS / Noé GAUMONT / Maziyar PANAHI / ISC-PIF / CAMS / CNRS Photothèque

INSTITUT DES SCIENCES HUMAINES ET SOCIALES
3, rue Michel-Ange 75016 Paris
www.inshs.cnrs.fr
@INSHS_CNRS
Subscribe to INSH Newsletter:
inshs.com@cnrs.fr

Design: InSHS Communication

Scan QR Code
to quickly join us on Twitter: