Deliverable Number: D8.3, version: 1.3

Report on Legal and Regulatory framework

CAREGIVERSPRO MMD

CAREGIVERSPRO-MMD PROJECT

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

COOSS / Ricerca e formazione

Mobiles Dynamics

FUB UNIVERSITAT A MANRESA

UNIVERSITY OF Hull

CHU Hôpitaux de Rouen

Q-PLAN INTERNATIONAL

CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 690211"

Document information

Project Number	690211	**Acronym**	CAREGIVERSPRO-MMD
Full title	Self-management interventions and mutual assistance community services, helping patients with dementia and caregivers connect with others for evaluation, support and inspiration to improve the care experience		
Project coordinator	Universitat Politècnica de Catalunya- BarcelonaTech Prof. Ulises Cortés, ia@cs.upc.edu		
Project URL	http://www.caregiversprommd-project.eu		

Deliverable	**Number**	D8.3	**Title**	Report on Legal and Regulatory framework
Work package	**Number**	8	**Title**	Project Management

Date of delivery	**Contractual**	01-01-2017	**Actual**	
Nature	Report ☑ Demonstrator ☐ Other ☐			
Dissemination Level	Public ☐ Consortium ☐			
Keywords				

Authors (Partner)	Atia Cortés (UPC), Cristian Barrué (UPC), Luis Oliva (UPC), Ulises Cortés (UPC)			
Responsible Author	Cristian Barrué		**Email**	cbarrue@cs.upc.edu
	Partner	UPC	**Phone**	+ 34 93 413 40 11

Document Version History

Version	Date	Status	Author	Description
0.1	11-02-2016	Draft	Cristian Barrué (UPC)	Creation of the document, gathering of state of the art
0.2	12-05-2016	Draft	Cristian Barrué (UPC)	Indexing and summarization
0.3	12-05-2016	Draft	Cristian Barrué (UPC)	Directives data protection, privacy and good clinical practices
0.4	12-05-2016	Draft	Atia Cortés (UPC)	Ethics data protection, privacy and good clinical practices
0.41	25-09-2016	Draft	Ulises Cortés (UPC)	Review
1.0	26-09-2016	Draft	Atia Cortés (UPC)	New structure
1.0UC	21-10-2016	Draft	Ulises Cortés	Review
1.1	21-10-2016	Draft	Atia Cortés	New structure (cont.)
1.2	28-11-2016	Draft	Atia Cortés + Luis Oliva	National Data Protection Acts
1.3	28-11-2016	Final	Atia Cortés	Appendix B & C

Executive summary

This deliverable summarizes the different directives and regulations at European and national level for the four pilot countries in terms of personal data protection, personal data privacy and good clinical practices in medical research with data subjects. All topics are studied from an ethical and legislative point of view.
As this is a living document, it may evolve, be updated or modified during the duration of the CAREGIVERSPRO-MMD if the legal context changes, to assure consistency we will reference previous changes.

List of Acronyms

Acronym	Title
AB	Advisory Board
CA	Consortium Agreement
C-MMD	CAREGIVERSPRO-MMD
CT	Clinical Trial
DC	Data Controller
DP	Data Processor
DPO	Data Protection Officer
DS	Data Subject
EC	Ethics Committee
IDPA	Italian Data Protection Authority
MS	Member State
SP	Service Provider

List of Tables

Table of contents

1 Introduction

Health research has become an important a mainstay for improving the state of the art in its different fields, such as epidemiology, biomedicine, health services as well as its socio-economic impact on society. One of the most common forms of health research is the clinical trial, where volunteer individuals will participate in studies in order to assess a new medical product, device or treatment. Most of this research is done through collecting different types of data, from biological characteristics to physical and/or cognitive assessments. During the last years, it has also included new data coming from sensors that will interact directly with the individual (bio-sensors or wearable sensors) or environmental sensors. In our case, the C-MMD platform will also collect user-generated content with sensitive personal data. Although health research aims to promote health and well being, as well as to improve health and social services, its management might also represent a risk to the society due to the type of data that is stored and processed. **It is, thus, obvious that our consortium puts special attention on defining pilot protocols and analysis methods that will ensure an ethical health research, where the privacy of personal data is protected as well as individuals' dignity**.

Ethics, an essential dimension of human research, is considered both as discipline and practice. For clinical research, ethically justified criteria for the design, conduct, and review of clinical investigation can be identified by obligations to both the researcher and human subject. Informed consent, confidentiality, privacy, privileged communication, and respect and responsibility are key elements of ethics in research.

Directives and regulations are established in order to apply the criteria defined in the ethical health research by defining a set of rules, or principles, accepted by different institutions or, in this case, member states of the EU. Directives are only a legislative act that all EU countries must achieve, although each one will decide their own laws to reach these goals. However, regulations are a binding legal act, which means that they must be applied in its entirety across the EU. The regulatory framework is, thus, a system of policies, regulations and procedures, contracts and agreements, which aims to harmonize the different EU Member States policies. In the scope of the CAREGIVERSPRO-MMD, its main objective is to provide transparent methods for health research by guaranteeing human subjects' fundamental rights.

This document covers the existing regulations and standards affecting the C-MMD platform and processes to be implemented on CAREGIVERSPRO-MMD project. The Consortium is aware that these may change again and new will be appearing during the lifetime of the project and, when possible, the Consortium will try to catch-up. Moreover, ethical aspects and best practices will also be covered in this reference document. The main purpose is to provide to all project partners and stakeholders, a common framework for the understanding and application of the legislation and recommendations related to each project stage, to build prototypes (and later products) that meet EU regulation and international standards.
Terms used in this document, as for example, company(ies), project partner(s), designer(s), developer(s) are referring to the organisations and responsible persons involved. Other terms used like medical device(s), prototype(s), pilot(s), product(s) are to be understood as per their correspondent development phase.

This document is therefore a preliminary over-view of the regulations and standards at the level of technology specs provided. Upcoming deliverable versions of D8.3 will complement and detail with uncovered issues or new regulatory aspects (every 12 months). Observation and reporting of regulatory requirements will be ready for the different stages of design and development although official reporting is due to the end of each project year.

For a better understanding, the document will be structured by main topics involved in health research with human subjects. Each topic will first be introduced from an ethical point of view; then we will describe the legal implications regarding these topics for the EU and National Regulatory Frameworks (*i.e*. EU regulations, ISO standards, *etc*). Relevant definitions found in the directives are added in Annex A.
The Annex and Formularies provided will be used through the whole project and will be labelled accordingly as per its status of review (with an indicative letter or date).

The success of the C-MMD project depends greatly on having all project partners and main actors being aware of the ethical challenges involved in the inception and implementation of the proposed platform and services. The C-MMD consortium must be able to identify potential ethical risks and know in beforehand best practices to reduce or avoid those risks.

2 EU Fundamental Rights

In 1950, the Council of Europe drafted a first version of the **European Convention on Human Rights**. The aim was to collect in a single document an international treaty defining principles for human rights protection and fundamental freedoms in Europe. It was the first instrument to give effect to certain of the rights stated in the Universal Declaration of Human Rights and make them binding. It is based on the previously existing national regulations from UK, France and Germany. Several amendments have been presented since then, adding every time new articles or protocols to the convention. The last accepted version dates from January 2010.

Similar to this Convention, the EU has also proclaimed the **Charter of Fundamental Rights (2012/C 326/02)**, which defines political, social and economic rights for the EU citizens and residents and for the Union itself, and provides directives on preservation and development of common values to be respected despite cultural and traditional diversity present in Europe, and which aim to be helpful for future changes in society, social progress or scientific and technological development. This Charter has full legal effect since its signature during the Treaty of Lisbon in December 2009.

The Charter aims to protect the fundamental rights of EU citizens and of future generations to promote the concept of EU human community, as well as to create a space for freedom, security and justice. It is mainly based on the European Convention on Human Rights.

The Charter is divided in seven sections; each of them includes a list of rights and/or responsibilities for the EU citizens:

- **Dignity:** includes the right to life and to the integrity of the person. In this sense, a person must always be informed about any medical or biological procedure and free to consent it.
- **Freedoms:** includes the right of protecting and accessing one's personal data, but also the right of freedom of expression and education, to have access to free compulsory education. It also protects the freedom on academic and artistic freedom.
- **Equality:** promotes equality before the law, independently of the gender, age, religion or cultural background. In the case of the elderly and disabled people, the Union recognises and respects the rights of leading an independently living and their social and occupational integration in the society.
- **Solidarity:** collects a list of rights protecting the well-being and security of workers and employers. It also guarantees the right of access to preventive health care.
- **Citizens' rights:** ensures the rights to vote and to have access to a good administration service and to any institutional document.
- **Justice:** provides means to assist any EU citizen whose rights and freedoms have been violated, as well as principles of legality.
- **General provisions governing the interpretation and application of the Charter:** explain the role and duties of institutions, bodies, offices and agencies of the Union in respecting and promoting the rights. It also defines the scope of application in relation to other Treaties and prevents from misinterpretation of abuse of these rights and freedoms.

3 Personal Data Protection and Privacy

The protection and privacy of personal data are two of the main rights that a EU citizen has, as it has been described in Section 2. In this section, we introduce the main directives and regulations regarding the data protection and privacy from a legislative point of view.

3.1 Introduction

One of the main principles of the EU Convention of Human Rights (Article 8) and the Charter of Fundamental Rights (second title: Freedoms) **is the right of protecting and individual's integrity and personal data privacy**. However, each member state had its own interpretation and legislation, which could in the end create conflicts in international exchanges. The EU has established a set of rules that define the strict conditions under which personal data can be **legally gathered and transferred**. At the same time, it specifies the different stakeholders involved in **data collection and processing**, as well as their rights and obligations.

The **Directive 95/46/EC of the European Parliament and the Council** on the protection of individuals with regard to the processing of personal data and on the free movement of such data, also known as the **Data Protective Directive**, is the reference text, at European level, on the protection of personal data that was approved on October 24th 1995. It sets up a regulatory framework that seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data[1].

On December 2015, a new set of rules on data protection where approved by the European Parliament, the Council and the Commission. As a result, the **Regulation 2016/679** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data was adopted in May 2016. The aim is to strengthen citizen's fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market.

As a complement to the Data Protective Directive, the EU presented the **Directive 2002/58/EC of the European Parliament and the Council** of July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, also known as **E-Privacy Directive**. This Directive has been amended by Directive 2009/136, which introduces several changes concerning cookies and data security breach notification system.

In addition, the EU set out the **Regulation 45/2001** on ensuring citizens' privacy, also known as the **European Data Protection Supervisor (EDPS)**. In particular, this law aims to ensure that the EU institutions and bodies respect the citizens' right to privacy regarding the processing of personal data.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012

3.2 Summary

The above-mentioned laws apply to data processed by automated means (*e.g.* a computer database of customers) and data contained in or intended to be part of non-automated filing systems (traditional paper files). Four main stakeholders are involved in this regulatory framework (see complete definitions in Annex 1):

- data subject (DS): the natural person from which personal data is being collected.
- data controller (DC): the entity (person, public authority, agency or other bodies) in charge of determining the purposes and means of processing the personal data.
- data processor (DP): the entity (person, public authority, agency or other bodies) in charge of processing the personal data on behalf of the controller.
- data protection officer (DPO): the person (data protection law and practices expert which can be employee of the data controller or an outside consultant) assigned in an Institution to keep register of all the processing operations on personal data

The regulatory framework defines the **citizens' rights towards their personal data**, i.e. the right to be informed about the processed data, the right to access to data, the right to object to the processing of data or the right to be forgotten.

On the other hand, it also establishes **data controllers and processors' obligations** in order to ensure the European Fundamental Rights, *i.e.* data might be processed fairly and lawfully, data might be processed for legitimate and specified purposes, data might be processed in a secure and confidential way. Finally, these regulations define standards in which personal data should be transferred among countries, including those outside the EU.

The **data protection officer's obligations** are, among others, to inform and advise the data controller of its obligations pursuant to the Regulation and is as well responsible for monitoring, notifying and otherwise communicating information about personal data breaches, and documenting public and regulators' requests regarding the removal, destruction and accessibility of data.

Finally, the regulatory framework aims to ensure security on data protection and privacy in the digital age. It offers a set of rules to provide secure communication services involved in the processing of personal data, the notification of personal breaches and confidentiality of personal data. It also bans unsolicited communications where the user has not given their consent. Data controllers and processors must secure their services by ensuring authorised access to data, protecting data preservation and implementing security policies on the processing of personal data. On the other hand, EU countries

3.2.1 National Regulations

Although the Data Protection Directive is general for all the EU member states, nowadays each state still has its own national regulation. In this section, we will highlight the special cases for each of the national regulations involved in the CAREGIVERSPOR-MMD project (France, Italy, Spain and UK) that would not appear in the general directive. The relevant issues related to the project will be highlighted in the summary of this section (see Table 1: Personal Data Protection).

All the national regulations apply to any person (data controller or data processor) in charge of collecting, processing or storing personal data. Although the presence of a data controller is mandatory in all national regulations, the role of the data processor is not mandatory in the cases of UK and Italy.

In addition, **all the national regulations allow personal data transfer inside the EU.**

3.2.1.1 United Kingdom's Data Protection Act 1998 (98/DPA UK)

An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

The Act applies to data controllers that are established in the United Kingdom and process data in that context or, if they are not established in the United Kingdom or EEA State, if they use equipment in the United Kingdom for any other purpose than its transition through the United Kingdom. In the latter case, the data controller must nominate a representative established in the United Kingdom for the purposes of this Act.

Data, according to the Act, refers to data as any kind of information held in a computer, which includes information recorded in paper that is intended to be stored on a computer. Personal data means data that is related to a living individual who can be identified from those data and/or other information that is in the possession of, or is likely to come into possession of, the data controller. This means that

Finally, an additional level of data is distinguished: sensitive personal data, which means personal data consisting of information such as racial or ethnic origin, political opinions, religious beliefs, and physical or mental health condition, etc. Basically, any information that is susceptible to be used in a discriminatory way. Processing this type of data requires complying with additional restrictions given its nature.

3.2.1.2 Italian Data Protection Code

In Italy, personal data processing is based on and governed by **Legislative Decree No. 196/2003**, which contains the Italian Personal Data Protection Code (the Code from now on), which has implemented Directive 95/46/EC on data protection (Data Protection Directive) into the Italian legal system.

The Italian Data Protection Authority (also known as "Garante" in Italian, IDPA from now on) is committed to accomplish the measures with regard to privacy and personal data protection especially, but not only, in the following areas:

- Video surveillance.
- Biometric data processing.
- Health data processing.
- Data breach notifications.
- Bank information processing.
- E-health records.
- Data processing carried out by system administrators.
- Data processing for marketing and profiling purposes.

- Mobile payment.
- Cookies.

The Code aims to provide guarantees for data subjects and mandatory requirements for those who process personal data, which is defined as any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a personal identification number (*Article 4(1)(b), Code*).

In this case, the Code makes a distinction between data controller, who have full autonomous decision making power regarding the purposes and mechanisms of data processing, and data processors, which role is optional for the data controller and act on behalf on them.

The Code covers all the phases in personal data processing, including any operation carried out both manually or by automated means. This process involves the collection, recording, organization, storage, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of personal data.

The Code tackles the processing of personal data in different professional sectors, one of them being the health care sector (Sections 75 to 94). The main requirements for processing health care data are the data subject's consent and the IDPA authorization. The Code simplifies the process to obtain consent.

The Code also enhances the importance of codes of conducts and professional practice in respect of the protection of personal data. In particular, it covers sectors such as processing of data via the Internet and/or employment context, for purpose of direct marketing, by private credit reference agencies, or in connection with video surveillance activities. These codes of conduct can be found in the Annex of the DPA.

3.2.1.3 Spanish data Protection Act

The Data Protection Act (Law 15/1999 on the protection of personal data) implemented Directive 95/46/EC on data protection (Data Protection Directive). It protects individuals with regard to the processing of personal data and the free movement of data. The Regulation developing the Data Protection Act was approved by Royal Decree 1720/2007 of 21 December (Data Protection Regulations).

The DPA and Data Protection Regulations apply to the processing of personal data, being any information relating to an identified or identifiable natural person (i.e. the data subject).

The Data Protection Act and the Data Protection Regulations apply to:

- Data processing carried out in the context of the activities of an establishment of the data controller in Spain. Where this is not the case, but the data controller uses a data processor established in Spain, the data processor must comply with the provisions on security measures established in the Data Protection Regulations.
- Data processing carried out by a data controller not established in Spain but in a place where Spanish law applies by virtue of international public law.

- Data processing carried out by a data controller not established in the European Union but using means located in Spain, unless such means are used only for transit purposes. In this case, the data controller must appoint a representative established in Spain.

Data processing means any operation or procedure (whether automated or not) for the collection, recording, storage, elaboration, modification, blocking or erasure of data. It also includes disclosure of data resulting from communications, queries, interconnections or transfers.

Data controllers and data processors must generate a security document in which minimum security measures to be implemented are specified, establishing three cumulative security levels: basic, medium and high. The security measures include specifications on access control, identification and authentication, incident records management of documents and media, backup copies, security officers, audits, access records and telecommunications.

3.2.1.4 French Data Protection Act

The Data Protection Act No. 78-17 dated 6 January 1978 (*Loi informatique et libertés*) (DPA) is the key legislation on the protection of personal data. Personal data is defined as "any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to them" (*Article 2, DPA*).

The DPA created the French Data Protection Authority (*Commission Nationale Informatique et Libertés* (CNIL). The DPA has been amended several times, in particular by Act No. 2004-801 of 7 August 2004.

The DPA applies to the processing of personal data by a data controller that either is established in France or carries out its activities in an establishment in France, regardless of its legal form. Means of processing are located in France if:

- Data is collected in France.
- The hosting server is located in France.
- The external service provider is located in France.

4 Good Clinical Practices: Research with Human Beings

Good clinical practice (GCP) is a set of internationally recognised ethical and scientific quality requirements that must be observed for designing, conducting, recording and reporting clinical trials that involve the participation of human subjects[2].
In this section, we introduce the ethical principles that clinicians and other researchers must take into account when designing a clinical trial. We will then analyse this issue from a legislative point of view. A summary table is provided in Section 5.2.

[2] Consultation Letter on the Medicines for Human Use (Clinical Trials) Regulations 2003. http://www.mhra.gov.uk/home/groups/comms-ic/documents/websiteresources/con007629.pdf

4.1 Ethical motivation and principles

The research involving the participation of human beings is particularly delicate, since it usually implies the collection of personal and/or biological data. Following the European Fundamental Rights, it is important to guarantee the protection of the identity and dignity of the participants. Several documents gather the different ethical principles that will affect any research process involving human subjects.

The **Declaration of Helsinki** is a document written and adopted by the World Medical Association (WMA) during the General Assembly of June 1964 in Helsinki. It has since been amended by the WMA in five occasions, the last one being in Seoul in October 2008. This Declaration aims to promote good practices during the design and execution of medical research involving studies with human subjects. The main objective of physicians must be to safeguard the health of patients and this has to be maintained during the research.

The Convention for the protection of Human Rights and Dignity of the Human Being with regards to the Application of Biology and Medicine, also known as the **Convention on Human Rights and Biomedicine**, is an agreement among the member States of the Council of Europe, the other States and the European Community in order to adopt some measures on human rights applied to biology and medicine. The Convention is the first legally-binding international text designed to preserve human dignity, rights and freedoms, through a series of principles and prohibitions against the misuse of biological and medical advances.

From the legislative point of view, the **European Parliament and of the Council approved on 4 April 2001 the Directive 2001/20/EC** on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, also known as the **Clinical Trials Directive.** This Directive establishes the basic principles framing the conduct of clinical trials on medicinal products, seeking for a faster and thorough assessment of an application by all Member States concerned, and ensuring one single assessment outcome and authorisation per Member State. Its aim is to ensure the quality and transparency of clinic trials data by respecting human rights and human dignity. However, the Directive has received negative feedback from Member States since the time and cost of conduct clinical trials among several EU countries has grown significantly[3]. A new **Clinical Trials Regulation (EU No 536/2014)** has been approved and is expected to be legally effective from June 2016 (clinical trials approved prior to this date will still apply to the 2001 Directive during the following three years after the approval date[4]). One of the main changes is the redefinition of the concept of 'clinical trial' by introducing the broader concept of 'clinical study'. There will thus be a dichotomy of 'clinical trial' and 'non-interventional study' in order to be in line with the EU law governing medicinal products (although the Regulation will not apply to non-interventional studies).

[3] Dr. Martine Dehlinger-Kremer, The New EU Clinical Trials Regulation: the Good, the Bad, the Ugly.

[4] CAREGIVERSPRO-MMD will not be affected by the 536/2014 Regulation.

4.2 Summary

The WMA Declaration of Helsinki aimed to establish a set of principles that physicians shall embrace to guarantee their **duty towards research subjects**, which is to protect *"the life, health, dignity, integrity, right to self-determination, privacy and confidentiality"* of their personal information. In order to control the abuse of personal data exploitation, **a research protocol must be presented and approved by a research Ethics Committee** before the study begins. It has to include (1) the design and performance of the study; (2) information regarding funding, sponsors and institutional affiliations; (3) incentives and compensations in case of harm for the participants; (4) expected beneficial outcomes and post-study access to data by subjects. On the other hand, the research team must also provide an **informed consent** to the participant where all the information related to the protection and processing of their personal data is explained, along with the description of the clinical trial, the expected outcomes and possible effects. In case of being physically or mentally incapable of giving consent, physicians must seek consent from a **legally authorized representative**.

The protocol should outline the procedures applied to follow the principles of this Declaration. It must also state that the **participation is voluntary** and that the research subject is allowed to consult to family members before consenting and free to refuse or withdraw the consent at any time. If the clinical trial aims to determine the efficacy of an intervention, the use of placebo or no treatment must be justified as a comparison method.

Another important aspect to guarantee the transparency in the process of a medical research is that **clinical trials must be registered in a publicly accessible database** before the recruitment of the first subject. Usually, clinical trials performed in the EU are stored in the European Database (EudraCT[5]).

In addition, the Clinical Trial Directive provides a set of internationally recognized ethical and scientific quality requirements as **good clinical practice**, which has to be adopted by all Member States involved in clinical trials with human subjects. Member States shall adopt the laws, regulations and administrative provisions necessary to comply with it[6].

In particular, the Directive focuses on the **protection of the research subjects**, its physical and mental integrity and its right to privacy. It also defines the **role of the Ethics Committee** in preparing its opinion on clinical trials. In particular, it shall take into consideration: *(i)* the relevance of the trial and the trial design; *(ii)* the protocol; *(iii)* the suitability of the investigator (i.e. the person responsible for performing the clinical trials on a site) and his supporting staff; *(iv)* the quality of the facilities. The Ethics Committee has a maximum of 60 days from the day of receipt of a valid application to provide a reasoned opinion; the clinical trial shall not start before receiving the approval from the Ethic Committee. Finally, the Directive describes the conditions and time limits to **conduct a clinical trial**. When necessary, the investigator must immediately send a **notification of adverse events** to the sponsor, except for those listed in the protocol or in the investigator's brochure as not requiring and immediate reporting.

[5] https://eudract.ema.europa.eu/
[6] The Appendix contains the basic definitions applied in this Directive.

5 C-MMD Relevance

In this section we provide a summary table for the Data Protection and Privacy and another for the Good Clinical Practices in medical research with human subjects. Each table contains:

- A list of the main topics referred in the different directives and regulations presented in previous sections
- The stakeholders affected in each topic (references to the acronyms are given at the beginning of the deliverable)
- A summary of the actions related to each topic
- The articles that make reference to each topic in the different legal documents revised

5.1 Summary of regulatory requirements relevant to C-MMD with regards Data Protection and Privacy

TOPIC	ROLE	DESCRIPTION	ARTICLE
Data Quality	DC	Personal data must be processed: - fairly and lawfully - collected for specified and legitimate purposes - adequate, relevant and not excessive with the purposes - accurate and up to date - permits identification of data subjects for no longer than necessary - further processing is permitted if there are appropriate safeguards about anonymity	Art. 6 95/46/EC Art. 4 2001/45/EC Art. 5 2016/679
Lawfulness & Special Categories of Processing	DP, DS	Personal data may be processed only if the DS has unambiguously given his consent, especially for revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life.	Art. 7 & 8 95/46/EC Art. 5 & 10 2001/45/EC Art. 6 & 9 2016/679
Information to be given to the DS	DC, DS	DC must provide the following information to the DS: - identity of DC - contact details of the DPO - purposes of the processing for which the data are intended - other information regarding the recipients of the data, type of questions, period of storage	Art. 10 & 11 95/46/EC Art. 11 2001/45/EC Art.13 2016/679 Art. 7 & 8 98/DPA UK
Right of Access	DS, DC, IDPA	DS should receive from DC within 3 months after request: - confirmation as to whether or not data relating to him are being processed - information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, - communication in an intelligible form of the data undergoing processing and of any available information as to their source,	Art. 12 95/46/EC Art. 13 2001/45/EC Art. 15 2016/679

		- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions	
		DS can write a complaint to the IDPA via a website form in case of data privacy breach. IDPA can also order businesses to abide by compliance requirements set out in its decisions. Businesses have 15 days to comply and the turn-around for dealing with complaints is 60 days.	Section 7-10 Code
		In the case of UK, DC is not obliged to supply any information unless he has received a written request or in prescribed cases. The answering time after the request reception is 14 days	Art. 7, sec 3-6 98/DPA UK Art. 7, sec 8 & 10 98/DPA UK Art. 8, sec 7 98/DPA UK
Right of Rectification	DS, DC	DS shall have the right to obtain from DC the rectification without delay of inaccurate or incomplete personal data	Art. 12 95/46/EC, Art. 14 2001/45/EC, Art. 16 2016/679
Right of Erasure ("right to be forgotten")	DS, DC, DPO	DS shall have the right to obtain from DC the erasure of personal data concerning him or her without undue delay	Art. 17 2016/679
		DC shall erase personal data undue delay under the following situations: - DS withdraws consent - personal data has been unlawfully processed - the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which DC is subject	Art. 12 95/46/EC Art. 16 2001/45/EC
		DC shall erase also in case DS objects the data processing	Art. 10 98/DPA UK
Right of Blocking	DS, DC	DS shall have the right to obtain from DC the blocking of personal data where: - Their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the data, or; - The controller no longer needs them for the accomplishment of its tasks but they have to be maintained for purposes of proof, or; - The processing is unlawful and the data subject opposes their erasure and demands their blocking instead	Art. 12 95/46/EC Art. 15 2001/45/EC Art. 18 2016/679
Right of Data Portability	DS, DC	DS has the right to receive the personal data concerning him/her, which s/he has provided to the DC. DS has also the right to transmit this data to another DC	Art. 19 2016/679
Notification to Third Parties	DC	To whom the data have been disclosed of any rectification, erasure or blocking	Art. 12 95/46/EC Art. 21 2001/45/EC
Confidentiality of processing	DC, DP	Any person acting under the authority of the DC or of the DP, including the DP himself, who has access to personal data must not process them except on instructions from the DC	Art. 16 95/46/EC Art. 21 2001/45/EC
Security of processing - Data	DC	DC shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected (e.g.	Art. 17 95/46/EC Art. 22 2001/45/EC

protection *by design* and *by default*		unauthorised disclosure or access, accidental or unlawful destruction or accidental loss or alteration, etc)	Art. 25 & 32 2016/679
Notification of data breach	DC, DP, DS	- When detected, DC shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent. - DP shall notify the DC without undue delay after becoming aware of personal data breach - When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay	Art. 33 & 34 2016/679
Data Protection Impact Assessment	DC	Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the DC shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks (see D7.3.4 Privacy Impact Assessment for further details)	Art. 35 2016/679
Prior consultation	DC, DP, DPO	DC shall consult the supervisory authority prior to processing data when a PIA indicates that the processing would result in high risk in the absence of measures. When consulting, the DC should provide the following information to the supervisory authority with: (a) where applicable, the respective responsibilities of the DC, joint DC and DP involved in the processing, in particular for processing within a group of undertakings; (b) the purposes and means of the intended processing; (c) the measures and safeguards provided to protect the rights and freedoms of DS pursuant to this Regulation; (d) where applicable, the contact details of the DPO; L 119/54 EN Official Journal of the European Union 4.5.2016; (e) the data protection impact assessment provided for in Article 35; (f) any other information requested by the supervisory authority.	Art. 36 2016/679
Processing of personal data on behalf of controllers	DC, DP	DC must choose the DP providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out. The DC must be governed by a contract or legal act binding the DP to the DC and stipulating that: - DP shall act only on instructions from the DC The obligations set out by the law of the Member State in which the DP is established, shall also be incumbent on the DP - The contract shall be in writing form or similar for purposes of keeping proof.	Art 23. 2001/45/EC
Notification to the Data Protection Officer	DC, DPO	DC must notify the public national supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. The information to be given shall include: - the name and address of the controller and an indication of the organisational parts of an institution or body entrusted with the processing of personal data for a particular purpose;	. Art. 18 95/46/EC Art. 25 2001/45/EC Art. 30 2016/679 Art. 16, 18, 19 & 20 98/DPA UK

		- the purpose or purposes of the processing; - a description of the category or categories of data subjects and of the data or categories of data relating to them; - the recipients or categories of recipient to whom the data might be disclosed; - a general indication of the time limits for blocking and erasure of the different categories of data; - proposed transfers of data to third countries or international organizations; - a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 22 45/2001/EC to ensure security of processing	
		DC shall notify to IDPA the processing of personal data of the following higher-risk categories: - genetic and biometric - geo-localization - behavioural advertising	Section 37 Code IT
		Before processing data, DC must either notify the CNIL or obtain authorisation from the CNIL. The notification regime applies to automatic procedding only. In the following cases, an authorization from the CNIL is required: - The processing of sensitive data. - The processing of genetic data. - The processing of data relating to offences and security measures. - Biometric identity checks. - The transfer of data outside the EU to a country without adequate protection CNIL has 2 months to make a decision.	Art. 23&24 04/DPA FR
		Registration of personal data files is required before processing. Data controllers must register their data files with the General Data Protection Registry. For this, DC must complete a notification form available on the Data Protection Agency's website.	Art. 26 99/DPA ES
Register	DPO, DC	DPO shall keep a register of processing operations Personal data shall only be transferred within or to other Community institutions or bodies if: - the data is necessary for the legitimate performance of tasks covered by the competence of the recipient - both DC and the recipient shall bear the responsibility for the legitimacy of this transfer - the recipient shall process the personal data only for the purposes for which they are transmitted	Art. 26 2001/45/EC Art. 39 2016/679
		Registration must be updated whenever there are changes to the data files affecting the information notified to the Data Protection Agency (including removal of the data file).	Art. 26 99/DPA ES
Protection of Personal Data and Privacy in	SP, Community	Community institutions and bodies shall take appropriate technical and organizational measures to safeguard the secure use of the telecommunications networks and terminal equipment, if necessary in	Art. 35 2001/45/EC Art. 5 2002/48/EC

The Context of Internal Telecommunications Networks	institutions	conjunction with the providers of publicly available telecommunications services or the providers of public telecommunications networks	
Confidentiality of Communication	MS	Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC	Art. 5 2002/48/EC
Location data and other traffic data	DS, SP	Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the DS or subscribers to the extent and for the duration necessary for the provision of a value added service.	Art. 9 2002/48/EC
Directories of Subscribers	MS, DS	Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public. Subscribers shall also have the opportunity to determine whether their personal data are included in a public directory and, if so, to the extent that such data are relevant to the purpose of the directory.	Art. 2002/48/EC
Penalties	DS	Without prejudice to any other administrative or judicial remedy, every DS shall have the right to lodge a complaint with a supervisory authority, in particular in the MS of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation	Art. 77 2016/679 Art. 13 98/DPA UK

Table 1: Personal Data Protection

5.2 Summary of regulatory requirements relevant to C-MMD with regards Good Clinical Practices

TOPIC	ROLE	DESCRIPTION	ARTICLE
Protection of clinical trial subjects	MS, DS, physicians	- CTs with DS must ensure methods of protecting the individual's dignity and integrity. MS also ensure that the DS has been informed and understands the CT. - The protocol presented to the EC shall include the process of anonymization of personal data for later analysis - DS shall be provided with the investigator or sponsor's contact point to obtain further information - DS has the right to refuse to participate in the study or withdraw consent to participate at any time without reprisal.	Art. 3 2001/20/EC Prin. 11, 14, 15, 22, 24 WMA DoH
Informed Consent	DS	- People participating in CTs have the right to be informed about the risks and benefits of the study - People shall not participate in a clinical study without signing a	Art. 3 2001/20/EC Prin. 22, 24, 26 WMA DoH

		formal consent - People have the right to withdraw the clinical trial once it has started	
Right of incapacitated adults on being informed	DS, EC	-In the case of persons incapable of giving their informed legal consent, a legal representative shall provide it and might be revoked at any time, without detriment to the DS - CT shall justify the necessity to include individuals that are no able to give informed consent (*e.g.* comparison with other subjects, CTs designed to minimize pain, discomfort, fear and any other foreseeable risk in relation to the disease and developmental stage)	Art. 5 2001/20/EC Prin. 27, 28, 29
Commencement of a trial	MS, sponsor	MS shall take the measures necessary to ensure that the following procedure is accomplished: - The sponsor may not start the CT before obtaining the approval from the EC - The sponsor must submit a valid request for authorization to the MS in which the sponsor plans to conduct the CT - In the case of non-acceptance, the sponsor may on one occasion only amend the content of the request. - MS must answer the request as rapidly as possible and may not exceed 60 days	Art. 9 2001/20/EC
Conduct of a clinical trial	MS, sponsor	The sponsor must, within 90 days of completion of the clinical trial, duly inform the MSs. MSs on whose territory the CT is performed must enter data extracted from the initial request, amendments as appropriate and the notification at the end of the clinical trial, into a database. The European Medicines Evaluation Agency can, by derogation, make part of the information entered in this database available to the public. A MS must immediately inform the other MS and the Commission whenever: • it suspends or prohibits the trial because the conditions set out in the application cease to be met or because doubts arise as to the safety or scientific justification of the trial; • it is of the opinion that the sponsor or investigator is no longer fulfilling his obligations.	Art. 10 2011/20/EC
Right on the access to health care	Physicians, DS	- The main priority for clinicians shall be to guarantee their patients well being and intervene in the case of risk of adverse effects - An individual has the right to continue with its regular medical attention even though s/he has withdrawn consent	Prin. 3, 4, 6 WMA DoH

Table 2: Good Clinical Practices

6 Appendix A: Definitions

This Appendix contains a set of definitions that are useful to understand the different documents that have been mentioned in this Deliverable. The first group of definitions is related to the scope of the protection of personal data, while the second corresponds to the scope of clinical trials. They define the main concepts, stakeholders, actions and types of data. We have also added other definitions that are particular of a national regulation.

6.1 Definitions Data Privacy and Protection

The following definitions are provided in the Data Privacy Directive, Data Privacy Regulation and the European Data Protection Supervisor Regulation (Art. 2 95/46/EC, Art 2 2016/679 and Art. 2 45/2001/EC respectively).

- 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
- 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
- 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
- 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
- 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
- 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
- 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
- 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

The E-Data Privacy Directive adds the following definitions to the previous set (Art. 2 58/2002/EC):

- 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;
- 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;
- 'location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;
- 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;
- 'call' means a connection established by means of a publicly available telephone service allowing two-way communication in real time;
- 'consent' by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;

The Data Privacy Regulation expands the definitions provided in the original Directive (Art 2 2016/679):

- 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
- 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- 'pseudoanonymization' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the

physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

- 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- 'main establishment' means: (1) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; (2) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, (3) if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;
- 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;
- 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- 'group of undertakings' means a controlling undertaking and its controlled undertakings;
- 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
- 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;L 119/34 EN Official Journal of the European Union 4.5.2016
- 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because (1) the controller or processor is established on the territory of the Member State of that supervisory authority; (2) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (3) a complaint has been lodged with that supervisory authority;

- 'cross-border processing' means either: (1) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (2) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
- 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
- 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1);
- 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
    - This rule set applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. [Art. 3 95/46/EC]
    - National provisions of each Member State to the processing of personal data shall be applied pursuing compliance with EU directives. [Art. 4 95/46/EC]

6.1.1 Data Protection Act 1998 (United Kindom)

- 'data' means information which
    - is being processed by means of equipment automatically in response to instructions given for that purpose,
    - is recorded with the intention that it should be processed by means of such equipment,
    - is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
    - does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; or
    - is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d);
- 'data controller' means, a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;
- 'data processor', in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;
- 'data subject' means an individual who is the subject of personal data;

- 'personal data' means data which relate to a living individual who can be identified—
  - from those data, or
  - from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

  and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;
- 'processing', in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—
  - organisation, adaptation or alteration of the information or data,
  - retrieval, consultation or use of the information or data,
  - disclosure of the information or data by transmission, dissemination or otherwise making available, or
  - alignment, combination, blocking, erasure or destruction of the information or data;
- 'public authority' means a public authority as defined by the Freedom of Information Act 2000 or a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002;
- 'relevant filing system' means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.
- 'sensitive personal data' means personal data consisting of information as to—
  - the racial or ethnic origin of the data subject,
  - his political opinions,
  - his religious beliefs or other beliefs of a similar nature,
  - whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
  - his physical or mental health or condition,
  - his sexual life,
  - the commission or alleged commission by him of any offence, or
  - any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

6.2 Definitions of Good Clinical Practices.

This second set of definitions are included in the Clinical Trial Directive (Art. 2 2001/20/EC)

- 'clinical trial': any investigation in human subjects intended to discover or verify the clinical, pharmacological and/or other pharmacodynamic effects of one or more investigational medicinal product(s), and/or to identify any adverse reactions to one or more investigational medicinal product(s) and/or to study absorption, distribution, metabolism and excretion of one or more investigational medicinal product(s) with the object of ascertaining its (their) safety and/or efficacy. This includes clinical trials carried out in either one site or multiple sites, whether in one or more than one Member State;
- 'multi-centre clinical trial': a clinical trial conducted according to a single protocol but at more than one site, and therefore by more than one investigator, in which the trial sites may be located in a single Member State, in a number of Member States and/or in Member States and third countries;
- 'non-interventional trial': a study where the medicinal product(s) is (are) prescribed in the usual manner in accordance with the terms of the marketing authorisation. The assignment of the patient to a particular therapeutic strategy is not decided in advance by a trial protocol but falls within current practice and the prescription of the medicine is clearly separated from the decision to include the patient in the study. No additional diagnostic or monitoring procedures shall be applied to the patients and epidemiological methods shall be used for the analysis of collected data;
- 'investigational medicinal product': a pharmaceutical form of an active substance or placebo being tested or used as a reference in a clinical trial, including products already with a marketing authorisation but used or assembled (formulated or packaged) in a way different from the authorised form, or when used for an unauthorised indication, or when used to gain further information about the authorised form;
- 'sponsor': an individual, company, institution or organisation which takes responsibility for the initiation, management and/or financing of a clinical trial;
- 'investigator': a doctor or a person following a profession agreed in the Member State for investigations because of the scientific background and the experience in patient care it requires. The investigator is responsible for the conduct of a clinical trial at a trial site. If a trial is conducted by a team of individuals at a trial site, the investigator is the leader responsible for the team and may be called the principal investigator;
- 'investigator's brochure': a compilation of the clinical and nonclinical data on the investigational medicinal product or products which are relevant to the study of the product or products in human subjects;
- 'protocol': a document that describes the objective(s), design, methodology, statistical considerations and organisation of a trial. The term protocol refers to the protocol, successive versions of the protocol and protocol amendments;
- 'subject': an individual who participates in a clinical trial as either a recipient of the investigational medicinal product or a control;
- 'informed consent': decision, which must be written, dated and signed, to take part in a clinical trial, taken freely after being duly informed of its nature, significance, implications and risks and appropriately documented, by any person capable of

giving consent or, where the person is not capable of giving consent, by his or her legal representative; if the person concerned is unable to write, oral consent in the presence of at least one witness may be given in exceptional cases, as provided for in national legislation.

- 'ethics committee': an independent body in a Member State, consisting of healthcare professionals and non-medical members, whose responsibility it is to protect the rights, safety and wellbeing of human subjects involved in a trial and to provide public assurance of that protection, by, among other things, expressing an opinion on the trial protocol, the suitability of the investigators and the adequacy of facilities, and on the methods and documents to be used to inform trial subjects and obtain their informed consent;
- 'inspection': the act by a competent authority of conducting an official review of documents, facilities, records, quality assurance arrangements, and any other resources that are deemed by the competent authority to be related to the clinical trial and that may be located at the site of the trial, at the sponsor's and/or contract research organisation's facilities, or at other establishments which the competent authority sees fit to inspect;
- 'adverse event': any untoward medical occurrence in a patient or clinical trial subject administered a medicinal product and which does not necessarily have a causal relationship with this treatment;
- 'adverse reaction': all untoward and unintended responses to an investigational medicinal product related to any dose administered;
- 'serious adverse event or serious adverse reaction': any untoward medical occurrence or effect that at any dose results in death, is life-threatening, requires hospitalisation or prolongation of existing hospitalisation, results in persistent or significant disability or incapacity, or is a congenital anomaly or birth defect;
- 'unexpected adverse reaction': an adverse reaction, the nature or severity of which is not consistent with the applicable product information (e.g. investigator's brochure for an unauthorised investigational product or summary of product characteristics for an authorised product).

7 Appendix B: Summary of National Regulations on Data Protection

This summary is extracted from the Practical Law webpage[7], which provides a set of 25 questions regarding Data Protection in each of the EU countries and others. Each National Regulation is analysed by experts of each country.

COUNTRY	ACTIONS
FRANCE	**General laws** The Data Protection Act No. 7817 dated 6 January 1978 (Loi informatique et libertés) (DPA) is the key legislation on the protection of personal data. The DPA created the French Data Protection Authority (Commission Nationale Informatique et Libertés (CNIL). The DPA has been amended several times, in particular by Act No. 2004801 of 7 August 2004. **Sectoral laws** The collection and use of personal data is also subject to special rules set out in the Postal and Electronics Communications Code (Articles L. 341 et seq and Articles R. 1012 et seq.), when such collection and use is carried out in the context of providing electronic communication services to the public. In addition, special rules on privacy and professional secrecy apply to the collection and processing of personal medical data (Articles L. 11104, L. 11118, L. 11123, L. 11213, L. 13433 and L. 21321, Public health Code).
ITALY	**General laws** In Italy, personal data processing is based on and governed by Legislative Decree No. 196/2003, which contains the Italian Personal Data Protection Code (Code), which has implemented Directive 95/46/EC on data protection (Data Protection Directive) into the Italian legal system. Sectoral laws In general, apart from the Code, there are no further specific laws that regulate other areas of data protection. However, certain laws dealing with relevant data protection matters contain some relevant data protection provisions, as well as crossreferences to the Code, including: - **The Workers Statute**. This law establishes several protections for employees. - **Law No. 633/1941.** This law provides for specific rules regarding copyright. - **Legislative Decree No. 81/2008**. This law provides for specific rules regarding health and security in the workplace. - **Legislative Decree No. 206/2005 (Consumers' Code).** This law provides for specific rules regarding consumer protection. - **Legislative Decree No. 70/2003 (E-Commerce Law).** This law expressly establishes mandatory rules directly applicable in the ecommerce field. In addition, the Italian Data Protection Authority (IDPA) is committed to issuing appropriate measures with regard to privacy and personal data protection matters. There are many areas directly regulated by the IDPA, including (but not limited to): - Video surveillance. - Biometric data processing.

[7] http://uk.practicallaw.com/

	- Health data processing. - Data breach notifications. - Bank information processing. - Ehealth records. - Data processing carried out by system administrators. - Data processing for marketing and profiling purposes. - Mobile payment. - Cookies.
SPAIN	**General laws** The Data Protection Act (Law 15/1999 on the protection of personal data) implemented Directive 95/46/EC on data protection (Data Protection Directive). It protects individuals with regard to the processing of personal data and the free movement of data The Regulation developing the Data Protection Act was approved by Royal Decree 1720/2007 of 21 December (Data Protection Regulations). **Sectoral laws** There are no sector-specific laws regulating the processing of personal data, but there are regulations that contain specific provisions on personal data processing (for example, Law 26/2006 on insurance and reinsurance intermediation). The most relevant regulations are the: - Spanish Information Society Services Act (Law 34/2002 on information society services and e-commerce). - Spanish General Telecommunications Act (Law 9/2014). In addition, specific legal provisions apply to the processing of: - Files regulated under the electoral regime legislation. - Files used exclusively for statistical purposes and protected by legislation on public statistical functions. - Files for storing data contained in personal classification reports referred to in the armed forces personnel legislation. - Files derived from the Civil Registry and the Central Registry of Convicts and Fugitives. - Files from video and audio recordings obtained by law enforcement agencies using video cameras.
UK	**General laws** The Data Protection Act 1998 (DPA) and associated secondary legislation implements Directive 95/46/EC on data protection (DP Directive). **Sectoral laws** The key sectoral laws are: - **The Privacy and Electronic Communications (EC Directive)** Regulations 2003 (PECR) (the implementing national legislation for Directive 2002/58/EC on the protection of privacy in the electronic communications sector (e-privacy Directive). - **The Regulation of Investigatory Powers Act 2000 (RIPA),** as amended by the Data Retention and Investigatory Powers Act 2014 (DRIPA) that regulates the interception of communications, access to communications data and the use of surveillance. - A tortious cause of action known as "misuse of private information" has also developed out of the duty of confidentiality (Campbell v Mirror Group Newspapers [2004] UKHL 22).
2. To whom do the laws apply?	
FRANCE	The Data Protection Act (DPA) applies to any person that is in charge of collecting, processing or

	storing personal data and is either a: - **Data controller**. A data controller is any person, public authority, department or any other organisation that determines the purposes and means of the data processing (Article 3, DPA). Whether a person is a data controller is determined on a case-by-case basis. - **Data processor**. A data processor is a person (often a subcontractor) that acts under the authority of the data controller and can only process personal data under the data controller's instructions (Article 35, DPA). A data processor is subject to reduced obligations as set out in Articles 34 and 35 of the DPA. An entity can be considered s a data controller for some of its activities and a data processor for others. For example, an accountant may be considered as a data controller when acting for small and medium-sized enterprises (SMEs) since he receives very few instructions on how to collect or process their data, and therefore enjoys a strong autonomy. However, the same accountant may be considered as a data processor when he acts for large companies that provide him with very detailed instructions on how to process data. In addition, the French Data Protection Authority (Commission Nationale Informatique et Libertés (CNIL) is not bound by the qualification chosen by an entity.
ITALY	The Italian Personal Data Protection Code (Code) provides for guarantees for data subjects and mandatory requirements for those who process personal data. In particular, the requirements provided for by the Code and other regulations apply to both natural persons and legal persons who are in charge of processing personal data. In addition, the Code makes a distinction between data controllers and data processors. **Data controllers** Data controllers have full autonomous decision-making powers regarding the purposes and mechanisms of data processing operations and related security matters. **Data processors** When data processors are selected (under the Code, selecting a data processor is optional for the data controller) they act on behalf of the data controller. Data processors must comply with the provisions that apply to data processing and related security matters.
SPAIN	The Data Protection Act and the Data Protection Regulations apply to data controllers and data processors. See Question 6 for further details on the territorial scope of application. A data controller is any natural or legal person, whether public or private, or administrative body that makes decisions on the purpose, content and use of personal data processing. Data processors process data on behalf of data controllers as a result of a relationship that links them. A data processor's scope for action is limited by the service it provides to the data controller.
UK	The Data Protection Act 1998 (DPA) primarily applies to data controllers. The definition covers those who determine the purposes for which and the manner in which any personal data is to be processed, whether they are acting individually or jointly with others (section 1, DPA). Some provisions of the DPA have general application. For example, certain criminal offences apply to all persons, such as the unlawful procurement or disclosure of personal data (section 55, DPA).
3. What data is regulated?	
FRANCE	The Data Protection Act (DPA) applies to the processing of personal data. Personal data is defined as "any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to them" (Article 2, DPA). This notion is very broad and, therefore, the collection of any data that can

	identify a person, whether directly or indirectly (for example, name, date of birth, phone number, email address, social security number), must comply with the DPA. Personal data include data that are not associated with the name of a person but can easily be used to identify such person and know his habits and tastes. To determine whether a person is identifiable, all the means that the data controller or any other person uses, or may have access to, should be taken into consideration (Article 2, DPA).
ITALY	In general, the Italian Personal Data Protection Code (Code) provides for a very broad definition of personal data. It is defined as any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a personal identification number (Article 4(1)(b), Code). Therefore, personal data can also include information that does not directly provide the identification of a natural person, unless such information has been duly anonymised.
SPAIN	The Data Protection Act and the Data Protection Regulations apply to personal data recorded on physical media for its processing and subsequent use. Personal data is any information relating to an identified or identifiable natural person (known as the data subject).
UK	The Data Protection Act 1998 (DPA) regulates personal data. This is data that relates to a living individual who can be identified either (section 1, DPA): - From that data alone. - From that data and other information which is in the possession of, or is likely to come into the possession of, the data controller. Personal data can include expressions of opinion and indications of intentions. Data covers (section 1 DPA): - Information held, or intended to be held on a computer system. - Information recorded, or intended to be recorded as part of a "relevant filing system". This refers to information that (although not processed automatically by electronic means), is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. - Data that forms part of an "accessible record" (section 68, DPA). This includes: - Health records made by or on behalf of a health professional; - Educational records; - Public records held by local authorities for housing or social services purposes. - All other information held by public authorities.
4. What acts are regulated?	
FRANCE	The Data Protection Act (DPA) applies to any processing of personal data. Processing is defined as any operation or set of operations in relation to such data, regardless of the mechanism used, especially the (Article 2, DPA): Obtaining / Recording / Organisation / Retention / Adaptation or alteration / Retrieval / Consultation / Use / Disclosure by transmission / Dissemination or otherwise making available / Alignment or combination / Blocking / Deletion or destruction. This definition is very broad and, therefore, a simple consultation or the mere archiving of data is considered as processing. The DPA also distinguishes between: - **Nonautomatic processing (manual processing)**. Nonautomatic processing must comply with the DPA. However, it is not subject to the prior notification obligation, provided that the processed data do not relate to sensitive information, offences or convictions (see Question 7). - **Automatic processing**. The definition of automatic system is broad and is not limited to databases, as even processing through simple text editors fall within this definition.
ITALY	The Italian Personal Data Protection Code (Code) covers all personal data processing, that is any

	operation, or set of operations, carried out with or without the help of electronic or automated means, and concerning data (Article 4(1)(a), Code): Collection / Recording / Organisation / Storage / Interrogation / Elaboration / Modification / Selection / Retrieval / Comparison / Utilisation / Interconnection / Blocking / Communication / Dissemination / Erasure / Destruction (regardless of whether the data is contained in a data bank).
SPAIN	The Data Protection Act and the Data Protection Regulations apply to the processing of personal data. Data processing means any operation or procedure (whether automated or not) for the collection, recording, storage, elaboration, modification, blocking or erasure of data. It also includes disclosure of data resulting from communications, queries, interconnections or transfers.
UK	The Data Protection Act 1998 (DPA) regulates the "processing" of personal information. Processing is defined extremely broadly, and extends to obtaining, recording or holding information, or carrying out any operation or set of operations on information (section 1, DPA). The Information Commissioner's Office (ICO) has clarified that it is difficult contemplate anything that an organisation can do with data that will not be processing.
5. What is the jurisdictional scope of the rules?	
FRANCE	The Data Protection Act (DPA) applies to the processing of personal data by a data controller that either is established in France or carries out its activities in an establishment in France, regardless of its legal form. The notion of establishment is not defined in the DPA. However, the French Data Protection Authority (Commission Nationale Informatique et Libertés (CNIL) considers that there is an establishment where there is an effective and real exercise of an activity through stable facilities. If the data controller is not established in France or in any other EU member states, but uses means of processing that are located in the French territory (with the exception of processing used only for the purposes of transit through France or any other EU member states), the processing will also fall within the scope of the DPA. Means of processing are located in France if: - Data is collected in France. - The hosting server is located in France. - The external service provider is located in France. At the European level, the control of, and coordination between, the national data protection authorities are organised under Directive 95/46/EC on data protection (Data Protection Directive). Under Article 29 of the Directive, a working group called "G29", which is composed of representatives of the national data protection authorities, the European data protection supervisor and the EuropeanCommission was established for national authorities to provide expert advice to the European Commission and to promote the uniform application of the Data Protection Directive in all member states. Based on this coordination, a data controller that processes personal data in several member states will be controlled by the authority of the member state where it is established. If the data controller is not established in France or the EU, it must designate a representative before the CNIL.
ITALY	The Italian Personal Data Protection Code (Code) applies to the processing of personal data (including data held abroad) where the processing is performed by any entity established in Italy or in a place that is under the Italian state's sovereignty. The Code also applies to the processing of personal data that is performed by an entity established in a country outside the European Union (EU). This is where an entity uses (in connection with the processing equipment), whether electronic or otherwise that is situated in Italy. This is unless the equipment is used only for purposes of transit through the territory of the EU. In such a case, if the Code applies, the data controller must designate a representative established in Italy to implement the provisions relating to the processing of personal data
SPAIN	The Data Protection Act and the Data Protection Regulations apply to:

	- Data processing carried out in the context of the activities of an establishment of the data controller in Spain. Where this is not the case, but the data controller uses a data processor established in Spain, the data processor must comply with the provisions on security measures established in the Data Protection Regulations. - Data processing carried out by a data controller not established in Spain but in a place where Spanish law applies by virtue of international public law. - Data processing carried out by a data controller not established in the European Union but using means located in Spain, unless such means are used only for transit purposes. In this case, the data controller must appoint a representative established in Spain.
UK	The Data Protection Act 1998 (DPA) applies to data controllers that are established in the UK. Persons considered to be established include: - Ordinarily resident individuals. - UK registered companies. - Partnerships and unincorporated associations governed by UK law. - Bodies that maintain an office, branch, agency, or regular practice in the UK. Data Controllers who are not established within the European Economic Area (EEA), but use equipment in the UK to process the data (other than for the purposes of domestic transit) must also: - Comply with the DPA. - Appoint a representative established in the UK.
6. What are the main exemptions (if any)?	
FRANCE	The Data Protection Act (DPA) does not apply to processing carried out for the exercise of exclusively private activities (Article 2, DPA). This applies to private phone books. In addition, the DPA does not apply to temporary copies made in the context of technical operations of transmission and provision of access to a digital network for the purpose of automatic, intermediate and transitory retention of data, and with the sole aim of allowing other recipients of the service to benefit from the best access possible to the transmitted information (Article 4, DPA).
ITALY	In general, the Italian Personal Data Protection Code covers all sectors and areas of data protection. However, in certain cases, specific rules apply to certain sectors and organisations, for example, rules applying to: - Public bodies. - State defence and security matters. - Healthcare professionals and public healthcare bodies. The Code expressly provides for certain specific exemptions from general data protection requirements, in particular regarding data processing by the police and in relation to other state defence and security matters.
SPAIN	Data protection law does not apply to: - Data files maintained by natural persons exclusively for personal or domestic activities. - Data files subject to the protection of classified matters. - Data files created to investigate terrorism and serious organised crime.
UK	The main exemptions are contained in part IV of the Data Protection Act 1998 (DPA). They apply only to the extent that the relevant DPA obligations are likely to prejudice the fulfilment of the exemption's purpose. This must be judged on a case-by-case basis. The following are the main purposes of exemption: - Data processing solely for personal or domestic purposes (section 36, DPA). It exempts:

	- compliance with data protection principles; - all rights of data subjects; and - Information Commissioner's Office (ICO) notification requirements. - Data processing for the purposes of detecting crime, the capture/prosecution of offenders and for the assessment/collection of tax (section 29, DPA). It exempts: - compliance with the first data protection principle (although controllers must still comply with Schedule 2 and 3 requirements (that is, the need for a lawful basis for processing)); - compliance with the second, third, fourth and fifth data protection principles (data quality, retention limitation, purpose limitation); - data subject rights to make access requests and object to processing; requirement to give privacy notices; and - data subject rights, in certain circumstances, to have inaccurate personal information rectified, blocked, erased or destroyed. - Data processing in the interests of national security (section 28, DPA). This exempts: - compliance with data protection principles; - all rights of data subjects; - notification requirements; and - DPA enforcement provisions. - Processing required by law or in connection with legal proceedings (section 35, DPA). This exempts: - provisions in the Act that would restrict data from being disclosed. - Processing in respect of "regulatory activities" carried out as core functions of entities engaged in key public functions (section 31, DPA). This exempts the: - obligation to provide privacy notices; and - data subject rights to make subject access requests. - Processing personal data for the purposes of art, literature and journalism with a view to publication in the public interest (section 32, DPA). This exempts: - compliance with the data protection principles (except principle seven (security)); - data subject rights to make a subject access request; - data subject rights to object to processing likely to cause damage or distress and automated decision making; and - data subject rights, in certain circumstances, to have inaccurate personal information rectified, blocked, erased or destroyed. - Data which organisations are legally obliged to make publically available (other than under the Freedom of Information Act (FOIA)). This exempts: - the duty to provide information notices; - the data subjects' rights to make subject access requests; compliance with the first to fifth data protection principles (although controllers must still comply with Schedule 2 and 3 requirements); and - the individual's rights to (in certain circumstances) have inaccurate information rectified, blocked, erased or destroyed. In addition, there are further (more limited) exemptions are found in Schedule 7 of the DPA.
7. Is notification or registration required before processing data?	
FRANCE	Before processing data, the data controller must either notify the French Data Protection Authority (Commission Nationale Informatique et Libertés) (CNIL) or obtain authorisation from the CNIL. **Notification regime** The notification regime applies to automatic processing only (see Question 4). The notification can

	be normal or simplified. ***Normal notification (déclaration ordinaire).*** This is the general regime that applies to any personal data processing. The notification form must include the following information: - Purpose(s) of the processing. - Identity and address of the data controller. - Possible interconnections between databases. - Personal data processed and categories of persons concerned by the processing. - Recipient(s) or categories of recipients of the processed data. - Time period for which the data will be kept. - Department or person(s) in charge of data processing. - Persons or departments before which the right of access is exercised. - Countries where the data will be sent, stored, used and/or processed (if outside the EU). - Measures taken to ensure the security of the processing. The applicant can start the processing as soon as it receives the acknowledgement of notification (récépissé). Under the Data Protection Act (DPA), the CNIL must deliver the acknowledgement "without delay" after the notification. In practice, it is delivered within a few days or a few weeks. If the notification is submitted through the CNIL's website, the acknowledgement is normally received within a couple of days after the notification. ***Simplified notification (déclaration simplifée).*** This applies to the most common forms of processing. In such cases, the data controller only needs to confirm that the processing complies with certain standards set in advance by the CNIL (for example, standards of data processing by a company to geolocate the vehicles used by its employees). Each set of standards describe the purpose of the treatment, the type of personal data processed, the recipient of the data, the time period for which the data are kept and the compliance with the rights of the data subjects. If no such standards apply, the data controller must submit a normal notification (see above). **Authorisation regime** Article 25 of the DPA sets a list of data processing, whether automatic or not, which are subject to prior authorisation. This regime concerns processes and data that could be particularly harmful to privacy and civil liberties, including: - The processing of sensitive data. - The processing of genetic data. - The processing of data relating to offences and security measures. - Biometric identity checks. - The transfer of data outside the EU to a country without adequate protection (see Question 20). The CNIL must make a decision within two months, renewable once. If the CNIL does not make a decision, the authorisation is deemed to be refused. A tacit or explicit refusal can be appealled before the French Supreme Administrative Court (Conseil d'Etat). The CNIL has also developed a simplified system of "unique authorisation" on the same lines as the simplified notification regime (see above, Notification regime: simplified notification (déclaration simplifée)). The unique authorisation regime applies to situations listed on the CNIL's website (for example, data processing relating to the whistleblowing system). A specific authorisation regime applies to data processing in the medical sector.
ITALY	**Notification** Under the Italian Personal Data Protection Code (Code), data controllers must notify the Italian Data Protection Authority (IDPA) when they process the following types of data (among others)

(Article 37, Code):
- Genetic and biometric.
- Geolocalisation.
- Behavioural advertising.

The notification must be provided before the data controller starts to process the data. The data controller can start to process the data as soon as the notification has been completed. The IDPA expressly established cases of exemption from the notification obligation through a general resolution issued in 2004.

Exemptions
Letter (a) of Article 37 of the Code provides for mandatory notification for processing genetic data, biometric data, or other data that discloses the geographic location of individuals or objects by means of an electronic communications network. However, the IDPA determined that this notification requirement will not apply to:
- Nonsystematic processing operations of genetic and/or biometric data carried out by health care professionals, acting as controllers of such processing operations, concerning data that is not organised in a data bank accessible to third parties via electronic networks. This provision only applies to such data and operations, including communication, that are necessary for the purpose of safeguarding the data subjects' and/or third parties' health.
- Processing of genetic and/or biometric data that is necessary as part of a legal operation to assist with investigations by defence counsel, as provided in Act No. 397/2000, and ultimately to establish or defend a legal claim that concerns a third party. This is on the condition that the claim is not overridden by the data subject's claim and that the data has been processed for the original purpose and for no longer than is absolutely necessary.
- Processing of data that discloses the geographic position of air, sea, and ground transportation channels, where it is only carried out for the purpose of transportation security.

Letter (d) of Article 37 of the Code provides for data that is processed with the help of electronic means and with the aim of profiling the data subject and/or his personality, analysing consumption patterns and/or choices, or monitoring the use of electronic communications
services. This is except for processing operations that are technically indispensable to deliver the services to users. The IDPA has determined that this notification requirement will not apply to the processing of personal data:
- That is not grounded exclusively on an automated processing operation aimed at defining professional profiles, where the processing is carried out exclusively for occupational purposes or else for the purpose of managing the employeremployee relationship. This is except for the cases referred to in Letter (e) of Article 37(1) (see below).
- That is not grounded exclusively on an automated processing operation aimed at defining an investor's profile, where the processing is carried out exclusively in order to fulfil specific obligations set out in financial brokerage legislation.

Letter (e) of Article 37 of the Code provides for sensitive data stored in data banks for personnel selection purposes on behalf of third parties. This is in addition to sensitive data used for opinion polls, market surveys and other samplebased surveys. The IDPA has determined that the notification requirement will not apply to the processing of sensitive data carried out:
- For the sole purpose of personnel selection exclusively on behalf of entities belonging to the same company and/or banking group.
- By public entities exclusively in order to fulfil specific obligations and/or duties as set out in

	employment and/or labour market legislation. - By trade associations and/or organisations for the sole purpose of carrying out sample surveys with regard to data concerning membership of such associations and/or organisations. Letter (f) of Article 37 of the Code provides for data that is stored in ad hoc data banks managed by electronic means in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct. The IDPA has determined that the notification requirement will not apply to the processing of personal data: - Carried out by public entities to keep public registers or publicly available lists. That is stored in data banks used to keep in touch with a data subject in connection with the provision of goods or services, or else to comply with accounting and/or tax requirements as also related to breach of contract, factoring of receivables and litigations involving the data subject. That is stored in data banks used by public and/or private entities exclusively to fulfil regulatory obligations concerning employment, social security, or assistance. - That are stored in data banks used by public bodies exclusively with a view to keeping and executing instruments, provisions and documents as related to the levying of taxes, imposition of administrative sanctions, or granting of licences, concessions, and authorisations. - Related to images and/or sound as temporarily stored for the sole purpose of securing and/or protecting individuals and/or property.
SPAIN	Registration of personal data files is required before processing. Data controllers must register their data files with the General Data Protection Registry. The Data Protection Act and the Data Protection Regulations define data files as sets of structured personal data that can be accessed according to specific criteria, regardless of how the data is generated, stored, organised or accessed. One data file can be composed of several databases (whether automated or nonautomated). Registration is completed through a standard notification form available on the Data Protection Agency's website. Data controllers must complete this form describing, among other aspects: - The purposes of the data file. - The categories of personal data it contains. - Any data disclosures. - The security level applied to the personal data. - Any international transfer to third countries. Registration must be updated whenever there are changes to the data files affecting the information notified to the Data Protection Agency (including removal of the data file).
UK	Data controllers are required to file specific information with the Information Commissioner's Office (ICO). This includes: - The data controller's name and address. - A description of the relevant personal data. - The purposes for which the data will be processed. - The ICO maintains a register of data controllers that is searchable by the public. There are limited exemptions to this requirement, including: - Organisations that only process personal data for standard business processes, such as staff administration, business relatedadvertising/marketing and accounts. - Certain not-for-profit organisations that meet the necessary selfassessment criteria. - Organisations that do not process personal information on a computer.

8. What are the main obligations imposed on data controllers to ensure data is processed properly?	
FRANCE	Data controllers' main obligations are listed in Article 6 of the Data Protection Act (DPA). The data controller must ensure that: - Data are collected and processed fairly and lawfully. - Data are collected for specified, explicit and legitimate purposes and are subsequently processed in a manner that is compatible with such purposes. - Personal data are adequate, relevant and not excessive in relation to the purposes for which they were collected. - Collected personal data are accurate, complete and kept uptodate. - Collected personal data are retained in a form that allows the identification of the data subjects for a period that is no longer than necessary for the purposes for which they were collected. In addition, data controllers must ensure that the individuals concerned are informed, have given their consent, and have the right to access the data and request amendments or deletions.
ITALY	The Italian Personal Data Protection Code (Code) provides for the following main obligations: - Personal data must be processed with respect for the data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection. - Information systems and software must be configured by minimising the use of personal data and identification data. This must be done in a way that prohibits their processing if the purposes for processing can be achieved by using either anonymous data or providing suitable arrangements to allow the identification of data subjects only in necessary cases. - Personal data processing must be: - processed lawfully and fairly; - collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with the original purpose; - accurate and, where necessary, kept up to date; - relevant, complete and not excessive in relation to the purposes for which the data is collected or subsequently processed; - kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which the data is collected or subsequently processed; - commenced only if data subjects have been previously informed about the processing; and - commenced only if the data subjects have given their consent (see Question 9).
SPAIN	Under the Data Protection Act and the Data Protection Regulations, data controllers must comply with several obligations, including: - Complying with the principles of data quality. - Informing data subjects about data processing on collection. - Obtaining data subjects' consent to process their data. - Registering personal data files. - Implementing security measures to protect personal data, including drafting a security document. - Attending to data subjects' rights of access, rectification, cancellation and opposition. - Entering into data processing agreements with data processors. - Keeping personal data confidential.
UK	The Data Protection Act 1998 (DPA) is founded on eight fundamental principles (Data Protection Principles). All data controllers (unless subject to an exemption) must comply with these principles when processing personal data. The Data Protection Principles are set out in Part 1, Schedule 1 of the DPA and require that personal data must be: - Processed fairly and lawfully, meeting at least one of the conditions in Schedule 2 of the DPA. For sensitive personal data, at least one of the conditions in Schedule 3 of the DPA must also be fulfilled.

	- Obtained only for one or more specified and lawful purposes, and not be further processed in any manner incompatible with that purpose or those purposes. - Adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed. - Accurate and, where necessary, kept up to date. - Kept for no longer than is necessary for that purpose or those purposes. - Processed in accordance with the rights of data subjects under the DPA. - Safeguarded by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. - Protected from transfer to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to its processing.
9. Is the consent of data subjects required before processing personal data?	
FRANCE	Article 7 of the Data Protection Act (DPA) expressly provides that the consent of data subjects is required before collecting and processing personal data. The DPA does not contain any provision on the form and content of consent, and on evidence of such consent. As a basic principle, consent must be obtained in accordance with the loyalty principle. Therefore, preticked boxes cannot constitute a valid consent. Article 7 also lists exceptional circumstances in which consent of the data subject is not required (see Question 10). Personal data processing regarding individuals under the age of 18 is subject to specific conditions. According to the French DPA (CNIL), the data controller must receive the consent of the parents and must provide clear information to the minor. Data controllers are not allowed to collect a minor's sensitive personal data. The CNIL also indicates that, to send a newsletter to a minor, data controllers can only collect his email address and age. Any further information on the minor's family, consumer habits, parents' situation is considered disproportionate and unfair. Under Article 226181 of the French Criminal Code, processing data despite the objection of the data subject is a criminal offence punished by five years' imprisonment and/or a fine of EUR300,000.
ITALY	As a general principle, the Italian Personal Data Protection Code (Code) provides that personal data processing carried out by private entities or for-profit public bodies is only allowed if the data subject gives his express consent. This can refer to the processing as a whole or to one or more of the processing operations. In addition, the consent is only effective if: - It is given freely and specifically with regard to a clearly identified processing operation. - It is documented in writing. - The data subject has been given the proper information as provided in section 13 of the Code relating to data subjects (section 23, Code). The data subject's consent must be in writing if the processing concerns sensitive data. Consent to the data processing can also be given online. A person under 18 years of age cannot give valid consent, and a parent or legal guardian must give the consent on behalf of the minor.
SPAIN	As a rule, consent from data subjects is required. Consent must be informed (see Question 12). Depending on the circumstances, it can be implied, express (for example, for health data) or written (for example, for data revealing ideology). Unless the law requires express consent, the Data Protection Regulations establish that data controllers can inform data subjects of the processing they intend to carry out and give them 30 days to oppose it. This way of obtaining consent is subject to limitations (for example, a data controller cannot request the same consent again until a year has passed).

UK	**General principle** A data controller can only process personal data if one of the conditions set out in Schedule 2 of the DPA 1998 can be satisfied. Consent is the first condition that is listed. However, other conditions can be used to justify processing (see Question 10) and the fact that consent is listed first in Schedule 2 of the DPA does not mean that data controllers must look for consent ahead of other conditions. **Formal requirements** There are no formal DPA requirements relating to consent. Implied consent is acceptable, unless sensitive personal data is processed (see Question 11). Therefore, consent can also be given online. The Information Commissioner and the courts will have regard to the definition of consent in Directive 95/46/EC on data protection (DP Directive) when considering if consent is valid. The Directive provides that consent is any freely given specific and informed indication of wishes by which the data subject signifies his agreement.
10. If consent is not given, on what other grounds (if any) can processing be justified?	
FRANCE	If the data controller has not received the consent of the data subject, processing can be justified on any of the following grounds: - Compliance with any legal obligation to which the data controller is subject. - Protection of the data subject's life. - Performance of a public service mission entrusted to the data controller or the data recipient. The processing relates to the performance of a contract to which the concerned individual is a party or of pre-contractual measures requested by that individual. - Processing the data is in the legitimate interests of the data controller or data recipient, subject to the interests and fundamental rights and liberties of the concerned individual.
ITALY	Under the Italian Code there are specific cases in which the processing of data can be carried out without obtaining the data subject's consent, including if it is: - Necessary to comply with an obligation imposed by a law, regulation or community legislation. - Necessary for the performance of obligations resulting from a contract to which the data subject is a party. - Concerns data taken from public registers, lists, documents or records that are publicly available, without prejudice to the limitations laid down by laws, regulations and community legislation regarding their disclosure and publicity. - Necessary to safeguard life or prevent injury to a third party. - Necessary for carrying out investigations by defence counsel. - Additional derogatory hypothesis are provided for in Articles 24 and 26 (for sensitive data) and other specific sections of the Code.
SPAIN	Data subjects' consent is not required when: - Data is collected by a public administration when exercising its functions. - Data refers to the parties to an administrative, employment or business contract or precontract, provided the data is necessary for its performance. - The purpose of the data processing is to protect the data subject's vital interest. - The data processing is necessary to satisfy a legitimate interest pursued by the data controller (or a third party to whom the data is disclosed), provided that the data subject's fundamental rights and freedoms are not overridden.
UK	Personal data can also be processed where the processing is: - Contractually necessary, that is, where it is necessary for the performance of a contact with the individual, or to take steps at the request of the individual with a view to entering into a contract. Necessary to comply with another noncontractual legal obligation of the data controller. - Necessary for the:

	- administration of justice; - the functions of either House of Parliament; - the exercise of statutory functions; - the exercise of functions of the Crown, a Minister or a government department; or - for the exercise of other functions of a public nature exercised in the public interest. - Necessary for the legitimate interests of the data controller (or a third party to whom personal data will be disclosed). This is except where it is unwarranted because it is prejudicial to the individual.
11. Do special rules apply for certain types of personal data, such as sensitive data?	
FRANCE	The DPA contains special rules for certain types of personal data, namely: - Sensitive data. - Social security numbers. - Data relating to offences, convictions and security measures. In principle, the collection and processing of sensitive data is prohibited. Sensitive data is data that reveal, directly or indirectly, a persons' racial and ethnic origins, political, philosophical, religious beliefs or opinions, trade union affiliation, health or sexual life. This prohibition does not apply to the processing of sensitive data which is: - Based on the express consent of the data subject. - Necessary for the protection of human life when the data subject is unable to give his consent because of a legal incapacity or physical impossibility. - Carried out by an association or any other nonprofit religious, philosophical, political or trade union body, provided that the processing relates to the object of the organisation, is limited to its members and the data collected are not transmitted to third parties, unless such transfer was expressly approved. - Based on data that have been made public by the data subject. - Necessary for the establishment, exercise or defence of a legal claim. - Necessary for healthcare. - Carried out for statistical purposes by the National Institute of Statistics and Economic Studies or one of the statistical services of the ministries. - Necessary for medical research. The processing of data relating to offences, convictions and security means is governed by Article 9 of the DPA. Regarding the processing of social security numbers, the French DPA CNIL has established a strict control regime, since social security numbers can provide access to a significant number of personal data and connection possibilities on many databases.
ITALY	The Italian Code and some important guidelines issued by the Italian Data Protection Authority (IDPA) provide more stringent rules when the processing refers to (among other things): - Sensitive data. - Biometric data. - Banking details. - The personal data of employees that is processed in the context of employment. - Mobile payments. The Code establishes that sensitive data can only be processed with the data subject's written consent and the IDPA's prior authorisation, and by complying with the prerequisites and limitations set out in the Code (Article 26(1), Code). The IDPA issues (generally on an annual basis) nine general authorisations most of which are related to sensitive data processing for specific sectors. Data that discloses health information cannot be distributed. Other specific rules are expressly provided for

	by both the Code and general resolutions issued by the IDPA with particular regard to the: - Biometric data processing. - Processing of personal data in the health care sector. - Data processing carried out in the context of employment. - Bank information processing. - Processing of data in relation to mobile payments. - Processing of personal data by using cookies. - Online profile.
SPAIN	Special rules apply to certain types of data, particularly to sensitive data. Sensitive data includes the following categories: - Ideology, trade union membership, religion and beliefs. As a rule, this data can only be processed with the data subject's express written consent. - Racial origin, health and sex life. As a rule, this data can only be processed on general interest grounds established by law, or with the data subject's express consent. - Data related to administrative or criminal infringements, which can only be processed by the competent public administrations. Data on ideology, trade union membership, religion, beliefs, racial origin, health and sex life can be processed when necessary for medical prevention or diagnosis, providing healthcare or medical treatment, or managing health services, provided that the processing is carried out by a healthcare professional bound by professional secrecy, or any another person subject to an equivalent obligation. This data can also be processed when necessary to protect a vital interest of the data subject or other person if the data subject is physically or legally unable to give consent. As a rule, data on ideology, trade union membership, religion, beliefs, racial origin, health and sex life is subject to the highlevel security measures established by the Data Protection Regulations.
UK	Sensitive personal data is personal data consisting of information as to (section 2, DPA): - Racial or ethnic origin. - Political opinion. - Religious or similar belief. - Membership of a trade union. - Physical or mental health or condition. - Sexual life. - Commission or alleged commission of an offence. - Proceedings for an offence, the disposal of proceedings and the related sentence. Sensitive personal data can be processed with the explicit consent of the individual. Alternatively, sensitive personal data can be processed where the processing is: - Necessary in connection with employment law obligations. - Necessary to protect the vital interests of the data subject, or, in certain situations, another person. C- arried out in the course of legitimate activities by a non-profit body, which exists for political, philosophical, religious or trade union purposes. - Personal data that has been made public as a result of steps deliberately taken by the data subject. - Necessary in connection with legal proceedings, to obtain legal advice or is otherwise necessary to establish, exercise or defend legal rights. - Necessary for statutory, parliamentary, legal or government functions - Being carried out in connection with certain antifraud organisations.

	- For medical purposes and processed by a health professional or someone subject to equivalent duties of confidentiality. - Carried out in the context of a properly conducted equality monitoring programme. Additional conditions when sensitive data may be processed are set out in secondary legislation. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) sets out additional restrictions on the processing of traffic and location data by certain communications service providers.
12. What information should be provided to data subjects at the point of collection of the personal data?	
FRANCE	At the point of collection of personal data, the data controller must inform data subjects of: - The identity of the data controller and its representative (if any). - The purpose of the processing. - Whether replies to questions are compulsory or optional. - The recipients or categories of recipients of the data. - The right to object, for a legitimate purpose, to the collection of such data. - The right to access the collected data. - The right to have the processed data rectified, completed, blocked or deleted. - Where data are to be transferred outside the EU, specific details on the intended transfer (that is, where, why, what data and under which level of protection). The information obligation can be fulfilled orally or in writing. However, it is recommended to use a written document for evidentiary purposes. Under Article 32 of the Data Protection Act (DPA), the information obligation can be reduced or set aside in specific circumstances.
ITALY	The data subject must be informed before the collection of data (either orally or in writing) about the: - Purposes of the processing for which the data is intended. - Voluntary or involuntary nature of providing the requested data. - Consequences in cases of failure to reply. - Entities or categories of entity to whom the data may be communicated, or who may get to know the data in their capacity as data processors, and the scope of dissemination of the data. - Rights recognised by the applicable law. - Identification of the data controller and, where designated, the data controller's representative in Italy.
SPAIN	When collecting personal data, data subjects must be informed of: - The existence of a data file or data processing. - The data controller's identity and address (or that of its representative if the processing is carried out by a data controller not established in the EU but using means located in Spain, unless such means are used only for transit purposes). - The purpose of the processing. - The data recipients, identifying them by name and address and specifying the purpose of the data transfer. - How the data subject can exercise his rights of access, rectification, cancellation and opposition. - Whether answering the questions is mandatory or voluntary (unless the information can be clearly inferred from the nature of the personal data requested or the circumstances in which the data is collected). - The consequences of providing the data or refusing to do so (unless the information can be clearly inferred from the nature of the personal data requested or the circumstances in which the data is collected).
UK	Certain prescribed information must be given to the relevant data subject in advance (section 7,

	DPA 1998). Where data is not provided directly from the data subject, notification must follow as soon as practicable after processing. The statement must include: - The name of the data controller (or their nominated UK representative if they are not based in the UK). - The purposes of the processing. - Any further information required so that the processing will be fair in all the circumstances. The latter requirement is intentionally flexible. Data controllers must consider the nature of the personal data held and the reasonable expectations of the data subjects. It may be necessary, for example, to inform them of any potential third party recipients of the data and the existence of the right to access or amend the data. The Information Commissioner's Office has issued a "Privacy Notices Code of Practice" to guide organisations in this area.
13. What other specific rights are granted to data subjects?	
FRANCE	Rights of individual data subjects are set out in Articles 38 to 43 of the Data Protection Act (DPA). A natural person is entitled, on legitimate grounds, to object to the processing of its personal data, unless the processing satisfies a legal obligation (Article 38, DPA). The data subject is entitled to obtain from the data controller (Article 39, DPA): - Confirmation as to whether its personal data are part of the processing. - Information relating to the purposes of the processing, the categories of processed data and the recipients or categories of recipients to whom the data are disclosed. - Information relating to the transfer of personal data outside the EU, if applicable. - A copy, in an accessible form, of its personal data, as well as any available information on the origin of the data. - Information allowing the data subject to know and object to the reasoning involved in the processing, where a decision based on automatic processing produces legal effects in relation to the data subject. A data subject can request the data controller to rectify, complete, update, block or delete personal data (Article 40, DPA) (see Question 14). However, the rights of access and rectification are limited when the processing involves state security, defence or public safety (Article 41, DPA).
ITALY	Under Article 7 of the Italian Code data subjects must be informed of the: - Source of personal data. - Purposes and methods of the processing. - Logic applied to the processing. - Identification of the data controller. - Data processor and data controller's representative (if any). - Entities and subjects to whom personal data can be communicated. - Data subjects must have the right to: - Update, rectify or integrate the data. - Erase, anonymise or block the data that has been processed illegally, including data that was retained for different purposes than what it was collected for. - Receive certification from the entities to whom the data was communicated, that the above processes have been complied with (unless this requirement proves impossible or involves a manifestly disproportionate effort compared to the right that is to be protected). Data subjects also have the right to object, in whole or in part: - On legitimate grounds, to the processing of his personal data, even if relevant to the purpose of the collection. - To the processing of his personal data, where it is carried out for the purpose of sending

	advertising materials or direct selling for the performance of market or commercial communication surveys.
SPAIN	Data subjects have the following rights: - Right of access. Data subjects are entitled to request information on whether their personal data is processed, the purpose of the processing, the source of their data and any data transfers, as well as information on specific data, data included in a specific file, or all the data that is subject to processing. - Right to rectify incomplete or inaccurate data. - Right of cancellation. Data subjects can request deletion of inappropriate or excessive data (see Question 14). - Right to oppose the data processing in specific scenarios established by law (for example, to oppose receiving commercial communications). - Right to challenge decisions that have a legal effect on them or that affect them significantly when the decision is exclusively based on automated data processing carried out to evaluate aspects of their personality (for example, work performance and credit). - Right to consult the General Data Protection Registry. - Right to claim protection of their rights from the Data Protection Agency when they have been denied by the data controller. - Right to be indemnified for damages caused by infringement.
UK	A data subject has the right to access his data. This right is commonly referred to as subject access (section 7 and 8, DPA 1998). Data subjects have the right to be: - Told whether any of their personal data is being processed. - Given a description of the data, the reasons it is being processed and the possibility of it being passed to a third party. - Given a copy of the data. - Given details of the source of the data. - Data subjects also have certain rights to object to the processing of their data: - **Marketing**. Data subjects can prevent processing for marketing purposes (section 11, DPA). - **Automatic processing**. Data subjects can also (in writing) require that a data controller ensures that no processing decision that significantly affects them is based solely on automatic processing. This does not apply where the decision is made in relation to the performance of or entry into a contract and the effect of the decision is to grant a request of the individual or safeguards are in place to protect the legitimate interests of the data subject.
14. Do data subjects have a right to request the deletion of their data?	
FRANCE	Under Article 40 of the DPA, data subjects can request the data controller to rectify, complete, update, block or delete their personal data that are inaccurate, incomplete, equivocal, expired, or whose collection, usage, disclosure or retention is prohibited. The right to be forgotten was recognised by the European Court of Justice (ECJ) in *Google Spain SL, Google Inc v Agencia Española de Proteccion de Datos and Mario Costeja Gonzalez (case C131/ 12).* This right is expressly mentioned in the draft data protection regulation that is being discussed before the EU Council. Under the right to be forgotten, people can request an internet search engine to remove the links to web pages that contain inaccurate and damaging information. However, this right is not absolute and will be assessed on a case-by-case basis in light of the right to freedom of expression and information, particularly in the case of public figures.
ITALY	Data subjects do have the right to request the deletion of their data (see Question 13).
SPAIN	Data subjects have a right to request the deletion of their data. Data controllers must cancel personal data when it is no longer necessary or relevant to the purpose for which it was collected. Cancellation means that the data cannot be used and must be blocked to impede its processing. It is kept available for public administrations, judges and courts to deal with any liabilities resulting from

	the processing until these liabilities expire. After any applicable liabilities expire, the data must be deleted.
UK	Data subjects have the right to apply to the courts for an order that inaccurate data is rectified, blocked, erased or destroyed (section 14, DPA 1998). They can also prevent a data controller from processing personal data where such processing causes or is likely to cause unwarranted substantial damage or distress (section 10, DPA).
15. What security requirements are imposed in relation to personal data?	
FRANCE	The data controller must take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by nonauthorised third parties (Article 34, Data Protection Act (DPA)). The French Data Protection Authority (CNIL) considers that the data controller must implement any security measure that is adapted to the nature of the processed data and the risks of the processing. In 2012, the CNIL published an advanced guide on identification of risks and best practices for security measures[8]. The CNIL recommended security measures and guarantees, such as: - Strong password management. - Secure workstations. - Identification tools. - Secure local network. - Secure physical access. - Training users on information technology risks. The processing of personal data without implementing the required security measures can be subject to five years' imprisonment and/or a fine of EUR300,000 (Article 22617, French Criminal Code).
ITALY	Under Article 33 of the Italian Code data controllers are required to adopt certain minimum security measures. **Personal data processing carried out through electronic means.** The following minimum security measures must be adopted: - Computerised authentication. - Implementation of authentication credentials management procedures. - Use of an authorisation system. - Regular update of the specifications concerning scope of the processing perations that may be performed by the individual entities. - Protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software. - Implementation of procedures for safekeeping backup copies and restoring data and system availability. - Implementation of encryption techniques or identification codes for specific processing operations performed by healthcare bodies in respect of data about health and sex life. **Personal data processing carried out without electronic means** The following minimum security measures must be adopted: - Regular update of the specifications concerning scope of the processing operations that may be

8 www.cnil.fr/linstitution/actualite/article/article/deuxnouveauxguidessecuritepourgererlesrisquessurlavieprivee/

	performed by the individual entities. - Implementing procedures, for example, safekeeping the records and documents committed to the entities in charge of the processing. - Implementing procedures to keep certain records in restrictedaccess filing systems and regulating access mechanisms with a view to enabling the identification of the entities in charge of the processing. Under the Code, data controllers must also do the following: - Appoint persons to be in charge of the processing. - Appoint data processors (if any). - Appoint system administrators. - Create company policies, on topics such as: - video surveillance; - use of the Internet and email; - use of company password policy.
SPAIN	Data controllers and data processors must implement security measures to protect personal data against accidental or unlawful destruction, accidental loss, alteration or unauthorised disclosure or access. The Data Protection Regulations set out specific minimum security measures to be implemented by controllers and processors, establishing three cumulative security levels: basic, medium and high. The applicable measures depend on the nature of the data (for example, sensitive data is subject to all three levels of security). The security measures established by the Data Protection Regulations include specifications on: - Access control. - Identification and authentication. - Incident records. - Management of documents and media. - Backup copies. - Security officers. - Audits. - Access records. - Telecommunications. All measures must be described in a security document that also specifies the obligations of any employees, agents and contractors accessing the data files, and the structure of the files, including a description of the systems processing them.
UK	Data controllers must take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Data controllers must also: - Ensure any data processor processing data on their behalf is under a contractual obligation to secure compliance with these requirements (see Question 16). - Take reasonable steps to ensure that the requirements listed in the point above are put into practice (see above). - Take reasonable steps to ensure the reliability of employees who may access any personal data. The Data Protection Act 1998 (DPA) does not define what specific security measures must be implemented. The nature of the information and the possible harm that may result from any breach will also be important. Management, organisational, technical and physical measures may all be necessary. Further guidance is available from the:

	- Information Commissioner's Office. - UK Department for Business, Innovation and Skills Cyber Essentials programme, which can lead to "cybersecurity" certification after assessment. - Other international security standards (such as ISO 27001) can also be used as reference points.
16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?	
FRANCE	There is no general obligation to notify personal data security breaches to data subjects or the French Data Protection Authority (CNIL). However, electronic communication service providers registered with the French Authority for the Regulation of Electronic Communications and Posts (Autorité de Régulation des Communications Electroniques et des Postes) (ARCEP) (that is, mobile phone operators and internet service providers) must notify all breaches to the CNIL, regardless of their seriousness (Article 34 bis, Data Protection Act (DPA) and decree 2012436 dated 30 March 2012). Notification must be made within 24 hours of the breach, although the CNIL accepts a two-stage notification (that is, a preliminary notification within 24 hours and then within 72 hours if more time is needed for further investigations). Notification is made through a form that can be returned by post or filed online. Under this regime, the electronic communication service providers must also inform data subjects, unless the breach did not affect their privacy rights. In addition, the CNIL can require the data controller to notify data subjects. Electronic communication service providers must also keep an updated record of all breaches (Article 34 bis, DPA). An electronic communication service provider that does not notify a security breach to the CNIL or data subjects faces five years' imprisonment and/or a fine of EUR300,000 (Article 226171, French Criminal Code).
ITALY	Under Article 32 bis of the Italian Code a data breach notification is considered to be mandatory only for the provider of publicly available electronic communications services, who must notify the breach to the IDPA without undue delay. In addition, if the personal data breach is likely to be detrimental to the personal data or privacy of the contracting party or another individual, the provider must also notify the contracting party or the individual without delay. Notification will not be required if the provider has demonstrated to the IDPA that he has implemented technological protection measures that render the data unintelligible to any entity that is not authorised to access it. The IDPA recently issued a resolution providing that data breach notification is also an appropriate measure to be adopted by banks and other companies belonging to a banking group, including third companies operating in outsourcing and that process bank information. The IDPA also provides that data breach notification is a mandatory measure to be adopted by data controllers that process biometric data.
SPAIN	There is no requirement to notify data security breaches under the Data Protection Act or the Data Protection Regulations. Acknowledging guilt for a specific breach will be taken into consideration by the Data Protection Agency when imposing penalties. Notifying data subjects can also reduce civil liability. The General Telecommunications Act establishes an obligation on telecoms operators to notify the Data Protection Agency without delay of any personal data breach. This Act defines personal data breaches as any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data transmitted, stored or processed in connection with the provision of a publicly available electronic communications service.
UK	Security breaches include unauthorised access to and alteration or deletion of personal data. There is no general requirement to notify security breaches to the Information Commissioner's Office (ICO) or data subjects. However, non-binding ICO guidance suggests that the organisation expects to receive reports of serious breaches. There is no defined threshold but it will take into

	account the potential consequent harm to data subjects, the amount of affected data and its sensitivity. ICO guidance also covers when notification must be given to individuals. There is a more exacting sectoral requirement for providers of public electronic communications services (for example, telecoms providers and internet service providers (ISPs)) to notify the ICO of data breaches (Regulation 5A, Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Where a breach is likely to adversely affect the privacy of data subjects, they must also be notified without unnecessary delay. Public bodies are subject to policy requirements to notify ICO and data subjects of data breaches, in line with the tests set out in ICO guidance.
17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?	
FRANCE	A data processor must offer adequate guarantees to ensure the implementation of the security and confidentiality measures (Article 35, DPA). The data processor must act on the basis of a contractual agreement concluded with the data controller, which must both: - Specify the processor's obligation regarding the protection of security and confidentiality. - Provide that the data processor can only act on the controller's instructions. The French Data Protection Authority (CNIL) has published several standard contractual clauses regarding the implementation of confidentiality measures by the data processor in the area of health[9] and regarding data transfer[10].
ITALY	The Italian Code allows personal data to be transferred to third entities providing outsourced processing services, where the transfer is legitimised by a contract or agreement between the data controller and outsourcer. However, such a transfer needs to be carried out by ensuring the due protection of the data. For example, in such a case, it is important to establish within the contract or agreement how the external provider will act with reference to the data protection profile (that is, whether the external provider will act as an autonomous data controller or as a data processor). If the third party acts on behalf of the data controller, the third party must be appointed as data processor and the data controller will have the duty to: - Provide him with the due instructions about the processing operations. - Periodically verify that the data processor is always able to guarantee compliance with the legal provisions applying to processing and related security matters.
SPAIN	When a company processes personal data by providing a service to the data controller, the data processing must be regulated by contract, specifying that the processor must: - Process the data only in accordance with the data controller's instructions. - Not apply or use the data for purposes other than those established in the contract. - Not communicate the data to third parties. - Implement the appropriate security measures. Data processors can communicate the data to others when authorised by the data controller. The Data Protection Regulations establish the conditions under which the main data processor can subcontract part of the services rendered to the data controller if the subcontractor can also process the data.

[9] www.cnil.fr/lesthemes/sante/fichepratique/accessible/non/article/soustraitancemodelesdeclausesdeconfidentialite/

[10] www.cnil.fr/vosobligations/transfertdedonneeshorsue/contratstypesdelacommissioneuropeenne/

UK	The data controller must select a data processor capable of providing sufficient security measures and take reasonable steps to enforce these measures. The contract with the processor must be evidenced in writing and must require the processor to act only on the instruction of the controller and to implement appropriate technical and organisational measures.
18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?	
FRANCE	A data controller can store cookies or equivalent devices if the following three conditions are satisfied: - The data subject must be informed of the purposes of any cookies. - The data subject must be informed of the means available to object to such storing. - The data subject must give his consent. The information provided to the data subject must be clear and comprehensive. In addition, the French Data Protection Authority (CNIL) has set very detailed guidelines regarding the data subject's consent[11]. The consent must be: - Given before using the cookies. Based on comprehensive information to ensure that consent is specific and given freely. - The result of a real choice. The CNIL considers that the consent must be given through a positive action and suggests the following consent mechanisms: - A banner on the first web page visited informing the data subject that continuing to visit the website constitutes consent. - Boxes to tick when registering for online services. In addition, the CNIL recommends inserting a "for more information" page where the data subject can refuse the use of cookies. The consent is valid for 13 months. The use of cookies is exempted from the requirements above where the cookies are either: - Exclusively intended to enable or facilitate communications. - Strictly necessary for the provision of an online communication service at the user's express request. For example, the CNIL considers that "shopping bag" cookies or authentication cookies are exempted.
ITALY	It will depend on the specific type of cookie. The Italian Code places a prohibition on the use of electronic communications networks to access information stored in the terminal equipment of a contracting party or user, store information, or monitor the operations performed by the user, without the previous and informed consent of the user. However, it is not prohibited to use cookies that are strictly necessary to operate the service as per the user's request, including in the absence of the previous and informed consent of the user. Therefore, for every specific purpose (for example, relating to cookies used for profiling, marketing and retargeting purposes), the provider must always inform the users and obtain their prior consent in order to lawfully use cookies in a manner that is different to that which is strictly necessary for the service requested (Article 122(1), Code).
SPAIN	Under the Information Society Services Act, information society services providers can use cookies and equivalent devices in users' equipment if the users consent to it. Users must first be provided with clear and complete information about the use of such devices, particularly with regard to data processing.

[11] www.cnil.fr/vosobligations/siteswebcookiesetautrestraceurs/queditlaloi/

	This requirement does not apply when the only purpose of the device installed in the users' equipment is to transfer information via electronic communication networks, or when using the device is necessary to provide a service expressly requested by the user. Under the Data Protection Agency's guidelines (which are not mandatory but should be followed by information society service providers/data controllers since they reflect how the Agency interprets the rules) users must be informed of cookies (and equivalent devices) using two layers: - The first layer (usually a pop-up) must briefly inform the user about the cookies, identifying their purpose and whether they are first or third party cookies. This layer must include an accept button or warn users that a specific action (like continuing to use the site) will imply acceptance of the cookies. It must also include a link to the second layer. - The second layer must include detailed information about cookies: definition, types of cookies and their purpose, how to disable or eliminate them and reject their use, and identification of third parties when third party cookies are used.
UK	Data controllers must (Regulation 6, Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) Amendments): - Provide the user with clear and comprehensive information about the purposes for which the cookie is stored and will be accessed. - Obtain the user's consent. The information must be sufficiently comprehensive to allow users to fully understand the nature and operation of the cookie. The Article 29 Working Party has stated that consent must be obtained prior to cookie placement. The Information Commissioner's Office recognises that providers often set cookies as soon as the user accesses a website and advise that, where possible, they should delay this until the user has had the chance to understand and consent to their use. There is no statutory definition for consent in the UK. However, Article 2(h) of the Data Protection Directive (95/46/EC) (DP Directive) defines it as a *"freely given, specific and informed"* indication of the individual's wishes. The consent must be unambiguously given (Article 7, DP Directive). The ICO guidance suggests that while individuals must ideally *"knowingly accept"* cookies (for example, through clicking an icon or ticking a box), providers can now rely by giving implied consent provided that: - They inform the user that a specific action will be interpreted providing consent (for example, a prominent notice on the homepage of a website). - An indirect expression of consent can be inferred from the user's actions. Consent is not required in limited circumstances only. Such exceptions include instances where a cookie is planted for the sole purpose of enabling the transmission of electronic communication data or where it is strictly necessary for the provision of a requested service.
19. What requirements are imposed on the sending of unsolicited electronic commercial communications?	
FRANCE	Unsolicited electronic commercial communication must comply with the requirements set out in Article L. 345 of the French Postal and Electronic Communications Code. Based on this Article, the French Data Protection Authority (CNIL) has issued recommendations[12] that distinguish between business-to-consumer (B2C) and business-to-business (B2B) relationships. **B2C relationships** The recipient must have explicitly agreed to receive unsolicited commercial communications when

12

www.cnil.fr/lesthemes/consopubspam/fichepratique/article/laprospectioncommercialeparcourrierelectronique/

	he provided his email address. However, there are two exceptions where prior approval is not required: - The recipient is already a customer of the company and the marketing messages relate to products or services that are similar to those previously provided. - The marketing messages are not commercial in nature. In any case, the recipient must be informed of the commercial use of his email address and must be able to object to such use. **B2B relationships** Unsolicited electronic commercial communications are authorised provided that: - The recipient has been informed at the time his email address is collected that it will be used for the purpose of electronic commercial communications. - The recipient is able to object to such use. Generic email addresses (for example, info@company.com or contact@company.com) are considered as a company's contact details and are therefore not subject to the principle of consent and the right to object. To fall within the category of B2B relationships, the unsolicited electronic communication must relate to the professional activities of the recipient. In both B2B and B2C relationships, the sender must always provide its identity and set a simple tool to object to the spam. If the requirements above are not complied with, the sender can be subject to any or all of the following: - An administrative fine (Article 47, Data Protection Act (DPA)). - A sanction equivalent to a fourth class offence fine which applies per email sent (Article R. 101, French Postal and Electronic Communications Code). - A criminal sanction (Articles L. 22618 and L. 226181, French Criminal Code).
ITALY	**Opt-in regime** The use of automated communications systems (without human intervention) for the purposes of direct marketing or sending advertising materials, or else for carrying out market surveys or interactive business communication, must only be allowed with the contracting party's or user's consent. This applies to electronic communications performed by email, facsimile or MMS or SMS-type messages. **Opt-out regime** For phone numbers that have been taken from public registers, lists, records and publicly available documents, the related processing can be performed without the data subject's consent, provided that the data subject has not objected to the processing by his registering with the Opposition Register. This is similar to a Robinson list (an optout list of people who do not wish to receive marketing transmissions). A similar register has not yet been implemented for the mail. The Italian Data Protection Authority (IDPA) has also issued some important measures and general resolutions to be taken into consideration, including the recent resolutions concerning the guidelines on promotional activities and spam, issued by the IDPA on 4 July 2013 and the guidelines on the activities of online profiling, issued by the IDPA on 19 March 2015.
SPAIN	Recipients must consent to receiving electronic commercial communications. An opt-out is valid for communications relating to first party products or services similar to those initially requested by the customer. An opt-in is required when communications relate to third party products or services, or products or services other than those initially requested by the customer.
UK	Spam covers any form of text (for example, email or SMS), voice, image (including video) or sound message sent over a public communications network that can be stored in the network or the

	recipient's equipment. In general, organisations cannot send unsolicited electronic marketing material to individual subscribers unless they have previously obtained their consent to do so. This is subject to an exception known as "soft opt-in". This allows unsolicited commercial marketing where the organisation: - Obtains the relevant contact details during the course of, or negotiations leading to, a sale of a product or service to the recipient. - Sends direct marketing in respect of its own goods or services similar to those involved in the sale. - Gives the recipient a free method, at the time the contact details were acquired, to optout of the use of their contact details for direct marketing purposes. - Includes a right to opt-out of future direct marketing in each subsequent email to an individual. Controllers must not conceal their identity in any such marketing emails and must provide a valid contact address by which data subjects can opt-out. The rules on consent and "soft opt-in" do not apply to communications sent to companies and limited liability or Scots law partnerships. These activities only require the sender to identify themselves and give a contact address. Additionally, if the email is sent to an individual contact at such an organisation, the general right to opt-out of direct marketing will apply.
20. What rules regulate the transfer of data outside your jurisdiction?	
FRANCE	Under Article 68 of the DPA, a data controller cannot transfer personal data to a state that is not an EU member if this state does not provide a sufficient level of protection of individuals' privacy, liberties and fundamental rights. This principle applies to all transfers, including intracompany or intra-group transfers. The European Commission recognises that the following states provide a sufficient level of protection: Andorra, Faroe Island, Jersey, Canada, Isle of Man, Guernsey, Argentina, Uruguay, New Zealand, Switzerland, Israel, Member states of the European Free Trade Association (EFTA). Transfers to the US can be done in accordance with the US/EU Safe Harbor. For transfers to other states, personal data transfers are allowed provided that either (Article 69, DPA): - The data subject has expressly consented to the transfer. - The transfer is necessary for: - protection of the individual's life; - protection of the public interest; - compliance with obligations allowing the acknowledgement, the exercise or the defence of a legal right; - consultation of a public register intended for the public's information; - performance of a contract between the data controller and the individual, or the precontractual measures undertaken at the individual's request; or - the conclusion or performance of a contract in the individual's interests, between the data controller and a third party. If the conditions above are not fulfilled, a personal data transfer is possible if it is authorised by the French Data Protection Authority (CNIL). The CNIL will assess whether there is an adequate level of protection, which can be reached through the following mechanisms: - The data controller uses contractual clauses to set a sufficient level of protection. In this respect, the European Commission has established model clauses that, if adopted, facilitate a CNIL authorisation (see Question 22). - Company internal rules that ensure sufficient protection for data transfers within the company.
ITALY	The Directive 95/46/EC on data protection (Data Protection Directive) and the Italian Data Protection Code (Code) allows data transfer inside the European Union (EU) and European and

	Economic Area (EEA). Under the Code, data transfer to third countries located outside the EU and EEA is not always allowed. The main ways for allowing international data transfers are by: Obtaining the data subject's express consent. - Incorporating standard contractual clauses (SCC). - Incorporating binding corporate rules (BCR). - Providing adequate protection decisions. The Code provides for further specific derogations that can legitimate the data transfer abroad, including if the transfer is necessary: - For the performance of obligations resulting from a contract to which the data subject is a party, or to take steps at the data subject's request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the data subject. - For safeguarding a substantial public interest that is referred to in laws or regulations. To safeguard a third party's life or prevent injury. - For investigations by defence counsel, or else to establish or defend a legal claim, provided that the data is transferred exclusively for these purposes and for no longer than is necessary, and in compliance with the laws applying to business and industrial secrecy.
SPAIN	International data transfers are transfers to countries whose level of protection has not been declared adequate by the relevant authorities (any country outside the European Economic Area (EEA) with some exceptions). Such transfers must be notified to the Data Protection Agency and authorised by its director, regardless of whether the data importer belongs to the same group as the data exporter. Authorisation can be obtained using the Model Contracts for the transfer of personal data to third countries approved by the European Commission. The Data Protection Agency must receive the contract and confirm that the parties' representatives have sufficient power to sign it. The Agency has up to three months from the date it receives the request to issue and communicate its decision. Data Protection Agency authorisation is not necessary in the following cases (although it must still be notified of the international data transfer): - When the transfer results from the application of an international treaty to which Spain is party. - When the transfer is meant to provide or request international judicial aid. - When the transfer is necessary for medical prevention or diagnosis, or providing healthcare or medical treatment or for managing healthcare services. - When the transfer relates to money transfers made according to their specific legislation. - When the data subject has unequivocally given consent to the data transfer (if the data subject has no real option to oppose the transfer (which is usually the case with employees) consent will not be valid). - When the transfer is necessary for the performance of a contract between the data subject and the data controller or to adopt precontractual measures at the data subject's request. - When the transfer is necessary to execute or perform a contract concluded or to be concluded, between the data controller and a third party in the interest of the data subject. - When the transfer is necessary or legally required to protect the public interest. - When the transfer is necessary for the recognition, exercise or defence of a right in a legal proceeding.
UK	There are no specific restrictions regulating the transfer of personal data between European Economic Area (EEA) states. Personal data must not be transferred from the UK to a country or territory outside the EEA unless the destination country or territory secures an adequate level of protection for data. The European Commission has made a formal declaration under Article 25(6) of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal

	data and on the free movement of such data (DP Directive) that certain non-EEA countries have an adequate level of protection for these purposes[13]. The adoption of legally binding corporate rules (BCR) can also allow multinational organisations to freely transfer data within their corporate group in circumstances where this would take the data outside of the EEA. The BCR must be approved by all relevant European authorities who will assess the adequacy of the group's rules. Schedule 4 of the Data Protection Act 1998 (DPA) provides for exceptions that allow the transfer of personal data to third countries and territories even if there is no adequate protection. These include circumstances where the consent of the data subject has been obtained or the transfer is necessary for reasons of substantial public interest.
21. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?	
FRANCE	Under Article 6 of the Data Protection Act (DPA), personal data can be stored if the following conditions are satisfied: - Data are obtained and processed fairly and lawfully. - Data are obtained for specified, explicit and legitimate purposes, and is not subsequently processed in a manner that is incompatible with such purposes. However, further data processing for statistical, scientific and historical purposes is considered compatible with the initial purposes of data collection, if it is not used to take decisions relating to the data subjects and is carried out in accordance with the principles and procedures provided for in: - Chapter II of the DPA; - Chapter IV of the DPA (formalities prior to commencing data processing); - section 1 of Chapter V of the DPA (obligations of the data controllers and rights of individuals); - Chapter IX of the DPA (processing of personal data for the purpose of medical research); and - Chapter X of the DPA (processing of personal medical data for the purposes of evaluation or analysis of care and prevention practices or activities). - Data are adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing. - Data are accurate, complete and, where necessary, kept uptodate. Appropriate steps must be taken to delete and rectify data that are inaccurate and incomplete with regard to the purposes for which they are obtained and processed. - Data must be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed.
ITALY	Restrictions are provided for the transfer of personal data outside the EU and the EEA. If the data is transferred within the EU or the EEA, no particular restrictions are established, due to the principle of free movement of personal data among EU member states. Both the law and the Italian authorities can provide restrictions with specific reference to certain purposes of data processing. For example, with regard to prize draws, the law establishes that for online prize contests, the server collecting the entries must be located in Italy. If the server is located abroad, the data concerning the contest's participants must be mirrored in real time from the abroad server to an Italian one.
SPAIN	There is no requirement to store personal data inside the jurisdiction.
UK	There is no requirement to store personal data in the UK.
22. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the	

[13] A full list can be found at http://ec.europa.eu/justice/dataprotection/internationaltransfers/adequacy/index_en.htm.

need to obtain consent) be satisfied?	
FRANCE	Although the use of model clauses approved by the European Commission is not mandatory, the French Data Protection Authority (CNIL) recognises that the adoption of such model clauses will facilitate the authorisation process and increase legal certainty. The European Commission has adopted three sets of model clauses: - Two sets apply to data transfers outside the European Economic Area (EEA) from one data controller to another, and were adopted in 2001 and 2004. - One set applies to data transfers outside the EEA from a data controller to its subprocessor, and was revised in 2010. On 21 March 2014, the G29 working group (see Question 5) issued a working document on draft ad hoc contractual clauses applying to EU data processors and non-EU subprocessors. This working document provides a new set of clauses to ensure adequate safeguards for the protection of privacy and fundamental rights and freedoms of individuals for transfers of personal data to a subprocessor. This document is currently under the review of the European Commission, which is expected to decide whether the 2010 set of clauses should be amended or supplemented.
ITALY	The Italian Data Protection Authority (IDPA) recognises the standard contractual clauses adopted by the EU Commission as a tool to guarantee the protection of the data transferred (see Question 20).
SPAIN	The Data Protection Agency has approved standard contractual clauses that regulate international data transfer from a data processor established in Spain to data subprocessors established in countries whose level of protection is not adequate. In this case, to obtain the Data Protection Agency's authorisation, the data processor must also provide the Data Protection Agency with an agreement between the data processor and the data controller under which the latter authorises the subcontracting and the international data transfer.
UK	The European Commission has determined that certain standard contractual clauses can be used to ensure adequate protection for personal data. The Information Commissioner has authorised use of such contractual clauses[14].
23. Does the relevant national regulator need to approve the data transfer agreement?	
FRANCE	A data transfer agreement is sufficient to legitimise transfer.
ITALY	A data transfer agreement (that incorporates standard contractual clauses) is sufficient to legitimise the transfer, and consent is not required.
SPAIN	Regardless of the requirements applicable to international data transfers (see Question 20), transfers on a controller-to-controller basis are subject to the consent rule (see Question 9) and data subjects must be informed of these transfers (see Question 12).
UK	If standard contractual clauses are used, there is no need to take additional steps to ensure adequate protection for the transfer of personal data. However, if the data controller wishes to transfer data outside the EEA to another data controller, this transfer of data will also amount to an act of processing. In addition to ensuring adequate protection for the data, the controller will need to ensure that the processing can be justified under Schedule 2 and, if relevant, Schedule 3 of the Data Protection Act 1998 (DPA). This can mean seeking the consent of the data subject.
24. What are the enforcement powers of the national regulator?	
FRANCE	The French Data Protection Authority (CNIL) does not need to approve the data transfer agreement. However, the CNIL must assess whether the contractual clauses of the data transfer agreement can ensure an adequate level of protection. Therefore, the CNIL can request to see the data transfer agreement during the authorisation process (if prior authorisation is required).

14 https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf

ITALY	Filing or authorisation is not required if the data controller uses the original wording of the standard contractual clauses issued by the EU Commission without making any change.
SPAIN	See Question 20.
UK	The national regulator does not need to approve the data transfer.
25. What are the sanctions and remedies for noncompliance with data protection laws?	
FRANCE	The enforcement powers of the French Data Protection Authority (Commission Nationale Informatique et Libertés) (CNIL) are set out in Article 44 of the Data Protection Act (DPA). To date, the CNIL is entitled to: - Conduct onsite inspections, on justification and prior authorisation of a judge (Juge des Libertés et de la Détention). The inspection can take place without notice and the person in charge of the premises cannot object to the inspection (although it can appeal against the authorisation after the inspection). During these onsite inspections, the CNIL has access to any storage devices. Request in writing the communication of documents (document review). - Conduct hearings. The Hamon Act No. 2014344 on consumer protection dated 17 March 2014 has increased the CNIL's investigation powers, enabling the authority to conduct remote online controls. Such controls are conducted within the CNIL's premises. The CNIL then reports any breach to the person controlled. Remote controls are limited to data that are public and accessible. The first online control was conducted in October 2014 and, since then, the CNIL has conducted 58 online controls. Under the Hamon Act, which is now codified in Article L. 1411 of the French Consumer Code, the authorities that are in charge of commercial and competition matters can now access relevant information and control compliance with personal data regulations while they investigate a company on any (other) matter. They can then report any infringement to the CNIL. These authorities include the: - General Directorate for Competition, Consumers and the Prevention of Fraud (Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes) (DGCCRF). - Competition investigation interregional authorities (Brigades Interrégionales d'Enquêtes de Concurrence) (BIEC). - Fraud investigation interregional authorities (Brigades Interrégionales d'Enquêtes de Répression des Fraudes) (BIERF). - Companies, competition, consumption, labour and employment regional authorities (Directions régionales des entreprises, de la concurrence, de la consommation, du travail et de l'emploi) (DIRECCTE). - Local authorities for the protection of population (directions départementales de la protection des populations) (DDPP). - Competition Authority. The CNIL can impose injunctions and fines for non-compliance with data protection laws (see Question 25). Impeding the action of the CNIL may result in imprisonment for a term of one year and a EUR15,000 fine (Article 51, DPA). In addition, where the CNIL considers that a criminal offence has been committed, it can notify the Public Prosecutor.
ITALY	The Italian Data Protection Authority (IDPA) must act autonomously and independently in its decisions and assessments. The IDPA's powers mainly consist of: - Verifying whether data processing operations are carried out in compliance with laws and regulations. - Receiving reports and complaints, and responding by taking appropriate steps. - Ordering data controllers or processors, ex officio, to adopt necessary or appropriate measures for

	the processing to comply with the provisions. - Prohibiting, ex officio, unlawful or unfair data processing operations, in whole or in part, or blocking such processing operations. - Drawing the attention of parliament and government to the advisability of legislation as required by the need to protect the rights. - Having a preference with regard to information on facts or circumstances that amount to offences to be prosecuted ex officio. In discharging its tasks, the IDPA can request the data controller, the data processor, the data subject or a third party to provide information and produce documents. The IDPA can order that data banks and filing systems be accessed and audits be performed on the spot regarding the premises where the processing takes place or investigations are to be carried out with a view to checking compliance with personal data protection regulations. Such inquiries must be carried out by staff from the office. The IDPA can also ask for the cooperation of other state agencies. In specific cases of non-compliance with the applicable law on privacy and data protection requirements, the IDPA can impose administrative fines provided in Articles 161 of the Italian Code.
SPAIN	The Data Protection Agency is responsible for imposing sanctions for non-compliance and it is entitled to inspect data files and request any information necessary to perform its functions. The Data Protection Agency's inspectors can ask to see documents and data and examine them wherever they are located, as well as check out the physical equipment and software used to process data by accessing the premises where it is installed.
UK	Section 42 of the Data Protection Act 1998 (DPA) allows data subjects who are concerned that data processing is directly affecting them to request an assessment by the Information Commissioner (IC) into whether or not such processing complies with the DPA. The IC has complete discretion as to how such investigations proceed and the data subject must be informed of any subsequent action. **Sanctions** The IC can serve data controllers with: - Enforcement notices. This represents legally binding documents requiring compliance with the data protection principles. Failure to comply represents an offence unless the data controller can show they exercised all due diligence. - Monetary penalties. See Question 26. In addition, the IC can use undertakings, where he requires organisations to follow a remedial course of action in lieu of taking formal enforcement action. **IC investigatory tools** The IC has the following investigatory tools (Schedule 9, DPA): - Information notices. These require the provision of information about the purposes for and manner in which data controllers process information. - Assessment notices. These can be served on government departments and public authorities/persons designated by the Secretary of State as being a data controller to investigate compliance with the data protection principles. - Powers of entry, inspection and seizure. The IC also has wideranging, sector specific powers of enforcement and investigation under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) Amendments (see Question 1).

Table 3: National Regulations on Data Protection

8 Appendix C Summary of National Data Privacy Regulations

This summary is extracted from the Practical Law webpage[15], which provides a set of 9 questions regarding Data Privacy in each of the EU countries and others. Each National Regulation is analysed by experts of each country.

COUNTRY	ACTIONS
1. What national laws (if any) regulate the right to respect for private and family life and freedom of expression?	
FRANCE	The right to respect for private and family life is protected under Article 9 of the French Civil Code, which provides that "everyone has the right to respect for his private life". Interferences with the right to private and family life can lead to criminal sanctions that are set out in Articles 226-1 and 226-8 of the French Criminal Code. The right to privacy also derives from Article 8 of the European Convention on Human Rights (ECHR) and Article 7 of the Charter of Fundamental Rights of the European Union. The French Constitutional Court (*Conseil Constitutionnel*) also considers the right for private and family life as a constitutional right (*decision n° 99-416 DC, dated 23 July 1999*). Freedom of expression is also a constitutional right, which is expressly protected under: • Article 11 of the Declaration of Human rights of 1789. • Article 10 of the ECHR. • Article 11 of the Charter of Fundamental Rights of the EU. Under French law, the rights to respect for privacy and family life and freedom of expression benefit from the same level of protection. In cases where the exercise of these rights pursues contradictory interests, the courts must strike a balance between the exercise of each right on a case-by-case basis. The right to respect for private life is also protected by the Act No. 78-17 of 6 January 1978, (*Loi Informatique et Libertés*) which regulates the processing of private data.
ITALY	The Italian Constitution (Constitution), promulgated on 27 December 1947 is the primary domestic law regarding the protection of fundamental rights. Article 2 of the Constitution provides that Italy "recognises and guarantees the inviolable rights of the person, both as an individual and in the social groups where human personality is expressed". Inviolable rights include the: • Right to respect for private life, including the inviolability of the personal domicile (*Article 14*) and the freedom and confidentiality of correspondence and of every other form of communication (*Article 15*). Any restriction or limitation of these rights can only be imposed by judicial decision stating the reasons and in accordance with the guarantees provided by the law. • Rights of the family as a natural society founded on marriage (*Article 29*). • Right of freedom of expression (*Article 21*). The right to respect for private and family life and freedom of expression are also protected under Articles 8 and 10 of the European Convention on Human Rights (ECHR). Italy ratified the ECHR with Law No. 848 on 4 August 1955. The Constitutional Court established that the ECHR does not have

[15] http://uk.practicallaw.com/

	the status of a constitutional law (*Judgments No. 348 and 349, 2007*). Legislative Decree No. 196/2003 (Italian Data Protection Code) (Code) provides for safeguards to the right to privacy, by establishing that "everyone has the right to protection of the personal data concerning them" (*Article 1, Code*).
SPAIN	Article 18 of the Spanish Constitution recognises the right to respect for private and family life. This right has been further developed by: • From a civil standpoint, Law 15/1999 on personal data protection (and its secondary regulation) and Law 1/1982 on civil protection of the right to honour, to personal and family privacy and of the right of self-image. • From a criminal perspective, by the Criminal Code (contained in Law 10/1995). While the rights to honour, personal and family privacy, and self-image are expressly recognised in the Constitution, the right to personal data protection (right to privacy) was introduced as consequence of the impact that technical developments have had on the processing of personal data. The right to freedom of expression is set out in Article 20 of the Constitution and has been developed through case law from the Spanish Constitutional Court. No other regulations enshrine this fundamental right, except for some specific laws relating to the so-called "conscience clause" (*see Question 3*) and the right to ask for rectification of incorrect or inaccurate information published in the media. The Spanish Criminal Code also protects freedom of expression.
UK	The Human Rights Act 1998 (HRA) incorporates the European Convention on Human Rights (ECHR) into the law of the UK. It requires public authorities, including courts and tribunals, to comply with Articles 8 and 10 of the ECHR (*section 6(1), HRA*) including when interpreting legislation (*section 3, HRA*). Courts and tribunals must take into account earlier relevant decisions of the European Court of Human Rights (ECtHR) when interpreting the scope and effect of rights under the ECHR (*section 2(1), HRA*). If it is not possible for a court to interpret legislation so as to be compatible with the ECHR, a declaration of incompatibility can be issued (*section 4, HRA*). ECtHR decisions are effectively binding on the courts of England and Wales. The question of whether the UK should remain sovereign over human rights law in the UK is now a contentious political issue. Article 8 of the ECHR provides that everyone has the right to respect for their private and family lives, their home and correspondence. This is qualified for some purposes, such as the protection of others' rights and freedoms, insofar as it is in accordance with the law and necessary in a democratic society. The obligation on courts (as public authorities) to interpret the law in order to be consistent with the ECHR has resulted in the development of judge-led Article 8 jurisprudence that has now established a tort of "misuse of private information" from traditional breach of confidence principles (*Campbell v Mirror Group Newspapers* [2004] UKHL 22 and *Vidal-Hall v Google* [2015] EWCA Civ 311). Therefore, in reality, Article 8 has direct effect and privacy rights can be enforced against anyone, not just public authorities. Article 10 of the ECHR provides the right to freedom of expression. Restrictions to this right must be prescribed by law and necessary in a democratic society for at least one of a number of reasons, such as protecting another's reputation or preventing the disclosure of confidential information. The rights under Article 8 or Article 10 of the ECHR do not take precedence over the other. Where both rights are engaged the court must perform a balancing act taking into account the comparative importance of the rights claimed, the justifications for interfering with or restricting each right and proportionality.
2. To whom do the privacy law rules apply?	

FRANCE	Under Article 9 of the French Civil Code, anyone can commence proceedings for the protection of private and family life, including public figures. However, public figures tend to be granted less protection than ordinary citizens. Although there is no statutory definition of public figures, French case law has suggested that courts approach such claimants (generally celebrities, well-known or famous persons) with less sympathy than ordinary citizens. In practice, the courts take into account whether the public figure takes ordinary precautions to protect his or her private life, or whether it regularly and voluntarily disclose some aspects of his or her private life to the media. Freedom of expression can interfere with the right to privacy when any person is involved in a news event, provided that the elements disclosed (such as pictures and personal information) are linked to the event. In addition, actions based on Article 9 of the Civil Code are individual in nature and must relate to breaches that cause personal harm to the claimant. Therefore, heirs are not entitled to introduce an action based on an alleged breach of privacy of a deceased person. Since breaches of privacy rights can constitute criminal infringements, criminal prosecutors can also commence proceedings, although this is unusual.
ITALY	The data subject, that is any natural person that is the subject of the personal data, can commence proceedings to protect privacy.
SPAIN	Proceedings for breach of personal data protection or privacy can be commenced by: • The affected individuals. Rights granted by law only vest in living individuals and cannot be used by entities. • Third parties (either individuals or entities) who become aware of a breach of the data protection law. In these cases, third parties can only request that the Spanish Data Protection Agency start administrative proceedings which can lead to sanctions. • The Data Protection Agency can also act *ex officio* should it become aware of any infringement of the law. Proceedings to protect honour, self-image and private and family life can be commenced by: • The affected individuals and/or entities. Entities can file an action for infringement of their honour and intimacy rights. • In the event that the affected individual has passed away, proceedings can be brought by: o the individual or entity specifically appointed by the individual's last will and testament; o the individual's spouse, descendants, ascendants or siblings that were alive when the affected individual passed away; or o the public prosecutor. Finally, proceedings to ensure protection of freedom of expression can be commenced by: • The affected individuals and/or entities. • Journalists (under the conscience clause). (In connection with the right of rectification), the representatives of the affected individual or entity or the heirs of the affected individual (or their representatives).
UK	Natural persons can bring claims to enforce their privacy rights before the courts of England and Wales. In certain circumstances it is also possible for an individual to bring a claim against the government before the European Court of Human Rights (ECtHR) (for example, *Mosley v United Kingdom* (2011) 53 EHRR 30). A corporate body does not have the necessary personal information to form the basis of an Article 8 claim and must instead rely on the law of confidentiality.
3. What privacy rights are granted and imposed?	
FRANCE	The notion of "privacy" is very broad and includes, for example, information related to a person's: • Health.

	• Marital situation. • Family life. • Domicile. • Estate and financial situation. • Religion. • Political orientations. In principle, any arbitrary interference with a person's private and family life is illegal. However, the right to privacy is not absolute. Therefore, certain interferences are accepted by courts on the grounds of freedom of expression, protection of a third party's interest, public safety and fight against criminality. This may be the case, in particular, when the private information that is disclosed permits to assess the actions or statements of a person which are in the public domain. In such cases, the courts must strike a balance between the protection of privacy and the other legitimate interest(s) at stake. This must be analysed on a case-by-case basis. Some elements of privacy benefit from a reinforced protection as "core" elements of a person's intimacy and identity, such as a person's image, physical intimacy, family life and marital situation.
ITALY	The Italian Data Protection Code recognises a set of rights towards data subjects. Data subjects must be informed of the: • Source of personal data. • Purpose and method of the processing. • Logic applied to the processing. • Identification of the data controller. • Data processor and data controller's representative (if any). • Entities and subjects to whom the personal data can be communicated. Moreover, data subjects have the right to: • On legitimate grounds, to the processing of his personal data, even if relevant to the purpose of the collection. • Erase, anonymise or block the data that has been processed illegally, including data that was retained for different purposes than what it was collected for. • Receive certification from the entities to whom the data was communicated, provided that the above processes have been complied with (unless this requirement proves impossible or involves a manifestly disproportionate effort compared to the right that is to be protected). Data subjects also have the right to object, in whole or in part: • On legitimate grounds, to the processing of his personal data, even if relevant to the purpose of the collection. • To the processing of his personal data, where it is carried out for the purpose of sending advertising materials or direct selling for the performance of market or commercial communication surveys.
SPAIN	Individuals have the right to be informed in advance of how their personal data is going to be processed and to consent to the processing before it takes place. In certain cases, consent is not necessary. Individuals must be informed about: • The identity and contact details of the person or entity responsible for processing the data (the data controller). • The purpose of the data processing. • Whether the data will be assigned to third parties. • Which rights are granted by law and how they can be exercised. In particular, the right to access data, amend incorrect or inaccurate data, request cancellation or oppose or object to the processing of data. These rights have been increased as a result of recognition by the

	Court of Justice of the European Union (ECJ) of the right to be forgotten (*C-131/2012, Google Spain, S.L. and Google Inc. versus AEPD and Mario Costeja González*). The right to private and family life granted under Law 1/1982 covers actions aimed at protecting image, voice, name, honour and private life (including family life) from unauthorised use. There is an exception for using an image belonging to a public person (such as a politician or celebrity). Images of public persons can be recorded and/or used if certain conditions are met (essentially, if used in cartoons or recorded in public spaces or during public events), and the image can be used without consent when recording events of public relevance. In addition, Spanish courts ruled that under certain conditions and taking into account all interests, freedom of expression can prevail over rights granted under Law 1/1982, particularly if there is a public interest. Finally, freedom of expression grants the right to: • Issue opinions, thoughts and/or ideas by any means. • Freely produce or create literature and/or artistic, technical or scientific works. • Academic liberty. • Freely communicate and receive truthful information by any means. The right to freely communicate information covers the conscience clause for journalists. The clause gives the right to terminate the relationship between the journalist and the media company for which he is working (under certain circumstances) or to object to producing information that is contrary to the ethical principles of communication. As part of the on-going development of freedom of expression, a new right has been approved granting the right to any individual or entity to ask for the rectification of incorrect or inaccurate information that may be harmful.
UK	Under Article 8 of the European Convention of Human Rights (ECHR), everyone has the right to respect for their private and family life, their home and correspondence. Information will be protected if it is such that the individual has a "reasonable expectation of privacy" in relation to it. A reasonable expectation of privacy will exist where a reasonable person of ordinary sensibilities would be caused substantial offence by the disclosure of information about them in similar circumstances. This question is a broad one and takes into account all the circumstances of the case. There are no fixed categories of what can constitute private information.
4. What is the jurisdictional scope of the privacy law rules?	
FRANCE	In principle, privacy actions must be introduced before the civil court where the infringement was committed. However, in practice, a breach of privacy often takes place in the country as a whole, and the claimant can therefore choose between multiple competent jurisdictions. Currently, cases relating to the media industry are often brought before the Civil Court of Paris or the Civil Court of Nanterre, which both have specialised chambers. If the breach of privacy is due to the action of a public authority, the action must be brought before an administrative court. The usual limitation period for tort actions under French law is five years, starting when the claimant becomes aware of (or should have become aware of) the infringement (*Article 2224, French Civil Code*). However, most cases regarding breach of privacy fall within the scope of the Press Act 1881, under which the limitation period is three months only, from the date the infringement starts.
ITALY	The Italian Data Protection Code (Code) ensures that personal data is processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection. The processing of personal data must be regulated by giving a high level of protection for the data subjects' rights and freedoms. This must

	be in compliance with the principles of simplification, harmonisation and the effectiveness of the mechanisms by which data subjects can exercise such rights and data controllers can fulfil the relevant obligations (*Article 2, Code*).
SPAIN	Spanish courts have interpreted privacy and freedom of expression in the light of international regulations and rules such as the European Convention on Human Rights and decisions from the European Court of Human Rights. In the case of personal data, interpretations made by the Data Protection Agency have broadened some of the rights granted to affected individuals and the obligations on data controllers. For example, Spanish regulations apply to data controllers based abroad as a result of installation and use of cookies on computers in Spain. In addition, there is now recognition of the right to be forgotten, granting individuals the right to ask search engines to delete links in their search results to third parties' websites containing personal
UK	The Human Rights Act 1998 (HRA) can be relied on against a public authority when it is acting "within the jurisdiction" for the purposes of Article 1 of the ECHR. This covers their actions and consequences within the UK. It can also cover extra-territorial acts in very limited circumstances (for example, where a state has effective control of another area) (*R (on the application of Al- Skeini and others) v Secretary of State for Defence* [2007] UKHL 26). The Court of Appeal has recognised that "misuse of private information" is a tort (*Vidal-Hall v Google* [2015] EWCA Civ 311). Practice Direction 6B of the Civil Procedure Rules (*paragraph 3.1(9))* states that tortious claims can be brought against non-resident defendants before the court of England and Wales where the damage: • Is sustained within England and Wales. • Sustained resulted from an act committed within the jurisdiction. This means that a claimant can obtain redress where intrusive and unauthorised photographs are taken abroad, but published in a magazine in England (see *Douglas v Hello! Ltd (No.2)* [2003] EWCA Civ 139). Even if one of the above grounds is met, the court must still be satisfied that the claim has a reasonable prospect of success and that England and Wales is the proper place in which to bring the claim (and that another jurisdiction would not be more appropriate) (*CPR 6.37*). Under the European jurisdiction rules there are multiple possible options that a claimant can elect when determining the jurisdiction in which to bring a privacy action. The general rule is that an EU defendant must be sued in the member state in which it is domiciled, that is, an English company must be sued in the courts of England and Wales (*Article 4, Regulation (EU) 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Recast Brussels Regulation)*). A claimant in this position is entitled to recover damages caused throughout the EU. An exception to the general rule is that an EU defendant can be sued in a tort claim (including a privacy claim) at the place where the harmful event occurred or may occur (Article 7(2), Recast Brussels Regulation). In this situation the claimant can only recover damages suffered in the jurisdiction in which the claim is brought. Finally, a claimant can bring an action, in respect of all the damage caused, before the courts of the member state in which the centre of his interests is based, irrespective of the location of the defendant (*eDate/Martinez* joined cases C-509/09 and C-161/10).
5. What remedies are available to redress the infringement of those privacy rights?	
FRANCE	In the case of an infringement of privacy, the claimant must be granted damages. Breach of privacy and breach of a person's right to image are considered as two separate damages for the calculation of compensation. In practice, the amount of compensation awarded is quite modest. In addition, under Article 9(2) of the French Civil Code, the court can order any measures that are

	necessary to cease a breach of privacy. Such measures include: • The suspension of the distribution of a book. • An obligation to issue a press release. • A warning. • The submission of documents. The measures must be proportionate to the seriousness of the breach. They can also be ordered as interim measures under a fast-track procedure for urgent cases.
ITALY	Data subjects can apply to the Italian Data Protection Authority (IDPA) to lodge a: • Circumstantial claim in order to point out an infringement of the relevant provisions on the processing of personal data. • Report, if no circumstantial claim can be lodged, in order to call on the IDPA to check up on the relevant provisions for processing personal data. • Complaint with a view to establishing the specific privacy rights (*see Question 3*).
SPAIN	Privacy and freedom of expression rights can be enforced both under civil and criminal law. In addition, certain administrative proceedings can be filed before the Data Protection Agency to ensure the protection of basic rights. Civil actions allow individuals or entities to obtain remedies ordering cessation of infringement and awarding damages. In criminal proceedings, the individuals or entities can ask the judge to impose the penalties applicable under the Penal Code along with any civil remedies. Under administrative proceedings, an individual who has unsuccessfully exercised his basic rights before the data controller (*see Question 3*) can seek protection from the Data Protection Agency. The Data Protection Agency will start specific administrative proceedings aimed at verifying whether the relevant legal conditions have been met and order, if necessary, the data controller to comply with the relevant rights.
UK	Remedies available for the tort of misuse of private information reflect those traditionally available for breaches of the equitable duty of confidence. These include: • Interim and final injunctions. • Compensatory damages or an account of profits. • Delivery up or destruction of unlawful material (in rare cases). Additionally, even if a privacy claim is settled out of court, the claimant can still be granted the right to make a statement in open court in order to put their case on the public record. For breaches of the Human Rights Act 1998 (HRA), the court can grant such relief or remedy, or make such order, within its powers as it considers just and appropriate (*section 8(1), HRA*). The court can: • Grant a judicial review to assess the lawfulness of the actions of a public authority. • Declare that a public authority has acted unlawfully. • Cancel a public authority's decision. • Restrain a public authority from acting in an infringing manner. • Make a declaration that an infringing law is incompatible with the European Convention of Human Rights (ECHR).

Table 4: National Regulations on Data Privacy