UNIVERSITAT DE BARCELONA

Data Protection Office
General Secretary's Office

Balmes, 7
08007 Barcelona

+34 934 020 416
protecciodedades@ub.edu
ub.edu/secretariageneral

GUIDE FOR RESEARCHERS AT THE UNIVERSITY OF BARCELONA ON THE PROTECTION OF PERSONAL DATA

1 Purpose of this guide

In many cases, researchers are already broadly familiar with principles related to the protection of personal data. However, in certain circumstances they may require additional support. This guide is intended to serve as a practical reference document that researchers at the University of Barcelona can consult when they have to process personal data within the framework of research projects. It is also intended to facilitate compliance with data protection by design and by default by indicating the main data protection issues that researchers are encouraged to consider during the design phase of research projects.

The University, through its existing research groups, centres and other research structures, is the controller of any personal data used for scientific research purposes. It is therefore responsible for ensuring that researchers carry out their research in a manner that respects all the fundamental rights and freedoms of individuals. This means focusing on two key points: the autonomy of persons participating in research to decide that their personal data may be collected and processed, and safeguards to ensure the confidentiality and security of their data throughout the course of projects.

To ensure that research is carried out in accordance with European standards on data protection, this guide reflects the recommendations given to researchers by the most prestigious European universities, which have extensive experience dealing with issues in this area.

2 Personal data protection regulation: the same rules of the game throughout the European Economic Area

Personal data protection is regulated in all member states of the European Economic Area based on the same principles, established by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter GDPR). One key principle is that neither universities nor research groups are the data subjects with respect to personal data; the data subjects are always the natural persons that the data relate to. However, universities and research groups are responsible for safeguarding and processing personal data in a diligent manner that respects the fundamental rights and freedoms of individuals.

Given that the GDPR makes over 50 references to the national law of each member state, Spanish legislators have approved Organic Law 3/2018, of 5 December, on protection of personal data and guarantee of digital rights, to complement and develop the GDPR. Therefore, these two regulations must be taken into account when carrying out research projects.

If personal data related to health (and contained in the health records of subjects) are to be processed for scientific research purposes, researchers must also consider the provisions of Law 21/2000, of 29 December, on rights to information related to health and patient autonomy, and clinical documentation (Parliament of Catalonia), and Law 41/2002, of 14 November, regulating patient autonomy and rights and obligations related to clinical information and documentation (Spanish Parliament). In addition, if biomedical research is to be carried out, researchers must comply with the provisions of Law 14/2007, of 3 July, on biomedical research, which is the specific regulation that includes the principles established in the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (ETS No 164, of 4 April 1997) of the Council of Europe.

3 Definitions

In this section, we define the personal data protection terms used throughout this guide.

Term	Definition
Personal data	Any information relating to identified or identifiable natural persons, whether numerical, alphabetical, graphic, photographic, acoustic or of any other kind.
Special categories of personal data	Personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.
Pseudonymized data	Personal data that cannot 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Anonymized data	Data that cannot be associated with an identified or identifiable person because the connection to that person has been broken.
Anonymous data	Data recorded without any link to an identified or identifiable person.
Data processing	Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data subject	The natural person who is the owner of the personal data being processed.
Consent of the data subject	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Controller	A natural or legal person, public authority, agency or other body which processes personal data, alone or jointly with others, and determines the purposes and means of the processing, even if it does not carry out the processing itself.

Term	Definition
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
International transfer of data	Data processing that involves the transfer of data outside the territory of the European Economic Area.

Table 1. Definitions of basic data protection terms in the context of university research projects. Prepared by the authors.

4 Issues to consider with regard to the design phase of a research project

When planning a research project, a number of points need to be borne in mind.

4.1 In what cases do data protection regulations apply to a research project?

Data protection regulations apply whenever personal data (i.e. information relating to an identified or identifiable person) must be processed within the framework of a research project. To determine whether a person is identifiable, researchers must consider all the means that can reasonably be used to identify them directly or indirectly (e.g. the costs and time required for identification), taking into account both the technology available at the time of processing and technological developments.

Data protection regulations do not apply to anonymous information (i.e. information which, from the time when it is obtained, does not relate to an identified or identifiable natural person) or to anonymized data (i.e. data that were originally related to an identified or identifiable person but have been modified in such a way that they can no longer be linked to that person). To produce anonymized data, anonymization techniques must be used.[1]

Bear in mind that if data are stored using an alphanumeric code rather than the data subject's name and there is a list linking the name to that code, the pseudonymized data are still personal data because the data subject is still identifiable.

Researchers should consider whether the objectives of their research project can be achieved without having to process personal data (e.g. using anonymous data). If and only if the objectives cannot be achieved without processing personal data, then data of this kind should be collected and processed in accordance with the guidance provided in this document.

4.2 Can any type of data be collected?

Personal data that are adequate, relevant and limited to what is necessary in relation to the purposes of a research project may be collected (principle of data minimization). For example, in the research context,

1. For more information on anonymization techniques, see Opinion 05/2014 on Anonymisation Techniques, produced by the Article 29 Data Protection Working Party (ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf), and *10 Misunderstandings Related to Anonymisation*, produced by the Spanish Data Protection Agency (aepd.es/es/documento/10-anonymisation-misunderstandings.pdf).

a researcher might consider obtaining the age range of a participant rather than their date of birth, or a postcode rather than their full postal address.

Data protection regulations give special protection to “sensitive data” or “special categories of data”, which are data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data, data concerning health, or data concerning a natural person’s sex life or sexual orientation. The collection of such data should be avoided as far as possible unless it is strictly necessary for the research project to be carried out.

4.3 Does personal data need to be pseudonymized during processing?

As mentioned above, whenever possible, research should be carried out without processing personal data (e.g. using anonymous or anonymized data). If this is not possible because the person to whom the personal data belong must be identified, we recommend that pseudonymization techniques be used while the data are being processed to make it more difficult for third parties to identify individuals and to reduce the impact of participation in the project on their privacy.

Pseudonymization involves processing personal data in such a way that the resulting data can no longer be directly attributed to a particular individual without the use of additional information, which must be kept separate and subject to technical and organizational security measures. For example, pseudonymization can be achieved by replacing an individual’s name with a randomly generated identification number and having an encrypted list that matches participants’ names to the corresponding random numbers.

Since pseudonymized information still allows a person to be identified indirectly, it is still considered personal data and is therefore subject to personal data protection regulations.

When data are used in a pseudonymized form, project information sheets should not use expressions such as “answers are anonymous” or “data are stored in anonymous form”. Rather, it should be explained to participants that the data are coded or pseudonymized, and that the list linking their identity to the code or pseudonym is only accessible to the principal investigator, for example, and is appropriately protected.

Finally, bear in mind that certain types of projects (e.g. when data mining techniques are used) may result in data that were anonymous or anonymized before being processed for the project becoming more closely related to an identifiable person after processing. As a result, after processing, such data may come to be considered personal data. Researchers should consider the risk of re-identification in such projects and take measures to mitigate it.

4.4 What security measures must be put in place according to the type of personal data processed?

Data can be collected in many ways (e.g. through forms, recorded interviews or online surveys) and stored in a variety of formats (handwritten notes, digital recordings, computer files, etc.). Each means of collecting and storing data raises certain issues in relation to security against unauthorized access and use, prevention of accidental loss or damage, and the possibility of the data being unavailable.

The GDPR requires that appropriate technical and organizational measures be taken to ensure a level of security commensurate with the risk, taking into account the nature, scope, context and purposes of processing, as well as the likelihood and impact of security risks on the rights and freedoms of natural persons. The security risks associated with research projects must therefore be analysed to determine what security measures need to be implemented.

In the public sector, it is also important to bear in mind that Additional Provision 1 of the Organic Law 3/2018, of 5 December, on Data Protection and Guarantee of Digital Rights establishes that the security measures provided for in the Spanish National Security Scheme must be applied. Royal Decree 311/2022 of 3 May, which regulates the National Security Scheme, came into force on 5 May 2022. Like the GDPR, this royal decree establishes that a risk analysis must be carried out to determine the technical and organizational security measures required.[2]

4.5 What if a research project is carried out jointly with other universities or organizations?

When two or more organizations (e.g. two or more universities) jointly determine the purposes and means of processing, they are considered joint controllers. For example, this situation may arise when research groups from different universities are working on a project and jointly define the types of data to be collected, the processing to be carried out, and the means to be used for processing. In this case, two research groups from different universities agree the type of data to be collected by means of an electronic form or the common platform where the data will be stored to carry out a project.

The joint controllers must enter into a "joint controllership arrangement for the processing of personal data" that sets out their respective responsibilities for compliance with the obligations imposed by the GDPR, particularly as regards responding to data subjects who choose to exercise their right to information.[3]

4.6 What if personal data are transferred outside the European Economic Area or to an international organization?

The transfer of data between organizations established in the countries of the European Economic Area (EU member states plus Iceland, Liechtenstein and Norway) is governed by the same rules that apply to transfers between organizations established in Spanish territory.

When data are sent to an organization located outside the European Economic Area (EEA) or to an international organization, this is called an "international transfer". Specific conditions apply in this case and must be taken into account by researchers. Specifically, personal data may not be transferred outside the EEA unless the country, territory or international organization to which they are to be sent ensures an "adequate level of protection of personal data" for data subjects. The EU considers that just over a dozen countries provide "adequate protection" for the transfer of personal data.[4]

2. For guidance on security measures that can be implemented, please consult the data protection website of the University of Barcelona (ub.edu/secretariageneral/ca/proteccio_dades/pd_recerca.html).

3. A model joint controllership arrangement is available on the University of Barcelona's data protection website (ub.edu/secretariageneral/ca/proteccio_dades/pd_recerca.html).

4. An updated list of countries to which personal data may be transferred on the basis of an adequacy decision issued by the European Commission can be found at aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales.

If you intend to share personal data with a research institution outside the EEA, or to contract a service provided from outside the EEA that is not located in one of the countries included on the list, the standard contractual clauses approved by the European Commission must be included in the relevant agreement.[5]

4.7 In what cases must a data protection impact assessment be carried out?

When processing involves a high risk to the rights and freedoms of data subjects, a data protection impact assessment must be carried out before processing begins.[6] To determine when a high risk exists, researchers can consult the indicative list of assessment criteria issued by the Catalan Data Protection Authority.[7] If two or more of the criteria indicated in the list apply, a data protection impact assessment must be carried out. In such cases, we recommend that you contact the University of Barcelona's data protection officer.[8]

5 Issues to consider with regard to the implementation phase of a research project

When the planning phase of a research project has been completed and the implementation phase is initiated, there are a number of data protection issues that should be considered.

5.1 How should participants be informed about the use of their personal data?

Before any personal data are collected, research project participants must be expressly, precisely and unambiguously informed of the following points, without prejudice to any other information that may be required from an ethical standpoint, either by the University of Barcelona's Bioethics Committee or under sectoral regulations (e.g. when biological samples are used):

a) The identity and contact details of the data controller, which, in the case of the University of Barcelona, is always the General Secretary's Office (even if it does not carry out the processing itself).[9]

b) The contact details of the data protection officer.[10]

c) The purpose of the processing, which is generally to manage and carry out the research project.

d) The legal basis for the processing:

---

5. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council can be found at eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

6. Regarding the data protection impact assessment, a guide published by the Catalan Data Protection Authority can be consulted at apdcat.gencat.cat/en/documentacio/guies_basiques/Guies-apdcat/Guia-sobre-la-evaluacion-de-impacto-relativa-a-la-proteccion-de-datos-en-el-RGPD.

7. The list of criteria issued by the Catalan Data Protection Authority for determining when a data protection impact assessment must be carried out can be found at apdcat.gencat.cat/web/.content/02-drets_i_obligacions/obligacions/documents/Lista-DPIA-CAT.pdf.

8. Contact details of the data protection officer: Gran Via de les Corts Catalanes, 585, 08007 Barcelona; <protecciodedades@ub.edu>.

9. Contact details of the Secretary General's Office: Gran Via de les Corts Catalanes, 585, 08007 Barcelona; <secretaria.general@ub.edu>.

10. Contact details of the data protection officer: Gran Via de les Corts Catalanes, 585, 08007 Barcelona; <protecciodedades@ub.edu>.

- As a general rule, the legal basis is the fulfilment of a mission carried out in the public interest, based on the provisions of Organic Law 2/2023, of March 22, of the University System, and Law 1/2003, of 19 February, on universities in Catalonia. In this case, explicit reference must be made to these two laws.
- When special categories of data are processed, the legal basis for the processing is the explicit consent of the data subject. In this case, it must also be stated that the data subjects have the right to withdraw their consent at any time, without retroactive effect.

e) The recipients or categories of recipients of the personal data.

f) The controller's intention to carry out international transfers of personal data to a third country or an international organization (if applicable). If transfers are made on the basis of an adequacy decision (i.e. to one of the states deemed to be safe) or with adequate safeguards (e.g. in accordance with standard contractual clauses), this must be specified. Participants must also be provided with information on how to obtain a copy of the relevant document, or the fact that a copy has been provided must be stated.

g) The time limit for storage or the basis for determining it.

h) The data subject's right of access to their personal data, to rectification or erasure, to restriction of processing, to object to processing, and to request data portability. It must also be indicated that these rights must be exercised by submitting a document, together with a photocopy of the data subject's national identity card or other valid identification document, to the General Secretary's Office.

i) The data subject's right to lodge a complaint with the Catalan Data Protection Authority.

j) The existence of automated decision-making, including profiling, if applicable; information about the logic involved; and the envisaged consequences for the data subject.

This information regarding the processing of personal data (provided in fulfilment of the "right to information") is usually included in the documents or forms provided to data subjects to inform them about the research project.[11]

Under current regulations, not all of the information indicated above needs to be provided in the body of an electronic form. Only the following points must be included: the identity of the data controller (in the case of the University of Barcelona, the General Secretary's Office), the purpose of the processing (in this case, to manage and carry out the relevant research project), the list of rights indicated in section *h*, and an email address where full information concerning the processing of personal data can be requested.

The form must also include a required tick box that enables the data subject to declare that he/she has read the information concerning the processing of personal data. If explicit consent[12] for the processing of personal data must be obtained because special categories of data are to be collected, a second box must be added so that by ticking it the data subject can also give consent for the processing of personal data in the terms indicated.

11. A model form for providing information on the processing of personal data is available on the University of Barcelona's data protection website (ub.edu/secretariageneral/ca/proteccio_dades/pd_recerca.html).

12. It is important not to confuse consent for the processing of personal data, which is covered by regulations on personal data protection, with informed consent, which may be required for ethical reasons or under other regulations (e.g. those governing clinical trials).

If the relevant data were not obtained directly from the data subject (e.g. when the research group has received them from another university), the data subject must be informed of all the points indicated above within one month of the date on which the data are received. The data subject must also be informed of origin of the data and the categories of data received.

In any case, it is important to retain proof that the above information has been provided and that the relevant consent has been obtained where applicable.

5.2 What if personal data are collected from foreigners?

If personal data are processed on national territory, they are subject to European and national data protection legislation, irrespective of the nationality and place of residence of the data subject. Therefore, foreign individuals participating in a project have the same right to have their data processed securely and can exercise the same rights over their personal data as nationals of any member state of the European Economic Area.

In such cases, the information concerning the processing of personal data indicated in the previous section must be provided in a language understood by the participant.

5.3 What if personal data are collected from minors?

In Spain, the minimum age for consenting to the processing of personal data is 14. If a project includes participants aged under 14, the holder of parental authority or the participant's legal guardian must grant consent.

However, in the case of health-related research projects, under sectoral regulations, minors aged 14 or over may give consent for the processing of their personal data to the extent that they are competent to understand the scope of the health intervention. Otherwise, the consent of the holders of parental authority or guardians is required, after the minor's views have been heard.

In the case of biomedical research projects (i.e. those involving the use of biological samples or genetic data), consent may only be given by participants aged 18 or over.

5.4 What if you need to contract a third party to provide a service?

If a third party is contracted to provide a service that requires the processing of personal data (e.g. transcription of interview recordings or a cloud storage service), that party is considered a "processor".[13]

In this case, the University remains responsible for ensuring that the third party complies with data protection regulations during the provision of the service and must therefore review the safeguards regarding data security and protection offered by the service provider before contracting it. In addition, certain points relating to data protection must be set out in the relevant contract or agreement.[14]

13. The processor should not be confused with the persons at the University of Barcelona who, in accordance with their functions, are authorized to process personal data.

14. A model data processing agreement is available on the University of Barcelona's data protection website (ub.edu/secretariageneral/ca/proteccio_dades/pd_recerca.html).

In any case, to better safeguard the privacy of individuals, we recommend that researchers use services provided by the University of Barcelona. Services provided by third parties should only be considered when the UB's internal services cannot meet the needs of a project.

5.5 What if university students need to process personal data for scientific purposes as part of a research project?

Students may only process personal data if they have the express permission of the principal investigator of the research project in which they are collaborating.

Researchers supervising university students who need to process personal data within the framework of a research project must inform them of the obligations established by data protection regulations (duty of secrecy, security measures, etc.). In such cases, we recommend that the students involved sign a declaration of confidentiality.[15]

Use of personal data by students must be limited to processing of the minimum amount of personal data necessary to achieve the relevant academic and scientific objectives.

Students may only delete personal data records or sets of personal data if they have the written authorization of the principal investigator of the research project.

5.6 What should I do when a data subject requests to exercise one of their personal data protection rights?

Data subjects have a series of rights aimed at ensuring their control over their personal data; namely, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to object to processing, and the right to portability. If a data subject requests to exercise one or more of these rights, their request must be sent to the General Secretary's Office as soon as possible, given that this office, as the data controller, is responsible for handling such requests within one month, without prejudice to the collaboration of the principal investigator, which will be required to give effect to the right exercised.

6 Issues to consider with regard to the publication of research results and retention of data

A number of points must be taken into account in the phase when the results of a research project are published and with regard to retention of the data processed.

6.1 Will you publish the research results with anonymous or anonymized data?

As a general rule, research results should be published with anonymous or anonymized data.

In the exceptional event that personal data (i.e. information that allows participants to be identified) must be published, participants must be informed in advance (e.g. in the section on recipients of the information) and, where applicable, their consent must be obtained.

15. A model declaration of confidentiality is available on the University of Barcelona's data protection website (ub.edu/secretariageneral/ca/proteccio_dades/pd_recerca.html).

6.2 Have you considered making the data reusable?

If research data are organized, documented, stored and made available for sharing, they can be reused. This means they can have a useful life that is longer than the duration of the research project for which they were collected. Bear in mind that providers of research funding and scientific journals may expect you to share the data obtained or the data underlying published results.

To do this, the data must first be anonymized. Only in exceptional cases where the data cannot be anonymized is it necessary to have informed the participants in advance.

6.3 How long can personal data be stored?

Personal data cannot be stored for longer than is necessary to achieve the purpose for which they were collected; that is, longer than is required to carry out the research project and publish the results obtained.

Researchers must therefore consider when data that allow participants to be identified can be deleted or anonymized. This is the point at which personal data are deemed to be no longer necessary. In some cases, it is necessary to retain the data beyond that point. This may be required by the rules of a call for applications or because a complaint about the use of the data has been lodged with a data protection supervisory authority.

Once this period has expired, the personal data (including the documents in which information about the project is provided and the participant's consent is obtained) must be blocked. In other words, the data must be identified and frozen by adopting appropriate technical and organizational measures to prevent their processing and ensure their authenticity and blocking date (e.g. by keeping them encrypted and separate from other project data). They may only be used when they must be made available to judges and courts, the Public Prosecutor's Office, or competent public administrative bodies, particularly data protection authorities, for the purpose of enforcing any liabilities arising from their processing. As a general rule, we recommend that researchers block data for three years from the date when processing was completed, given that this is the statute of limitations for the most serious breaches of data protection regulations.

In the case of longitudinal studies, it is understood that the data obtained during the initial project are still required and can therefore be retained for use in the subsequent project. However, participants must have been informed that for the purpose of carrying out a longitudinal study, their personal data will be retained for a period longer than the duration of the project in which they are participating. In studies of this kind, participants in the initial project are usually informed that they may be contacted to invite them to participate in the subsequent project, and that if they opt not to do so, the personal data obtained during the initial project will be anonymized.

6.4 How are personal data deleted?

Personal data used in research must be anonymized or destroyed when they are no longer required for the purpose for which they were collected. If they are anonymized, they are no longer personal data and are therefore not subject to personal data protection regulations.

When personal data must be deleted, we recommend taking the following steps:

- Paper documents containing personal data should be destroyed using paper shredders.
- Whenever possible, data recorded in digital format should be destroyed by using an overwriting algorithm. If the delete function of a computer is used or a simple disk reformat is done, data are usually not permanently erased.

- Data held on non-rewritable digital media such as CDs or DVDs should be disposed of by destruction of the physical media (e.g. by shredding).

If equipment that has contained personal data is to be donated, we recommend removing the hard disks before handing it over.

7 References

7.1 Regulations

- Council of Europe Convention No 164, of 4 April 1997, for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine.
- Law 21/2000, of 29 December, on rights to information related to health and patient autonomy, and clinical documentation.
- Law 41/2002, of 14 November, regulating patient autonomy and rights and obligations related to clinical information and documentation.
- Law 14/2007, of 3 July, on biomedical research.
- Organic Law 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights.
- Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- Royal Decree 311/2022, of 3 May, which regulates the National Security Scheme.

7.2 Online resources

- Spanish Data Protection Agency. (2018). *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD*. <https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf>
- Spanish Data Protection Agency. (2021). *10 Misunderstandings Related to Anonymisation*. <https://www.aepd.es/es/documento/10-anonymisation-misunderstandings.pdf>
- Spanish Data Protection Agency. (2021). *Garantías para las transferencias de datos personales a terceros países u organizaciones internacionales*. <https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales>
- Catalan Data Protection Authority. (2018). *Guia per al compliment del deure d'informar a l'RGPD*. <https://apdcat.gencat.cat/ca/documentacio/guies_basiques/Guies-apdcat/guia_per_al_compliment_del_deure_d_informar_RGPD>
- Catalan Data Protection Authority. (2019). *Guia pràctica sobre l'avaluació d'impacte relativa a la protecció de dades*. <https://apdcat.gencat.cat/ca/documentacio/guies_basiques/Guies-apdcat/Guia-sobre-la-evaluacion-de-impacto-relativa-a-la-proteccion-de-datos-en-el-RGPD>
- Catalan Data Protection Authority. (2019). *Llista de tipus de tractaments de dades que requereixen avaluació d'impacte relativa a la protecció de dades*. <https://apdcat.gencat.cat/web/.content/02-drets_i_obligacions/obligacions/documents/Lista-DPIA-CAT.pdf>

- European Commission. (2018). *Ethics and data protection*. <https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf>
- European Commission. (2021). "Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council". <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN>
- Commission Nationale de l'Informatique et des Libertés. (2018). *L'analyse d'impact relative à la protection des données (AIPD)*. <https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd>
- European Data Protection Board. (2019). "Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) [Article 70(1)(b)]". <https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf>
- Article 29 Data Protection Working Party 29. (2014). "Opinion 05/2014 on Anonymisation Techniques". <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>
- Imperial College London. (2021). *Guide 4 – Research*. <https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/internal-guidance/guide-4---research>
- European Data Protection Supervisor. (2020). "A Preliminary Opinion on data protection and scientific research". <https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf>
- University of Cambridge. (2018). *Academic Research Involving Personal Data: Quick Guide*. <https://www.research-integrity.admin.cam.ac.uk/academic-research-involving-personal-data>
- University of Oxford. (2018). *Data protection & research*. <https://researchsupport.admin.ox.ac.uk/policy/data#/collapse470516>
- Pompeu Fabra University. (2021). *Recerca i dades de caràcter personal*. <https://www.upf.edu/web/proteccio-dades/recerca-i-dades-de-caracter-personal>