FORS GUIDES
to survey methods
and data management

Data protection: legal considerations for research in Switzerland

Pablo Diaz [1]

[1] FORS - UNIL

FORS Guide No. 17, Version 1.0

January 2022

Abstract:

The advent of Open Science poses a number of challenges for researchers with regard to research data management. Amongst the most salient is the necessary balance between data protection and openness. This guide aims to clarify the rights and obligations of researchers regarding the protection of personal data, following the main questions that should be asked before conducting a research project.

Keywords: data protection, data management, open research data, open science

How to cite:

Diaz, P. (2022). *Data protection: legal considerations for research in Switzerland*. FORS Guide No. 17, Version 1.0. Lausanne: Swiss Centre of Expertise in the Social Sciences FORS. doi:10.24449/FG-2022-00017

The FORS Guides to survey methods and data management

The FORS Guides offer support to researchers and students in the social sciences who intend to collect data, as well as to teachers at university level who want to teach their students the basics of survey methods and data management. Written by experts from inside and outside of FORS, the FORS Guides are descriptive papers that summarise practical knowledge concerning survey methods and data management. They give a general overview without claiming to be exhaustive. Considering the Swiss context, the FORS Guides can be especially helpful for researchers working in Switzerland or with Swiss data.

Emilie Morgan de Paula (emilie.morgandepaula@fors.unil.ch)
Giannina Vaccaro (Giannina.Vaccaro@unil.ch)

FORS, Géopolis, CH-1015 Lausanne
www.forscenter.ch/publications/fors-guides
Contact: info@forscenter.ch

Acknowledgement:

I warmly thank Benjamin Amsler for his attentive proofreading, his pertinent advice and his precious inputs. His contributions were more than essential to the writing of this guide. I am also very grateful to Emilie Morgan de Paula and Brian Kleiner for their valuable feedback.

1. INTRODUCTION

The advent of the digital revolution has put the processing of personal data at the heart of public debate. While the constant increase in available data represents for some an opportunity for economic growth and progress, for others it constitutes a major threat to the fundamental rights of individuals. Indeed, informational self-determination[1], as guaranteed by the Universal Declaration of Human Rights (art. 12), the European Convention on Human Rights (art. 8) and the Swiss Federal Constitution (art. 13 par. 2), is undermined by the often abusive use of personal data. In response to this, many governments have decided to strengthen their data protection policies. The introduction of the 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 – better known as the GDPR – as well as the ongoing revision of the Federal Act on Data Protection (FADP) are good examples of this trend. While these legal measures seem to be mainly aimed at major private companies (such as Google, Facebook, Apple, etc.), they impact all sectors whose core activities are based on the processing of personal data, including scientific research – particularly in the social sciences. In parallel to this "protective impulse", public research funding institutions are increasingly requiring that the data produced by the projects they support be shared in the name of Open Science. The Swiss National Science Foundation (SNSF) requires, for example, the researchers it funds to archive the data they produce during their projects and to share it with other researchers – unless major legal, ethical, copyright or confidentiality requirements prevent this.

Many researchers are concerned about these new injunctions and the tensions they create – particularly between protection and openness – and wonder what they are allowed or not allowed to do in their work. This guide aims to provide some answers to these questions from the perspective of Swiss law. More specifically, it will clarify – in a general way – the rights and obligations of researchers affiliated with public institutions[2], based on the main questions that should be asked before conducting a research project:

- Does my research project involve personal data?
- Am I processing personal data?
- What personal data legislation applies to my research?
- Under what conditions is it possible to collect personal data?
- What information should be given to data subjects?
- How long can personal data be kept?
- Is it possible to share my research data?
- Is there a research privilege?

For reasons of clarity, this guide is based primarily on Swiss federal legislation. More specifically, it relies on the federal law of 25 September 2020 on personal data (new Federal

[1] The notion of informational self-determination refers to the idea that individuals should be able to decide for themselves when and to what extent their private information can be disclosed to others.
[2] This guide is based on the special legal provisions to which researchers affiliated with public sector institutions are subject. Research conducted by private individuals or companies is covered by general provisions that are not addressed here.

Act on Data Protection here abbreviated nFADP), which should come into force in 2022.[3] However, it is important to keep in mind that universities and universities of applied sciences are primarily subject to cantonal laws. This said, as the content of federal and cantonal laws is generally quite similar, the considerations and good practices presented in this paper remain valid for the entire research community. Finally, this guide does not take into account the special legal provisions applicable to research projects carried out by the Swiss Federal Institutes of Technology (ETH) or to research projects falling within the scope of the Human Research Act (HRA).

2. DATA PROTECTION IN 8 QUESTIONS

In this section we will look at the main questions that should be asked about data protection when starting a research project. General legal considerations, good practices, and concrete examples will be presented.

2.1 DOES MY RESEARCH PROJECT INVOLVE PERSONAL DATA?

The first question to ask before conducting a research project is whether it involves personal data. This is an important question since, if this is not the case, personal data protection legislation does not apply. In other words, if a research project does not involve any personal data (e.g. if the data are completely anonymous[4] or if the research project is on a subject that does not involve human beings), there is no need to worry about this particular area of the law.

The nFADP considers personal data to be all information relating to an identified or identifiable natural person (art. 5 let. a). Some common examples of personal data are:

- A name
- An address
- A telephone number
- An IP address
- A picture of somebody
- A voice recording
- An iris scan
- Etc.

Some personal data may be more subtle than the examples given above, as they may identify individuals indirectly. For example, the following may be considered as personal data depending on the context:

- A position held by only one person at a time (e.g. president of a given country, CEO of a specific company, etc.)
- A title or distinction (e.g. 1968 cycling Olympic champion, winner of the 2016 Nobel prize for literature, etc.)

[3] As the law has not yet been translated into English, the translations in this guide are those of the author.
[4] Note that with the ever-increasing amount of data available and, with that, the ability to link more and more information, anonymization has become an almost impossible exercise. More developments on the challenges of anonymization are available in the dedicated FORS Guide (Stam & Kleiner, 2020).

- The way of moving, walking, dancing, etc.
- The way of writing text[5], computer code, etc.

From the moment it is linked to an identified or identifiable person, all information becomes personal. For example:

- “63 people graduated in criminal sciences in 2020” is not personal data but,
- “John Smith graduated with a degree in criminal science in 2020” is personal data.

Note that making personal data public does not make it lose its status. Information related to identified or identifiable persons available online (e.g. on social networks, blogs, websites, etc.) remains personal data.

Sensitive data: a sub-category of personal data

Certain categories of personal data must be qualified as sensitive. This qualification is far from being a detail in the sense that sensitive data must be handled with extra care. Qualifying data as sensitive is not done subjectively, but according to the delimitations set by the applicable legislation. According to the article 5 letter c of the nFADP, sensitive personal data refers to:

- Personal data on religious, philosophical, political or trade union opinions or activities;
- Personal data on health, intimacy or racial or ethnic origin;
- Genetic data;
- Biometric data univocally identifying a natural person;
- Personal data on criminal and administrative proceedings or sanctions;
- Personal data on social security measures.

The lists of categories of sensitive data are exhaustive. If information processed in the context of a research project does not correspond to one of the categories provided for by the law, it should not be considered as sensitive (e.g. a person's salary is personal data but does not constitute sensitive data).

2.2 AM I PROCESSING PERSONAL DATA?

Once the presence or absence of personal data has been determined, it is appropriate to check what the law describes as “processing” is being carried out. It is important here to distance oneself from the vocabulary of certain scientific fields, since processing in the legal sense does not only refer to digital manipulation of data.

The nFADP defines the processing of personal data as any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, recording, storage, use, revision, disclosure, archiving, erasure or destruction of data (art. 5 let. d). From this definition, we see that the operations that correspond to processing are diverse and numerous. Thus, any operation carried out with personal data is a “processing”, even including use.

Conducting a social science project often involves several types of personal data processing. For example, when conducting individual interviews, a researcher will collect information about the participants, record it on a medium, carry out analytical operations, transmit data to other researchers, etc. All of these operations constitute processing.

[5] A good example of this is the case of Elena Ferrante. Indeed, after many years of mystery, efforts to unmask the identity of the novelist behind the pseudonym "Elena Ferrante" have been crowned with success. Thanks to the work of a research team who, through analyses of a corpus of Italian novels, concluded that it was the work of a single pen, namely that of Domenico Starnone (Tuzzi & Cortelazzo, 2018).

2.3 WHAT PERSONAL DATA LEGISLATION APPLIES TO MY RESEARCH?

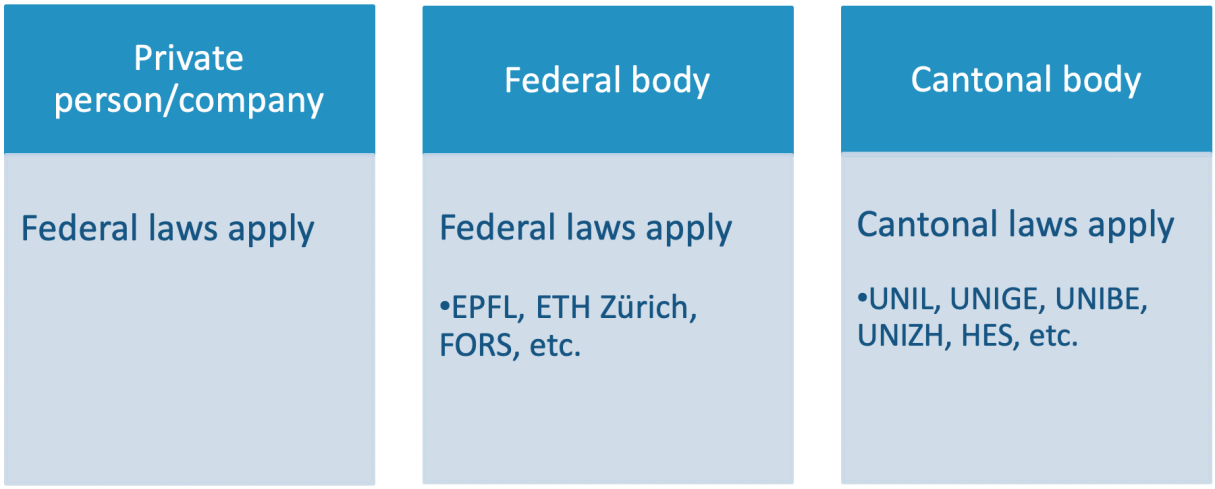
To determine the legal regime applicable to a research project, two sub-questions need to be addressed:

- Who am I?
- Is there any special law applicable to my research?

Who am I?

The "legal status" of the person processing personal data largely determines which general data protection law applies.

For example, while federal bodies (ETH, national research institutions, etc.) and private individuals are subject to federal law (nFADP), cantonal bodies (universities, universities of applied sciences, university hospitals) are subject to cantonal laws on data protection.



It is important to note, however, that for some research projects, particularly in the context of mandates or collaborations between cantonal and federal bodies, the question will arise as to which law applies to the various partners involved in the research with regard to the processing operations.

Finally, it may be interesting to note that no data protection laws apply to research conducted by an individual for strictly personal use (e.g. genealogical research that is not published).

Is there any special law applicable to my research?

Answering this question requires knowledge of the "normative landscape" in order to be able to determine whether there is a special law applicable to the researcher or to the field in which the research is conducted.

Depending on the identity or the sector of activity of the researcher, a number of specific laws may be relevant. For example:

- Researchers working on human diseases as well as the structure and function of the human body are subject to the Human Research Act (HRA);
- Researchers affiliated with institutions belonging to the Federal Institutes of Technology Domain are subject to the Federal Act on the Federal Institutes of Technology (ETH Act);

- Researchers affiliated with universities or universities of applied science are subject to the cantonal laws governing such institutions;
- Research involving materials of high historical value may be subject to federal or cantonal archiving laws;
- Research involving data provided by the Federal Statistical Office (FSO) may be subject to the Federal Statistics Act (FStatA).

It is important to be aware of these special laws and their provisions on the protection of personal data, since they complement, or in some cases take precedence over, the general laws on data protection. It is therefore advisable to examine the normative framework before starting a research project.

2.4 UNDER WHAT CONDITIONS IS IT POSSIBLE TO COLLECT PERSONAL DATA?

The nFADP provides for different regimes for private persons and federal bodies. In this section, we will only present the special provisions for the processing of personal data by federal bodies, as these are closest to the cantonal laws to which researchers are generally subject as employees of public institutions.

Researchers affiliated with federal bodies may process personal data if there is a statutory basis for doing so. With regard to the processing of sensitive data and profiling, the legal basis must be provided by a formal enactment (art. 34 par. 1 & 2 nFADP).

In the absence of a legal basis, researchers affiliated with federal bodies may process personal data only under certain conditions. The most common is that the data subject – i.e. the research participant – has consented to the processing in question.

Since laws that explicitly allow the processing of personal and sensitive data are rare – the ETH Act is one of the few that does so in Switzerland – we recommend always obtaining the consent of individuals. Such consent is valid only if given freely (in some cases an explicit consent is even required) and on the provision of adequate information, as detailed in the next section.

2.5 WHAT INFORMATION SHOULD BE GIVEN TO DATA SUBJECTS?

Researchers affiliated with federal bodies have an absolute duty to inform data subjects of any collection of personal data. This duty to provide information also applies where the data are collected from third parties (i.e. when personal data are not collected directly from the data subject). More precisely, the article 19 of the nFADP stipulates that data subjects must be provided with at least the following information:

- The identity and contact details of the data controller;
- The purpose of the processing;
- Where applicable, the recipients or categories of recipients to whom personal data are disclosed; and
- Where personal data are disclosed abroad, the name of the State or international body to which they are disclosed.

In the context of a research project, this information will generally be as follows:

The identity and contact details of the data controller	The data controller is the entity, private person or federal body that, alone or jointly with others, decides on the purposes and means of processing personal data. Generally, this will be the Principal Investigator (PI) and/or his/her team, on behalf of their home institution.
The purpose of the processing	In the context of a research project, the purpose of processing is usually to complete the project by producing analyses, reports, publications, etc.
The recipients or categories of recipients to whom personal data are disclosed	This is to inform the research participants if the data are, for example, transmitted to organizations outside the research team (subcontracting for instance). Note that using cloud storage services (such as Dropbox, etc.) is considered a disclosure (subcontracting type).

It should be noted that this information must always be provided, even if the personal data are not collected directly from the data subject, unless an exception is made – for example when the information is impossible to transmit or requires disproportionate efforts (art. 20 nFADP).

Note that the Federal Data Protection and Information Commissioner (FDPIC) recommends being generous and not hesitating to add information such as[6]:

- Anonymization/pseudonymization of data (possibility of re-identification, if so in which cases, who holds the correspondence list, who has access to it and in which cases), retention (form, duration) and re-use of data;
- The contract and confidentiality obligations with third parties;
- The possibility for the data subject to be informed of the results of the research.

Giving the above information to research participants can be combined with obtaining their consent. Swissethics provides useful templates for consent forms on its website.[7]

2.6 HOW LONG CAN PERSONAL DATA BE KEPT

The article 6 paragraph 4 of the nFADP stipulates that personal data must be destroyed or anonymized as soon as they are no longer required for the purposes of processing.

First, it should be noted that researchers have two options: to delete all of their entire materials or to anonymize all personal data. The second option, however, may be very complicated – if not impossible – and time consuming depending on the type of data collected (e.g. interview transcripts that run to many pages and contain many direct and indirect identifiers). Furthermore, anonymization of data is risky, as even if a lot of information is removed, the

[6] https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/statistik--register-und-forschung/recherche/protection-des-donnees-et-recherche-en-general.html
[7] https://swissethics.ch/en/templates/studieninformationen-und-einwilligungen

likelihood of re-identification may remain high. Moreover, technological advances and the increase in available data may in the future allow re-identification that seems impossible today.

Second, it is essential to set the correct storage period as early as possible in the research design process. Indeed, setting a storage period that is too short could prove problematic as time goes by. In this regard, the purpose of the processing is a key notion in the sense that it determines the time limit for the retention of personal data. The retention period will therefore not necessarily be equivalent to the duration of the research funding and will not end with the first scientific publication based on the research data. It is therefore preferable to provide for retention periods that take into account the time needed for full exploitation of the data, including archiving for re-use where this is desired and possible. Note that while the nFADP does not provide any precise indication as to the maximum conservation period, one can, by analogy, estimate this period at 20 years as recommended by the ETH Act (art. 36d par. 2). Even if the storage period is not included among the minimum information to be communicated to data subjects, in our opinion it is appropriate to clearly inform participants in a research project not only of its objectives, but also of its temporality.

2.7 IS IT POSSIBLE TO SHARE MY RESEARCH DATA?

The sharing of data constitutes a special kind of processing known as “disclosure”. As with any processing, disclosing data requires a legal basis (art. 36, par. 1 nFADP). However, this requirement may not apply to disclosure for research purposes (art. 39 nFADP). Indeed, it is possible for researchers affiliated with federal bodies to share personal and sensitive data with other researchers if a certain number of conditions are met, which are detailed below.

While disclosure of data for research purposes may be justified even without consent, researchers affiliated with federal bodies are still required to inform the individuals whose data are disclosed. This said, the nFADP relieves researchers affiliated with federal bodies of the duty to inform when collecting personal data from third parties, if the duty to inform is impossible to comply with or requires disproportionate efforts (art. 20, par. 2). It is conceivable that if individuals are difficult to trace – old or very large amounts of data – researchers need not systematically provide information.

Disclosure abroad

If the researcher plans to disclose the data abroad, a number of special legal provisions apply. The article 16 paragraph 2 of the nFADP stipulates that personal data may be disclosed abroad if the Federal Council has established that the State concerned has legislation ensuring an adequate level of protection or that an international body guarantees an adequate level of protection. The FDPIC maintains a list of countries offering such guarantees. It is therefore necessary in each individual case to examine whether the country of destination is on this list or not.

The articles 16 paragraph 2 and 17 paragraph 1 of the nFADP provide for a number of exceptions to the principle of prohibiting the disclosure of data abroad in the absence of an adequate level of protection in the country of destination. The most “likely” ones in the context of the research are:

- The existence of an international treaty;
- The existence of data protection clauses in a contract between the controller or processor and its co-contractor (previously communicated to the FDPIC);

- The existence of standard data protection clauses previously approved, established or recognized by the FDPIC;
- The fact that the data subject has expressly given his/her consent to the disclosure of their personal data;
- The fact that the data subject has made the personal data accessible to everyone and has not expressly objected to the processing.

Sharing data through an archive

The provision of research materials containing personal data via archive services (such as FORS) raises a number of challenges. Indeed, as we have seen, the nFADP requires that individuals be informed whenever their data are collected, whether directly from them or from a third party. This makes the task of disseminating research data through dedicated infrastructures considerably more complex when personal data are involved.

This said, it is conceivable that a research project could be designed from the outset in such a way that it includes data sharing among its objectives. The purposes of the processing (study goals) and the categories of recipients (researchers who would have access to the data) should, however, be recognizable. A research project that deviates from the initial topic is therefore likely to be problematic. The challenge is, thus, to be specific enough to properly inform the data subject while being broad enough to allow the deposit and the sharing.

2.8 IS THERE A RESEARCH PRIVILEGE?

The article 39 of the nFADP provides relief from the general data protection rules when federal bodies process personal data for purposes not relating to individuals, in particular in the context of research (research privilege).

This provision concerns exclusively "second-hand" data (the collection of data for research purposes is not included in this exception regime) and applies both when the federal body processes itself data for research purposes and when it communicates them to other bodies (federal or cantonal) or to private persons.

More specifically, the "research privilege" allows the following exemptions:

- Data can be processed for purposes other than those for which they were collected;
- There is no longer a need for a formal law for the processing of sensitive data or profiling;
- There is no longer a need for a legal basis for the communication of personal data.

For research privilege to apply, however, a number of conditions must be met:

- The data are anonymized as soon as the purpose of the processing allows it;
- The federal body only discloses sensitive data to private persons in a form that does not allow the persons concerned to be identified;
- The recipient shall only disclose the data to third parties with the consent of the federal body that transmitted the data;
- The results of the processing are published only in a form which does not allow the data subjects to be identified.

By providing a legal basis, the research privilege makes it possible to justify processing personal data for research purposes without necessarily having to obtain consent. However, as we saw, this privilege does not exempt federal bodies from the duty to inform. Moreover,

researchers must always respect the general principles laid down by the articles 6 and 8 of the nFADP.

If researchers cannot ensure compliance with the conditions of research privilege (anonymization of data as soon as the purpose of the processing permits and non-identifying publication) the general data protection regime applies. The principle that personal data may only be collected for specified purposes that are recognizable to the person concerned and must be further processed in a way compatible with these purposes will therefore apply.

3. PRACTICAL RECOMMENDATIONS

Recommendation 1 – If the data are complex and/or massive, it is best to assume that they are personal data.

Recommendation 2 – Always inform people fully and accurately when collecting data. The information to be provided is: the identity and contact details of the data controller; the purpose of the processing; where applicable, the recipients or categories of recipients to whom personal data are disclosed; and where personal data are disclosed abroad, the name of the State or international body to which they are disclosed.

Recommendation 3 – Always obtain consent from individuals to participate in a research project and keep a record of it.

Recommendation 4 – When data sharing is possible and desired, provide for it in the information given to participants.

Recommendation 5 – Provide a timeframe that allows for adequate storage for data use and sharing where possible.

4. FURTHER READINGS AND USEFUL WEB LINKS

Two good books that can help introduce you to the issue of data protection are Meier (2011), in French, and Belser et al. (2011) in German.

The European Commission (2021) has published an excellent guide on the issue of ethics and data protection in relation to the GDPR. See: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

The online tool "DMLawTool" (Data Management Law Tool) answers questions about copyright and data protection law relating to research data management. See: https://dmlawtool.ccdigitallaw.ch/

The website of the Federal Data Protection and Information Commissioner provides useful information relating to research. See: https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/statistik--register-und-forschung/recherche.html

The Swissethics website gives good examples of information and consent sheets. See: https://swissethics.ch/en/templates/studieninformationen-und-einwilligungen. We also recommend our FORS Guide dedicated to informed consent (Kruegel 2019).

REFERENCES

Meier, P. (2011). Protection des données : fondements, principes généraux et droit privé. Stämpfli.

Besler, E. M., Epiney, A., & Waldmann, B. (2011). Datenschutzrecht. Grundlagen und öffentliches Recht. Stämpfli: Bern, Berlin und München.

Council of Europe (1952). The European convention on human rights. Strasbourg: Directorate of Information.

European Commission (2021). Ethics and Data Protection. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

Federal Act on Data Protection (FADP) of 19 June 1992 (1992). https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en

Federal Act on Research involving Human Beings (Human Research Act, HRA) of 30 September 2011 (2011). https://www.fedlex.admin.ch/eli/cc/2013/617/en

Federal Act on the Federal Institutes of Technology (ETH Act) of 4 October 1991 (1991). https://www.fedlex.admin.ch/eli/cc/1993/210_210_210/en

Federal Constitution of the Swiss Confederation of 18 April 1999 (1999). https://www.fedlex.admin.ch/eli/cc/1999/404/en

Federal Statistics Act (FStatA) of 9 October 1992 (1992). https://www.fedlex.admin.ch/eli/cc/1993/2080_2080_2080/en

Kruegel, S. (2019). The informed consent as legal and ethical basis of research data production. FORS Guide No. 05, Version 1.0. Lausanne: Swiss Centre of Expertise in the Social Sciences FORS. https://forscenter.ch/fors-guides/fg-2019-00005/

Loi fédérale sur la protection des données (nFADP) du 25 septembre 2020. https://www.fedlex.admin.ch/eli/fga/2020/1998/fr

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) (2016). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679

Stam, A., & Kleiner, B. (2020). Data anonymization: legal, ethical, and strategic considerations. FORS Guide No. 11, Version 1.0. Lausanne: Swiss Centre of Expertise in the Social Sciences FORS. https://forscenter.ch/fors-guides/fg-2020_00011/

Tuzzi, A., & Cortelazzo, M. A. (2018). What is Elena Ferrante? A comparative analysis of a secretive bestselling Italian writer. Digital Scholarship in the Humanities, 33(3), 685-702.

United Nations (1948). Universal declaration of human rights. Retrieved from: https://www.un.org/en/about-us/universal-declaration-of-human-rights