Guidelines on 'informed consent' when conducting scientific research

Consent is a commonly used legal basis[1] for the processing of personal data for the purpose of scientific research. This document deals with obtaining consent that is legally valid under the AVG/GDPR[2].

The first sentence above referred to three basic concepts that are critical in this context: 'personal data', 'processing' and 'legal basis'. We will first briefly discuss these three key concepts, after which we will provide a detailed outline of what is needed to obtain legally valid 'informed consent'.

Contents

[1] The GDPR sets out six legal bases for the processing of personal data (see Article 6 of the GDPR).

[2] The GDPR (General Data Protection Regulation), known in Dutch as the *Algemene Verordening Gegevensbescherming* (AVG), has been in force in the entire European Union since May 2018 and sets out how individuals and organisation must deal with the personal data of European citizens. For certain aspects covered by the GDPR, individual Member States may lay down more detailed provisions in national law. In the Netherlands, these detailed provisions concerning the GDPR are laid down in the Dutch General Data Protection Regulation (Implementation) Act (*Uitvoeringswet Algemene Verordening Gegevensbescherming*). Whenever this document refers to the GDPR, it also refers to the Dutch GDPR (Implementation) Act.

Summary – Step by step

1. Establish that participants are able to legally give their free consent. In the case of a relationship of dependence (employer/employee, teacher/student) this is not the case. In that case, you cannot rely on 'consent' as a legal basis for participation in your research.
2. Determine specifically what you are requesting consent for and describe this purpose as clearly as possible. This will form the basis for your declaration of consent.
3. Draw up a text in language that is easy to understand for your participants, in which you inform participants, among other things, about all aspects of the research and the role the participants' personal data plays within that context.
4. In all your communication, you must emphasise that participation is entirely voluntary, that participants are in no way obliged to take part, that refusal will not have any negative impact, and that participants can withdraw their consent at any time.
5. Collect the declarations of consent so that you are able to demonstrate that all participants have legally given their consent.
6. Retain the declarations for as long as any non-anonymised personal data of the participants is retained.

Key concepts

Personal data

In the GDPR, personal data is defined as 'any information relating to an identified or identifiable natural person ("data subject") […]'. As such, it relates to a living natural person about which the personal data provides information (hereafter referred to as 'participant'). Individuals are more easily identifiable within a small group than within a large group, which is why the personal data of individuals in a small group must be handled more carefully.

The term personal data covers far more data than most people realise. For example, the answer to a yes/no question is also personal data when it can be linked to a particular respondent. The image on the following page provides examples of personal data divided into categories (also available on the UU Intranet).

See also: What is personal data? – (UU Intranet)
What should I consider when handling personal data? – (UU Intranet)
Research Data Management Support – Handling Personal Data

Anonymised and pseudonymised personal data

Anonymised data refers to data from which the identifying link with the participant has been permanently removed. In the case of truly anonymised data, it is impossible to find out who has participated in a study. Anonymised data no longer constitutes personal data and this means that it is no longer covered by the GDPR. However, please note that by combining multiple anonymised pieces of data that relate to different aspects of the same person, it is

often still possible to identify that individual – particularly if the individual concerned is a member of a specific, defined group or community. Anonymisation is a highly specialised process. Simply removing the individual's name is rarely ever sufficient, especially given current technology and the digital availability of data.

For that reason, often times pseudonymised data will be used instead of anonymised data. In the case of this type data, the identity of the participant can still be retrieved through the use of additional information. As such, pseudonymised data still qualifies as personal data, but due to the extra step that is needed to be able to identify individuals on the basis of this data, it will (often) require a lower level of security.

With pseudonymisation, a key is often used through which research can be linked to specific participants. By erasing the key, you make the data anonymous; individual participants can then no longer be identified from the research data. You should always ask yourself for how long the key may be retained. The general rule is: do not retain the key any longer than necessary. As long as you can provide valid arguments as to why you need the key, you may retain it. 'Because it's convenient' is not a good enough reason![3]

Audio and video

Many studies involve making audio and video recordings, which by definition do not qualify as anonymous data, because even with the use of voice distortion or use of blurred images or silhouettes, someone might still be able to establish the identity of the interviewee. Please keep this in mind – also when making recordings via Teams, for example.

Anonymous data

A study is completely anonymous:

- if identifiable personal data has never been requested or recorded;
- if, even when combining several sets of data, it is not possible to identify the person from whom the data originated;
- if there is no way to link the data to a natural person;
- if the key used to link pseudonymised data to a natural person has been permanently destroyed.

Please refer to: Anonymisation and pseudonymisation – (UU Intranet)

Special categories of personal data

Article 9 of the GDPR is dedicated to special categories of personal data[4], which constitute a separate category. These types of data are particularly sensitive due to their nature, in particular because they could give rise to discrimination, racism and exclusion. The processing of special categories of personal data is prohibited, but there are some exceptions. Conducting

[3] Erasing the key can have an added benefit for your research: once you have erased the key, participants can no longer withdraw their consent, as it is no longer possible to determine which data belong to whom. This makes erasing the key a win-win: the privacy of the participants in your research is better protected, and your data are no longer jeopardised by the withdrawal of consent.

[4]The following categories of personal data are considered to be special categories of personal data: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; biometric data for the purpose of uniquely identifying a natural person; data concerning health; data concerning a natural person's sex life or sexual orientation.
In addition, all data relating to an individual's criminal history is subject to stringent rules.
The processing of Citizen Service Numbers (BSN) within the context of scientific research is in principle prohibited.

scientific research may constitute such an exception. Special categories of personal data require (far) stronger protection and security measures than 'normal' personal data.

NB Although the processing of special categories of personal data for the purpose of scientific research is therefore not (in principle) prohibited, these types of processing always will require a legal basis – in most cases that basis will be 'consent' (see **Legal basis**).

Processing

The term 'processing' refers to *any operation you can perform on personal data*. This includes manual and automatic processing, for example: recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, analysis, transmission, dissemination or otherwise making publicly available, combination, restriction, erasure or destruction of data. As such, please keep in mind that 'retention' and 'erasure' for example also fall under the definition of processing.

It makes no difference whether you are processing the personal data yourself or instructing others to do so: these operations will still constitute 'processing' and you will remain responsible for them in your capacity as the data controller.

Legal basis

In order to process personal data, you need a legal basis. That legal basis answers the question as to *why you have the right* to process that data. In the context of scientific research, there are, generally speaking, three relevant bases*: consent, the public interest* and the *legitimate interest*. Out of the above, consent is by far the most common basis. Only under specific conditions will you be able to rely on the public interest or legitimate interest as a basis, for example in cases where it is impossible or extremely laborious to request the consent of all parties involved or where requesting consent would affect the results. Even in such cases, numerous additional requirements would apply.

Please note! If you are not working on the basis of consent within your study, please always contact the Privacy Department: privacy.gw@uu.nl.

Please refer to: Which legal bases for processing exist? – (UU Intranet)
When do I use consent as a legal basis for processing? – (UU Intranet)

Consent

The GDPR defines the 'consent' of the data subject (participant) as follows in Article 4:

> ***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;*

The terms outlined in bold are essential to legally obtained consent. Below is a detailed description of what is meant by these terms:

- **Freely:** this means that participants can freely decide and may not suffer any adverse consequences if they do not provide consent (for example, a participant need not deregister if he or she did not register themselves in the first place);
- **Specific:** consent must be given for a specific and well-defined purpose. The data may not be reused or stored indiscriminately, for example, for reasons of convenience. The GDPR offers slightly more flexibility in the context of conducting scientific research.
- **Informed:** before participants give their consent, they must be fully aware of the purpose and intended use of the data. It must be clear to them that consent is being requested and for what specific and well-defined purpose this is being done and it must be specified as exactly as possible what data will be collected from them, such as: name, contact details, date of birth, research data (to be specified!), audio or video recordings, etc.;
- **Unambiguous:** in the definition, the concept makes an appearance twice: first, as an unambiguous indication of the participant's wishes and, second, as a clear affirmative action. The bottom line is that there should be no doubts as to whether the participant has given his[5] consent and what he has consented to;
- **Statement:** the participant may sign a statement confirming that he or she has consented to the intended processing activities;
- **Affirmative action:** giving consent requires a so-called 'affirmative action', such as signing a form or ticking a box. This is crucial, given that consent will never be legally valid without such affirmative action. In practice, this means that wording such as 'You do not have to do anything further to consent' or 'If you do not respond, we will assume that you consent to…' does provide for legal consent. Pre-ticked checkboxes are likewise not permitted. The participant must 'actively' tick those boxes. For example: 'I have read and understood the information listed above and I agree to the use of my personal data for the purposes of scientific research.'

Consent can only be used as legally valid basis if the research projects meets the foregoing requirements. If one or more of these requirements have not been met, the data processing is therefore unlawful! In the following, we will be taking a closer look at the practical significance of the terms mentioned above.

NB! If your research is truly anonymous, the GDPR does not apply and it is not permitted to obtain declarations of consent from participants under their name. This is because such declarations serve only one purpose, demonstrating that the relevant participant has consented to the processing of their personal data. However, when your research is anonymous, you do not process any personal data! It is also unlawful to obtain any other declarations from participants under their name, such as a declaration in which they confirm that they have been adequately informed, as this violates the principle of data minimisation under the GDPR.

[5]Where the text refers to 'he', this can also be read as 'she' or 'they'.

When can consent be considered to be 'freely given'?

'Freely given' means that the participant actually has a choice and can exercise control over that choice. There should be no doubt that the consent was given voluntarily, and the participant may not suffer any negative consequences as a result of refusing or withdrawing his or her consent.

Hierarchical relationship (general)

If the free choice of the participant is in jeopardy in any way whatsoever (for example in cases where the participant may experience a certain degree of pressure to provide his or her consent or where there is a hierarchical relationship between the researcher and the participant, such as that of an employer/employee or teacher/student), then the consent is not legally valid. For that reason, students typically cannot give 'free' consent if the researcher is also their teacher or supervisor.

Pupils / students

If you are conducting a study among pupils or students (hereinafter collectively referred to as 'pupils') and if the research focuses on activities (such as assessments) that they would also be doing if a study was not being conducted (so-called didactic research), then consent need not be obtained (under the GDPR). In such cases, the study is taking place on the basis of public interest or legitimate interest. Nevertheless, from an ethical point of view, pupils (and/or their parents) must still be informed of the fact that research is being carried out on the basis of those activities. Individual pupils (and/or their parents) may then object to the processing of their data. In the case of this type of didactic research, as a researcher, you will have to balance the interests of the research against the privacy risks for the pupil in question. Your assessment of interests must be shared with the relevant pupil (and/or their parents). If the privacy risks for the pupil are such that they outweigh the importance of the research, then their personal data must be erased.

Arrange with the school to which address the objection forms should be sent. The teacher needs to be aware of this, as they usually need to prevent the work of pupils from reaching the researchers. If you first want to determine whether the objection can be 'granted' on the grounds of the participant's specific situation, then the form first needs to be sent to you in your capacity as the researcher, and you then need to provide the 'granted' objection form to the teacher.

In the case of non-didactic research, the consent of the pupil and/or their parents is always required by the GDPR. If the researcher is also the teacher or supervisor, non-didactic research cannot take place – even with the participant's consent. Completely anonymous research constitues an exception to this rule, but even then consent must be obtained for ethical reasons.

Arrange this in such a way that the forms are sent to you, because in your capacity as the researcher, it is your duty to retain these documents. The teacher needs to know which pupils' work they should pass on to the researcher and which pupils' work they should discard.

	teacher ≠ researcher	teacher = researcher
didactic research	public / legitimate interest: From an ethical point of view, pupils and their parents must be informed of the fact that research is being carried out on the basis of those activities. Individual pupils may object to the processing of their data.	public / legitimate interest: From an ethical point of view, pupils and their parents must be informed of the fact that research is being carried out on the basis of those activities. Individual pupils may object to the processing of their data.
non-didactic research	informed consent of parents and/or pupils (depending on age) required	only possible: - in relation to recruitment: for example, refer to a web environment where pupils are able to register or take part voluntarily; - in the case of actual anonymous research, please see **Anonymous data**.

Children and persons legally incapable of giving consent

It is possible to carry out research with children or persons legally incapable of giving consent (*wilsonbekwamen*) on the basis of the basis of consent, however other conditions will apply.

- **Children:** By law, the consent of a parent/guardian will be required in lieu of the consent of the data subject (the participant) if the participant is under 16 years of age. For children aged 12 to 15, the consent of both the child and the parent/guardian is required.
- **Persons legally incapable of giving consent**: This refers to participants who have been placed under guardianship, are wards of the court or for whom a mentorship has been established. People suffering from dementia, for example, may fall under this group. Insofar as it concerns matters for which the participant is incapable of giving informed consent or is incompetent, their legal representative must provide consent in the participant's stead.

When is consent 'specific'?

'Specific consent' means that the participant has consented solely to the relevant well-defined processing operations. In the event of multiple data processing operations for various purposes, the participant must provide consent seperately for each of these operations.

All types of consent that are strictly necessary for your research can be combined – additional types of consent must be specified separately.

Example: In your study, it is a *requirement* that participants complete questionnaires as well as take part in interviews. In addition, it would be *desirable* for participants to take part in observation and screening. The relevant section of your declaration in such a situation may, for example, look like this:

By signing this declaration, I consent to written questions being put to me. I also consent to being interviewed by a researcher.

- ☐ By ticking this box, I also consent to being observed. This means that researchers will be monitoring me.
- ☐ By ticking this box, I also consent to being screened by the researchers and I am aware of what that entails.

When is consent 'informed'?

Under the GDPR, 'informed' means that, prior to consenting, data subjects (i.e. participants) must be informed and aware of the purpose of the research for which their consent is requested. In addition, they must be informed of their individual rights as set out by the GDPR, inter alia in Articles 15 to 22.[6]

Informing participants is known as the obligation to inform. The GDPR does not set out how to comply with this obligation. It may, for instance, be in the form of a letter or brochure or in the form of a privacy statement on the website (to which the researcher must explicitly refer) or by way of an oral statement.

In any case, the fact that the required information has been made available to the participant by the researcher must be demonstrable:

- In the case of a written statement on paper (i) the researcher must sign the document to show that he adequately informed the participant and (ii) the participant must sign the document to confirm that he has read the information and has had the opportunity to ask questions.
- In an online environment, the participant may be asked to tick a box indicating that he has read the required information. It is vital that checking the box is mandatory in order to be able to continue.
- In the case of an oral statement, which must be recorded separately (audio recording), (i) the researcher will state that he has duly provided the information and (ii) the participant will declare that he has read the information letter or has been informed orally and that he has been given the opportunity to ask questions.

By law, the information must be communicated in clear and comprehensible language. Therefore, you should use language that is appropriate to the intended participants and/or their representatives in all communications. If a participant does not speak Dutch, then the information must be provided in a language that the participant has designated to be one in which he/she is sufficiently proficient.

What information are you required to provide participants?

- Describe the research project in plain language. The participants must be able to understand what they are consenting to.

[6]These rights are: The Right of access by the data subject (Article 15), the Right to rectification (Article 16), the Right to erasure (Article 17), the Right to restriction of processing (Article 18), the Right to data portability (Article 20), the Right to object (Article 21), the Right not to be subject to automated individual decision-making, including profiling (Article 22).

- Provide a description of the research team. Participants must have a clear picture of who you are (student, PhD candidate, PhD researcher) and, if this is the case, who else is involved in the processing of their data – for example, if other co-workers are given access to that personal data. These individuals do not have to be named, but you will have to indicate that 'researchers who are directly involved in the study' will similarly have access to the personal data. Set out who is responsible for the study. For example, if the study is being carried out by students or PhD candidates, the supervisor will be the person responsible. There may be more than one controller, however the participants should be able to easily contact one of the researchers responsible. An email address or other details to contact the controller must be provided.
- Outline the timeline of the study for the participants, how long the study will take for them (lead time, time per session, etc.) and what is expected of them. Set out what the burden will be for participants during the study and what risks may be associated with the study – including in the long term. For participants, their individual role within your study must be crystal clear.
- You must state that you will be collecting and processing data based on the consent of the participants – for example, you should specifically use the term 'consent' when asking the participants for their consent.
- Describe the specific types of data you will be collecting from participants and how you intend to use them. Try to find the right balance between completeness and brevity. Detailed enumerations will not encourage the reader to continue reading. Missing information, however, can lead to misconceptions. If you intend to create image or sound recordings (e.g. of online interviews), you must set out whether you intend to store, transcribe, destroy, etc. these recordings and who has access to the recordings. Often a recording will first be transcribed (whether or not pseudonymised), after which the recording is destroyed. Whatever the case: you must outline how the recordings of your study will be processed and retained.
- You must set out how long their data will be retained, and in what form (meaning as 'raw data' or anonymised/pseudonymised). Within the UU, a retention period of at least 10 years applies to scientific research data.[7] The retention period depends on various and sometimes conflicting requirements and guidelines established by publishers, financiers, the researcher's institute and by law. Examples of criteria include scientific considerations for reuse and replication of research, requirements laid down by publishers and financiers and legal requirements or scientific guidelines. You will have to assess the situation yourself. However that assessment turns out, it is vital that you formulate the information in such a way that a participant is able to identify what the retention period will be for specific data/purposes based on his or her own situation.

  It is insufficient to state in general terms that the personal data will be retained 'for as long as necessary for the purposes of the data processing activities'. Different retention periods will often have to be established for different categories of personal data and/or

[7] According to the Netherlands Code of Conduct for Scientific Practice, research data must be retained for (at least) 10 years. Indeed, the UU research data policy makes the following addition in this regard: 'starting after any publication'. If the raw research data has not be anonymised, the declarations of consent must likewise be archived during this period.

different processing purposes, including archiving. Video and audio recordings, for example, will often be erased after they have been transcribed. Due to the scientific verifiability of research data, retaining or archiving recordings is not prohibited, provided that they are adequately secured. This represents a clash between the interests of data minimisation and academic integrity, for which the Faculty of Humanities has as yet not formulated a clear policy.

- Outline what data you intend to share with others, with whom and in what way. You should state whether the data will be shared as raw data or in pseudonymised or anonymised form (please see above). Research data can remain very useful to other research projects. In order to be able to reuse that data outside of your own project, participants must be aware of this and must have given their explicit consent for that purpose. Please refer to: https://www.uu.nl/en/research/research-data-management/guides/informed-consent-for-data-sharing.
- If you are working with an external company or an external organisation (including if this relates to researchers from outside the Faculty of Humanities or outside the UU), you must clearly give notice that this is taking place, clearly stating who the data controller is.[8] In these types of cases, please always contact privacy.gw@uu.nl first before submitting an application to the FETC-GW.
- Where applicable, you must provide information regarding the use of the personal data for the purposes of automated decision-making,[9] and regarding the potential risks of transfer of the personal data to 'third countries'. These are countries outside the EEA (the EEA is the EU plus Norway, Iceland and Liechtenstein).[10] In the case of automated decision-making and transfer to third countries, it would be prudent for you, as a researcher, to contact the Privacy Department: privacy.gw@uu.nl

Please note! If you are not working on the basis of consent within your study, please always contact the Privacy Department: privacy.gw@uu.nl

Concluding paragraph

Every information letter will end with a standard section that informs the participants of their rights and provides them with the key contact details. Please consult the sample letters for the exact content of this section and read a description of the contents below:

- Inform participants of their rights and what steps they need to take to exercise those rights, who they can contact and how to file a complaint and ask questions. It must also be perfectly clear to participants that they can withdraw their consent (at any time and without stating reasons), but that the data processing that has taken place until the time of withdrawal will remain legally valid and does not have to be reversed. If the consent is subsequently withdrawn, and at that point you still have non-anonymised research data from the participant in question, then that data must be deleted. Only in exceptional

[8] A so-called data processing agreement must be concluded with any external data processor prior to the data processing activities starting.

[9] This only applies, for example, in the case of profiling taking place or if decisions are made by the computer that may have legal consequences for the participants. This rarely seems to be the case in relation to scientific research.

[10] Certain 'third countries' have been designated by the European Commission as countries that are secure for the exchange of information. Other conditions for data transfer apply to other countries.

cases may data be anonymised at that time. In such a case, always contact the privacy officer first, privacy.gw@uu.nl. Please also remember that withdrawing consent should be as easy as giving it.

- You must state that the Faculty Ethics Assessment Committee has approved the research proposal and that if a participant wishes to lodge a complaint about the ethical procedure that applies to the study, he or she may contact the Secretary of the Faculty Ethics Assessment Committee of the Faculty of Humanities (FETC-GW, fetc-gw@uu.nl).
- You should also state that participants may contact the Data Protection Officer with regard to any privacy issues or to exercise their individual rights under the GDPR. Provide the contact details for the Data Protection Officer of the UU: privacy@uu.nl.
- Inform the participants of their right to file a complaint with the Dutch Data Protection Authority: www.autoriteitpersoonsgegevens.nl.

What does a statement or clear affirmative action entail?

The GDPR clearly states that giving consent requires affirmative action but does not describe what is meant by this, although it may include one of the following options:

- **Oral declaration:** Consent may be given orally, but in that case, the data controller (i.e. the researcher responsible) must be able to demonstrate that the consent was given in a legally valid manner. This can, for example, be achieved by making a recording of the consent being given. Furthermore, as a researcher, you must be able to demonstrate that the participant has been sufficiently informed in advance. For example, at the start of the recording session, the participant could say: “My name is XY. I have received the information for this study. I have read the information and I understand it completely. I hereby give my consent to participate in this study." Next, the researcher could say: "My name is YZ, and I am the interviewer in the study entitled `123’. I have provided all required information to the person who just consented to participate in this study.” This informed-consent part of the recording session should be saved as a separate file, i.e. not in the file of the interview. After it has been transcribed, the interview, in many cases, can be deleted. However, the consent must be retained for as long as any non-anonymised research data of the participant is retained.
- **Written declaration:** According to the GDPR, obtaining explicit consent can take place by way of a written declaration – in various forms. Below are a few examples. If none of the methods below should apply to your study, or if you are in doubt, then please contact privacy.gw@uu.nl.
    - **Electronic consent via a web page:**
        - If the data will be processed anonymously, it is sufficient for you to be able to demonstrate that the answering process can only be completed if the participant has ticked the checkbox with which he indicates that he has read the information and consented to the processing of his personal data.
        - If the identity of the participant is not important and is not registered, but you likewise cannot exclude that the participant could be identified based on a combination of responses, then similarly in this case it would be

sufficient for you to be able to demonstrate that the answering process can only be completed if the participant has ticked the checkbox with which he indicates that he has read the information and consented to the processing of his personal data. The risk that someone could be identified based on a combination of responses must, however, be stated in your information letter/screen.

- If the identity of the participant is, however, relevant, for example for the purposes of sending them a gift voucher or to make a follow-up, then the data will not be processed anonymously. In that case, the participant must provide his or her personal email address and respond to a(n) (automatically generated) confirmation email stating for what purpose consent is given. Returning this email will be considered to be giving consent. This email procedure is crucial as otherwise it is impossible to establish the identity of the participant with any certainty. The confirmation email must be retained.

  Please note! The confirmation email must come from the participant's personal email address. An email address such as info@mybigcompany.nl is not good enough – for obvious reasons.[11]

- **Consent by email:**

  If you are distributing a questionnaire or a similar research tool via email, then you must provide the information about your research (the information letter) immediately alongside the email or incorporate it in the email itself. If a participant is returning the questionnaire (or similar tool) by email from a personal email address, then that email must be retained as proof.[11] In the return email, you must have the participant indicate that he/she consents to the processing of his/her personal data as set out in the information letter.

- **Consent on paper:**

  If participants are asked to sign a declaration of consent 'on paper', that declaration will not be legally valid without a signature. You will therefore have to ask the participant for his/her signature – even if that participant only wishes to take part under a pseudonym. The demonstrability of the consent in this case takes precedence over the principle of data minimisation, which states that you may not collect data that you do not need. It is good practice to scan and save any paper declarations (separate from your research data) and subsequently to destroy the paper versions.

Opt-in vs. opt-out: As stated previously, when requesting consent it is strictly prohibited to use pre-ticked boxes ('opt-out'). Instead, a participant must actively give their consent, by means of opting in, meaning that he or she must take a specific action. 'Clear' or 'unambiguous' means that there should be no doubt about whether the participant has given their consent. In the simplest case, this means that he or she will tick a box that says 'I hereby consent to …'.

[11]The fact that the email comes from the personal email address of the participant legally replaces his/her signature. This means that following receipt of a consent email from the personal email address of the participant, a separate consent form no longer needs to be completed and signed.

The use of sentences and phrases such as 'if you do not respond, we will assume that you consent to…' are likewise out of the question!

How long is proof of consent retained?

You will be required to be able to demonstrate that consent has been given for as long as the data processing activity continues. At the end of the data processing activity, proof of consent may not be retained any longer than is strictly necessary to comply with statutory obligations (or to serve as evidence in any judicial proceedings). In most cases, the various types of proof of consent in relation to research projects would have to be deleted after completion of the project (particularly if they contain personal data such as names and signatures). However, they would still have to be retained for as long as any (non-anonymised) data was retained.[7]

For any long-term projects, the European data protection authority[12] recommends renewing the consent at appropriate intervals as a best practice. Reissuing all the information will help to ensure that the participant remains properly informed about how their data is being used and how they can exercise their rights. A good rule of thumb is to renew declarations of consent every two years. Please note that this does not apply to the archiving period, but to the duration of the study.

Additional information

The foregoing guidelines were drawn up in part based on the official documentation listed below. If in doubt, please feel free to consult these guidelines to accurately assess whether the consent for your research project is lawful and appropriate.

Guidelines 05/2020 on consent under Regulation 2016/679,Version 1.1 Adopted on 4 May 2020.

Guidelines on transparency under Regulation 2016/679. Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018.

[12]This is the European Data Protection Board (EDPB).