Consent manual for D3i researchers

Digital Data Donation studies

Inhoudsopgave

This document contains a **consent manual** which explains **how valid consent** as laid down in the **General Data Protection Regulation (GDPR)** can be obtained from **research participants in the context of data donation studies**. To obtain valid consent, a researcher must offer participants a **privacy policy** in which the researcher offers details about the envisaged research, and a **consent form** which the participant signs or ticks before the processing of their data starts.

Obtaining valid **participant consent** is a crucial part of **legal** and **ethical** compliance researchers must consider **prior** to processing a **participant's personal data.**

Liability & warranty notice of the manual and templates

This D3i consent **manual** contains **general recommendations** for D3i researchers that are subject to the legal evaluation of each university. Both the **privacy policy template** and the **consent form template** serve as **exemplar models** from which researchers can draw inspiration and that they can use for their own participant consent procedures. Researchers should however bear in mind that for participant consent to be compliant with the Faculty/University policy**,** they must **always** get approval from the **ethical research board** (ERB) and/or Data protection officer (DPO) of their **own Faculty/University**. The D3i-project **cannot** take any w**arranty/liability** for a researcher's use of the templates; these remain with the **researcher themselves**.

1. Introduction

We explain what a privacy policy and consent form should comprise, what their aim is, what conditions for GDPR-compliance are, why they are important; in other words, how researchers can provide participants with an appropriate privacy policy and consent form. At the end of this manual, researchers will find **model templates** for a privacy policy and a consent form.

1.1 Privacy policy

A **privacy policy** outlines generic **information** and **conditions** as well as the ways a researcher collects, uses, or shares participant personal data. A privacy policy is a legal **document**: it serves as **evidence** that the participant is properly informed about the processing of their personal data. It tells participants in clear and plain language how researchers collect and handle their personal data, whom they share it with, and any other relevant details. A scientific researcher's privacy policy outlines for instance:

- the identity and contact details of the researcher, and the University the researcher is affiliated with;
- the purpose(s) of the scientific research;
- how participant data is collected; or
- whether other parties will get access to the participant's data

The list with minimum requirements is presented in §3.5.6.

Why do researchers need a **privacy policy**? The GDPR gives **participants** the right to be **informed** about the **collection** and **use** of their personal data. Personal data often reveals intimate details of a person's private life and of that of their friends and relatives with whom they communicate. It is therefore of utmost importance that a **privacy policy informs participants** in an easily **accessible** manner, whereby that information is written in **clear** and **plain language**. A privacy policy stipulates how the researcher

intends to process the data of all participants. The privacy policy is of a **generic** nature and applies to all participants.

However, to obtain valid participant agreement, a **privacy policy** is **not enough** under the GDPR: researchers need to obtain an **active agreement**, in GDPR-terms, **consent** from the participant. In GDPR-speak, a participant must declare their **specific** and **unambiguous consent** before collection of their personal information can start. To obtain valid consent, a consent **form** informing and addressing the **participant's needs** and **concerns** must be offered. The consent form directly relates to the privacy policy: information found in the **consent form** must **align** with the information in the **privacy policy**. A privacy policy is usually richer in information, and may take more text compared to the consent form.

1.2 Consent form

To obtain **valid** consent from **an individual participant**, a scientific researcher must prepare a **consent form** a **participant** should **sign**[1] to **express** that he or she **agrees** with the processing of their personal data. This should happen **before any start** of that processing by the researcher. To ensure that the researcher will obtain valid consent from the participant, all relevant information must be brought to the attention of the participant, in a **concise**, **transparent**, and **easily accessible form**, using **clear** and **plain language**, so that the participant can give their **genuine agreement** for the processing of their personal data. A consent form is also a **legal document**: it serves as evidence that the participant agreed with the processing of their personal data.

1.3 Manual structure

The privacy policy and the consent form are central in this **manual.** The manual presents to the following:

- a **background** to and **explanation** of what a researcher must **do** to obtain **valid consent**;
- a **template** for an exemplary **privacy policy** (see Annex 1);
- a **template** for an exemplary **consent form** (see Annex 2).
- annex 3 contains GDPR Articles and Recitals that are relevant to obtaining a participant's consent.

Researchers can make these templates **specific** for the **study** they wish to conduct and for which he or she needs to obtain a participant's consent. These templates can be provided in **electronic form** – see [mention website].

1.4 Version control

This **consent manual** and the **templates** will be **used** and **tested** throughout the **three pilots** in the D3I-project. The consent manual and templates' **design**, its **effectiveness** and **GDPR compliance** will be **analysed** and where necessary be **adjusted** to the **needs** of **researchers**.

These analyses will be based on the **experiences** collected during each of the **pilots**, after discussions with the **University Data protection officers (DPOs), data stewards** and **ERBs** of the FSW departments. The documentation must also **align** with the **technical architecture** and **operational aspects**, and **vice versa**.

[1] Singing a document is very common, but agreement can also be given in other ways, this will be elaborated next.

- In the **first pilot**, we stay close to the current consent documentation, as used by the **University of Amsterdam**.
- After **gaining experience** from the **pilots**, we may have to **adjust** the consent **documentation** where that is **necessary** to adequately **safeguard** the **rights** and **interests** of the data subjects (**participants**) and/or to **clarify** the documentation for the **researchers** (data controllers).

2. Consent

In this section, we first introduce often used **GDPR terminology** researchers may engage with whenever they develop their privacy policy and consent documentation. We describe how the terminology relates to obtaining consent for scientific research, including that D3i-related (§1.1). We then continue with unpacking the **concept** of consent: what it means and **why** it is important to obtain it in the right way from research participants (§1.2).

2.1 Key terminology

Before explaining what consent means and how it can be obtained, we first address a few important terms of the GDPR and how they apply to the researchers and the participants, and to other actors that may get involved in a research project.

- **Data controller**: The **university** is regarded under the GDPR as the "**data controller**".[2] The university enables the researchers it employs to perform scientific research. While in **practice**, the researcher determines the purpose(s) of the data processing for a specific research purpose, the university ultimately acts as data controller. Being **employed** by the university, the researcher acts under the **responsibility** of the university. The controller is the **main responsible actor** under the GDPR.
- **Data subject:** This is the individual whose personal data will be processed for research purposes. The **participant** is regarded as the **data subject** under the **GDPR**.
- **Joint data controllers:** Whenever **researchers from other universities** are involved in the research for which personal data will be collected from participants, the researchers from these other universities are considered **joint data controllers**.
- **Data Processor:** Sometimes researchers **hire** a **person** or **organisation** that helps them to process the data for the researcher's research purposes. If that person or organisation **acts on behalf of** (i.e., receives instructions from) the **researcher**, that **person** or **organisation** probably acts as a **data processor**.
- **Personal data**: personal data means **any information** relating to an **identified** or **identifiable person** (this person is the research participant).
- **Special category data:** the processing of personal data **revealing** a participant's racial or ethnic origin, political opinion, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation is in principle prohibited – unless the participant gives their **explicit consent**.[3] See further on how researcher consent requests for special category data work §2.3.
- **Data Protection Officer:** a university has to employ at least one data protection officer ('DPO').[4] Where issues relating to the protection of data protection in any university activity occur,

[2] Art. 4(7) GDPR).

[3] Art. 9(1); see for explicit consent Art. 9(2)(a) GDPR.

[4] Art. 37(1) GDPR.

including those by scientific researchers, a DPO needs to be timely involved.[5] DPOs are tasked with advisory functions, and most importantly, they monitor a university's (and hence a researcher's) GDPR compliance, and they are a University's contact point for the supervisory authority.[6]

- **Supervisory authority:** means an independent body tasked with, amongst other, monitoring and enforcing the GDPR and that investigative powers to issue warnings or to impose administrative fines where controllers do not comply with the GDPR.

As of now, we term the **key actors** in D3i research contexts **researcher** as data controller, whereby the researcher acts under the ultimate responsibility of the University as data controller[7], and as **participant** (= data subject). Whenever joint data controllers and data processors are introduced, they will be termed accordingly (as joint controller or as data processor).

Most responsibilities concerning a GDPR-compliant and secure collection, use and/or sharing of a participant's personal data fall on the **researcher**, while the **participant** mainly has **rights** related to their personal data (they have for instance a right to access data that is held by a researcher, and if that right is exercised, the researcher must give the participant access to their data).[8] The GDPR terminology is further elaborated in the **background document** about the GDPR and **scientific research**.

2.2 Concept of consent

The **concept** of consent is traditionally linked to putting **individuals** whose personal data is processed, in **real control** over that **processing**, and to build their **trust** and **engagement** in that processing.

Control being exercised through someone's **consent** is a **crucial concept** in data protection law: control over one's personal data relates to someone's rights to **personal autonomy**, **self-determination** and right **privacy.** Whenever a researcher processes a participant's personal data, that processing can have impactful **consequences** for the **participant**: the researcher may get to know very detailed information about a participant's often **intimate, personal life**. The researcher may know, for instance, based on the participant's data, what movies they prefer, what physical or mental diseases a participant carries, how they behave on websites, or what their sexual preferences are – often information that individuals are usually very careful with to share it with their outer world. In some cases, participants may not even be aware of having a certain condition (e.g., not being aware of having a disease).

In other words, sharing personal data with a researcher can create many **vulnerabilities** for participants, for instance, whenever participant data is **shared** with others, whenever their personal

[5] Art. 38(1) GDPR.

[6] Art. 39 GDPR.

[7] Where the researcher is mentioned, they are mentioned in their role of data controller; we thereby bear in mind that the ultimate data controller is the university employing the researcher.

[8] Art. 15 GDPR. Participant data rights and the researcher's obligations relating to participant's exercises of data rights are further elaborated in the background document about the GDPR and scientific research.

data occur in **public documents** (such as research reports), whenever that data is **illegally accessed** by others, ow whenever participant data reveals information about the participant that the participant was not aware of. These risks and vulnerabilities must be addressed in appropriate ways, but it also means that a researcher seeking to obtain a participant's **decision** to **accept** that researcher's data processing **operation,** is subject to **strict conditions** as prescribed by the **GDPR** for obtaining their consent**.**

To make a participant's consent **genuine**, the GDPR stipulates that their "consent" should give a **freely given**, **specific**, **informed** and **unambiguous** indication of the participant's **agreement** to the processing of his or her personal data. This agreement can be expressed by a **statement** or by a **clear affirmative action**.[9] These terms and their conditions will be further elaborated in §2.

When **requesting** participants for **consent**, a **researcher** has the **duty** to assess whether their own consent request meets **all** the **GDPR requirements** to obtain a participant's **valid consent**. If a researcher's consent request is valid, consent is a **tool** that gives **participants control** over **whether or not** their personal data can be processed.

To obtain a participant's consent for scientific research studies, researchers usually ask that participant to sign a consent form. This legal documentation for D3i-researchers also encompasses a consent form that can be made specific for a researcher's research purpose.

Compliance with the GDPR is **important**, because the GDPR has tasked the **Supervisory Authority** – in the Netherlands: **Autoriteit Persoonsgegevens** (AP) – with powers to submit (high) **fines.** Such fine can also be imposed whenever a researcher obtains a participant's consent in an **invalid** way.[10]

In order to prevent this from happening to researchers, we **explain** how the GDPR applies to obtaining consent and how its conditions can be met. The **consent form template** and **the privacy policy template** aim to provide researchers **exemplar models** they can **make specific** for the purposes of their own research for obtaining participant consent for their own research purposes.

3. Consent in the GDPR

The GDPR defines consent as:

- any **freely given**,
- **specific**,
- **informed**, and
- **unambiguous indication**

of the **participant's wishes** by which he or she, by a **statement** or by another **clear affirmative action**, signifies **agreement** to the researcher's **processing** of their personal data.

A researcher's consent request to a participant must fulfil these four conditions for a participant's consent to be **valid**. How these conditions apply will be elaborated in this section.

[9] Art. 4(11) GDPR.

[10] The penalties for infringements to the GDPR can run up to €20 Million (Art. 83(5)(1)(a) GDPR).

3.1 "Freely given"

The element "freely given" implies a **real** and **meaningful choice** and **control** for participants over their personal data. As a rule of thumb, the following may help to understand the concept of "freely given" consent:

- Whenever a participant has **no** real choice, or feels **compelled** to consent, or will endure **negative consequences** if they do not consent, their consent will not be considered freely given, and thus be **invalid**.
- If consent is **bundled up** as a **non-negotiable part** of terms and conditions, it is presumed not to have been **freely given**.
- Consent will **not** be free if the data subject is **unable** to **refuse** or **withdraw consent,** without **detriment**.
- Potential **imbalance** between the **researcher** and the **participant** must also be considered (such imbalance is often present in relationships between employer-employee, or public organisation and citizen).

In general terms, any element of **inappropriate pressure** or **influence** upon the participant (which can be manifested in many different ways) **preventing** a participant from exercising their **free will**, will render the consent **invalid**. An **example** in the context of the use of a commercial app might explain how freely given consent practically works:

> "A mobile app for photo editing asks users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geo-localisation nor online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given".[11]

Some researchers consider offering participants **incentives** for their participation. As incentives can potentially influence a participant's choice, for instance where the incentive entails a financial gift, it is important that the **researcher** is able to **demonstrate** that a participant can **refuse** or **withdraw consent without any detriment**.[12] For example, the researcher must be able to prove that withdrawing consent does not lead to any costs for the data subject or to other disadvantages for those withdrawing consent (in terms of that the cost of the incentive has to be reimbursed). The researcher must moreover **explicitly** inform the participant that they have a right to withdraw their consent (see further §2.5.6).

3.2 "Specific"

For consent to be **specific**, the participant must at least be notified about the researcher's intentions with the data processing, by stipulating in the researcher's privacy policy and in their consent form:

- **what kind** of personal data from a participant will be processed,
- **how** that data will be used,

[11] Example borrowed from EDPB's Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020.

[12] Recital 42 GDPR.

- and for what **specific research purpose** the data processing operations are envisaged.

As a rule, scientific research can only include personal data where that processing is based on a participant's consent, if that consent is based on a **specific purpose**. In **scientific research** contexts however, specification of the research purpose can sometimes be challenging. For situations where purposes for data processing within a scientific research project **cannot** be specified at **the outset**, the GDPR **allows** for some **flexibility,** meaning that the purpose **may be described** at a **more general level**:

> "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."[13]

The more flexible regime for scientific research can however not be applied in such a way that the **essence** of a participant's **right** to data protection is **emptied out**, meaning that this flexibility regime does **not dismiss** a researcher's obligation to do his or her utmost to specify their intention of the processing of a participant's data altogether. Whenever a researcher cannot specify the research purpose, they

3.3 "Informed"

The GDPR requires that consent to be **informed**. The requirement relates to the data processing principle of **transparency,** which is one of GDPR's **key principles**. Researchers must provide participants with appropriate **information** to enable them to make **informed decisions**, so they **understand** what they are agreeing to; that is, researchers must inform a participant in a concise, transparent, intelligible and easily accessible form, thereby using clear and plain language.[14]

The GDPR includes a list of aspects that researchers must inform participants about.[15]
For consent to be **informed**, the participant must at least be notified about the **researcher's identity.** The participant must also be informed about their right to **withdraw** consent **anytime**.[16] Consent withdrawal must be **as easy as giving** consent (see on consent withdrawal §2.5).[17] Where relevant, the researcher also has to inform the participant about the use of the data for **automated decision-making** and/or **profiling.** Participants should also, whenever their personal data is shared with researchers outside the EU, about possible risks that may come with **data transfers** (due to absence of appropriate safeguards protecting their data). As explained under "specific" in 2.2, participants must be informed about the **purpose** of each processing operation the researcher wishes to undertake, and about the **type of data** that will be collected and used.

[13] Recital 33, GDPR.

[14] Art. 12(1) GDPR.

[15] Article 13 GDPR.

[16] Art. 7(3) GDPR.

[17] Art. 7(3) GDPR.

If a participant's consent should enable the researcher's processing of **special categories** of personal data, the **information provided** to the **participant** must **expressly** refer to the **specific special category** (or categories) of data the researcher seeks to obtain. Researchers wishing to process this type of participant data must request a participant's **explicit consent**.[18] Special category data urge a researcher's **scrutiny**: as the processing of this type of data may entail **vulnerabilities** for the participant**,** researchers must in their privacy policy explain and give reasons, in clear and plain language that is comprehensible for the targeted participant, why they seek to process a participant's special category data.

3.4 "Unambiguous indication of wishes"

Valid consent requires a participant's **active statement**, or a clear **affirmative act**, meaning that consent must be given through an **active motion** or **declaration**: the data subject must have taken a **deliberate action** to consent to the processing.[19] Consent can be collected through a **written** or (a recorded) **oral** statement, including by **electronic means**. **Written statements** can come in **many shapes** and **sizes** that could be **compliant** with the **GDPR**.

Valid consent can for instance not occur in the form of **pre-ticked boxes**; it must be 'an active behaviour with a clear view on the part of the data subject with a view to giving his or her consent.[20] A website with a tick-box which needs to be **actively ticked** by the participant in order to give their consent is allowed.

3.5 Considerations for scientific researchers obtaining consent

In this subsection, we elaborate some practical considerations related to the GDPR as they may often arise in scientific research context.

3.5.1 Type of documentation to inform participants

The GDPR requires researchers to choose a proper manner to inform participants, whereby that information must be offered in a **concise**, **transparent**, **intelligible** and **easily accessible form**, using **clear** and **plain** language. The information must be offered in **writing**, whereby that information can also be offered by **electronic means.**[21] Researchers can offer such information in several ways, as long as they meet all requirements just mentioned:

a. By providing them a link to and/or reference to the University's privacy statement, the researcher should critically check whether that information meets the requirements to obtain freely given, specific and informed consent.
b. By way of a privacy policy that was adjusted to the participant's level of comprehension.

---

[18] Article 9(2)(a) GDPR.

[19] Recital 32 sets out additional guidance on this.

[20] C-673/17 Planet49, judgment of 1 October 2019, para 65: "The [GDPR] must be interpreted as meaning that the consent […] is not validly constituted if, […] the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent."

[21] Art. 12(1) GDPR.

- Information in that privacy policy should be adjusted to a **participant's level** of **comprehension**, meaning that the researcher should use clear and plain language.[22] For instance, if the participant is a child or an elderly person, another language may be used compared to where the participant is a student.
- The privacy policy can be one document informing the participant about the researcher's intention with the personal data they collect, but the privacy policy can also be offered in a **layered** manner.
    i. First, the **consent form** can include a **link** to the privacy policy so as to enable a participant **easy access** to the privacy policy.
    ii. Second, to enhance the readability of a more extensive and/or complex privacy policy, the researcher may consider offering participants the **privacy policy itself** in a layered manner. That is, the most important information is given in the first layer, while more detailed information can be found in a second (or even third) layer. By adding links in the first layer to the other layer(s), participants can be easily directed to the information in the other layer(s). This can help improve a researcher's obligation of an **intelligible** and **easily accessible form** of communicating the researcher's intention with the personal data.[23]

3.5.2 Type of information researchers must provide participants

Information that **must** be provided to participants is precisely listed in the GDPR.[24] This information is usually offered in a researcher's privacy policy:

- the **identity** and the **contact details** of the **university** and, where applicable, of the controller's **representative** (this can be a person or department within the university);[25]
- the contact details of the **Data Protection Officer** of the University where the researcher has an appointment;[26]
- the **purposes** of the processing, as well as the **legal basis** for the processing (in D3i-research context, this will be "consent");[27]
- the (categories) of **recipients** of the **personal data**, if the researcher will **share** the personal data with others;[28]
- If that applies, the fact that the researcher intends to **transfer** personal data to a third country or international organisation **outside the EU**;[29]
- The **storage period** for which the personal data will be stored;[30]
- the existence of the **participant's right** to request from the researcher (i) **access** to and **rectification** or **erasure** of personal data, or (ii) **restriction** of processing data concerning the

[22] Art. 12(1) GDPR.
[23] Art. 12(1) GDPR.
[24] Arts. 13(1) and 22 GDPR.
[25] Art. 13(1)(a) GDPR.
[26] Art. 13(1)(b) GDPR.
[27] Art. 13(1)(c) GDPR.
[28] Art. 13(1)(e) GDPR.
[29] Art. 13(1)(f) GDPR.
[30] Art. 13(2)(a) GDPR.

participant, or (iii) to **object** to the data processing, as well as (iv) the participant's right to data **portability**;[31]

- the existence of the right to **withdraw consent** at **any time**, without affecting the lawfulness of processing based on consent **before** its withdrawal;[32]
- the right to lodge a **complaint** with a supervisory authority;[33]
- the **existence** of **automated decision-making**, including **profiling**. Where these indeed apply, the researcher must provide participants meaningful information about the logic involved, as well as about the significance and the envisaged consequences of such processing for the participant.[34]

3.5.3 "Further processing" of personal data

As a general rule, data controllers wishing to use data subject data for **other purposes** must **ascertain** whether that processing and use of data is **compatible with the purpose for which the data subject gave their initial consent**.[35]

In a **scientific research context**, things look a bit different. Some controllers may consider using the personal data obtained from participants. **Further** processing of personal data obtained from participants for **purposes other** than the purpose for which the participant gave their **consent** for **scientific research purposes** should in principle be considered to be **compatible** with the GDPR.[36] In other words, a researcher is allowed to use participant data for a purpose other than the purpose for which the participant gave their consent, but the **researcher** must take appropriate **technical** and **organisational measures** to properly **assure** the participant's **data protection rights**, and particularly ensure data **minimisation**.[37]

GDPR's principle of **data minimisation** prescribes that the collection of personal data must be relevant and limited to what is **necessary** in relation to the **purpose** for which they will be processed. **Technical measures** helping to assure that participants are no longer identified may help a researcher to meet this principle; a researcher could for instance apply **pseudonymisation** or **anonymisation** techniques so that the personal data is no longer exposed than necessary.

Regarding anonymisation: processing data may not be enough to anonymise the data. Anonymisation applies as soon as the data can no longer be traced to an identifiable individual (even if combined with other datasets). Where anonymisation applies, the GDPR no longer applies. If data can be traced back to an identifiable individual, (or the risk of re-identification cannot be excluded), another solution will have to be found (researchers might for instance learn from experiences in medical research).

[31] Art. 13(2)(b) GDPR.

[32] Art. 13(2)(c) GDPR.

[33] Art. 13(2)(d) GDPR.

[34] Art. 13(2)(f) GDPR.

[35] Arts. 6(4) and 13(3) GDPR.

[36] Art. 5(1)(b) GDPR; Recital 50 GDPR.

[37] Art. 5(1)(c) GDPR.

A tech-savvy researcher might also consider using other **Privacy Enhancing Technologies** ('PETs'),[38] such as differential privacy, homomorphic encryption or secure multi-party computation. A university or faculty **data steward**, a person usually tasked with assisting researchers on their data management might also help researchers with using such techniques to enable a secure use of sensitive data for scientific research interest.

3.5.4 Researcher's access to participant data: variables and risks with data types

Participant data can be made available to researchers in several different ways, but not every way may be GDPR compliant. GDPR's principle of data **minimisation** requires scientific researchers to consider capturing participants' personal data being **adequate**, **relevant** and **limited to what is necessary** in relation to the research purpose.[39] Researchers must therefore consider what data they need, highlighting another time the **importance** of the **specification** of the research **purpose**, and how they envisage to accomplish that purpose by using participant data.

Some **manners** of a researcher's **accessing** participant data imply **higher risks** for the participants, while deploying other ways of access may entail **lower** risks. Mirroring the participant's risks, some data access types might entail higher risks to the researcher's research results. A **key variable** in risks associated with data access is the **level of detail** and **granularity** of data, which define the possibilities of researchers to use it and derive meaningful information from it. Data can be accessed at different level of detail:

- raw (as it is collected from the source);
- pre-processed (e.g., cleaned, re-sampled, normalised);
- processed (aggregated and combined); or
- presented as insights resulting from internal analysis.

For **participants**, giving researchers access to **raw** data often entails **higher** risks for the participant, given that raw data often reveals, compared to the other types, a participant's personal, intimate information at the most detailed level.

Notably, some researchers may consider offering participants an opportunity to **(de)select data** participants may want to share. This does not necessarily decrease the risk of a researcher accessing the participant's personal, intimate life, but such participant-regulated data access would help increase a participant's control over what a researcher can do with their data. This approach however **presupposes** a **participant's comprehension** of what data should be de-selected for sharing with the researcher.

Researchers considering giving participants this choice should appropriately **inform** participants about meaningful (de)selections of personal data in for instance their privacy policy if this method is meant to **meaningfully** increase **participant control** over what data the researcher will access. Note, however, that such participant control can**not replace participant consent**: consent must be

[38] Several types of PETs are presented in The Royal Society report 'From privacy to partnership. The role of privacy enhancing technologies in data governance and collaborative analysis' (London, 2023). <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf?la=en-GB&hash=4769FEB5C984089FAB52FE7E22F379D6> accessed 1 June 2023.

[39] Art. 5(1)(c) GDPR.

obtained prior to the beginning of any data processing by the researcher. Giving participants an opportunity to (de)select data files to be shared can only occur **after** a researcher's processing of some participant data.

Researchers might however be most interested in obtaining a participant's **raw** data, opposed to acquiring data that underwent (pre-)processing or where insights resulting from processing are presented, as raw data likely entails less interference by others, and hence less risks for others being able to influence the research results.

3.5.5 Pseudonymised & anonymised data

Another manner to consider data types to be shared, is by deliberating the use of **anonymised** data or of **pseudonymised** data. The GDPR applies to personal data only, meaning that in situations in which a participant can no longer be directly or indirectly identified by using a specific data file, or where combining that specific file with other data or data files does not unveil a participant's identity, the GDPR does not apply. To achieve this, a data file must be **anonymised**, but anonymisation often comes with considerable challenges.[40] Whenever de-anonymization cannot be fully excluded, the researcher should consider other techniques to appropriately protect a participant's data. instead of anonymisation, pseudonymisation might offer useful ways forward. For instance, **encryption** is a powerful tool for **pseudonymisation**.

Pseudonymisation means the processing of personal data in such a way that that data can no longer be attributed to a specific participant **without the use of additional information**.[41] That additional information must be kept separately and be secured by technical and organisational measures. Note that **pseudonymised** data is **still personal data**.

The EU data protection regulator and the Spanish Supervisory Authority identified 10 misunderstandings about pseudonymisation that may help you decide to categorise the data you seek to work with and to take the right decision where it comes to taking appropriate measures to safeguard participant data, which are copy-pasted below:[42]

1. "Pseudonymisation and anonymisation are the same". False, as pseudonymisation allows for identification of individuals, anonymisation does not (if done correctly).
2. "Encryption is anonymisation". False, as encryption is a technical means to prevent access to data, but does not render it unidentifiable.
3. "Anonymisation of data is always possible". False, as datasets may become useless under specific circumstances if the data is anonymised.
4. "Anonymisation is forever". False, as new technologies or additional data may allow for re-identification in the future.

[40] 10 Misunderstandings related to anonymisation, European Data Protection Supervisory Board and Spanish Supervisory authority (2021), retrieved from https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf.

[41] Art. 4(5) GDPR.

[42] 10 Misunderstandings related to anonymisation, European Data Protection Supervisory Board and Spanish Supervisory authority (2021), retrieved from https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf.

5. “Anonymisation always reduces the probability of re-identification of a dataset to zero". False, although this is the desired outcome of anonymisation measures, this cannot be guaranteed in all cases.
6. "Anonymisation is a binary concept that cannot be measured". False, as it is possible to measure and analyse the degree of anonymisation.
7. "Anonymisation can be fully automated". False, as human expert intervention is required together with automated technological tools.
8. "Anonymisation makes the data useless". False - if done properly, the datasets can still be used for the intended purpose.
9. "Following an anonymisation process that others used successfully will lead our organisation to equivalent results". False, as the process needs to be tailored for the specific purpose, data, risks etc.
10. "There is no risk and no interest in finding out to whom this data refers to". False, as (personal) data is of great value and re-identification may be of risk for individuals' rights and freedoms.

3.5.6 Consent withdrawal

Participants have the right to withdraw their consent they initially gave to the researcher for processing their personal data.[43] Consent withdrawal comes with considerations and obligations researchers should be aware of:

- The researcher **must inform** the participant about their **right** to withdraw consent.[44]
- Consent can be withdrawn at **any time**.[45] That is, the researcher **cannot** limit the **term** for consent withdrawal.
- Consent **withdrawal** must be **as easy as giving** consent.[46]
- Consent withdrawal does **not** apply to **anonymised** data, as the GDPR only applies to personal data. As pointed out earlier, anonymisation of personal data however can be **challenging** (see §2.5.4).
- A participant’s consent withdrawal does **not affect** the **validity** of a researcher’s processing of that participant’s data **before** their withdrawal.[47] As a rule, this means that any processing of a participant’s data **after** the withdrawal can **no longer** be based on the participant’s **consent**, and that any such processing is **not valid**.
- However, for scientific research, the GDPR has created an **exception** that is subject to **conditions**.[48] Where the data processing is **necessary** for **scientific research purposes,** and in and so far as the right to withdraw consent is likely to render impossible or seriously impair the purpose of that processing, the researcher does not have to erase the participant’s data from a study. The consequences coming with a participant’s withdrawal of consent do, in such a situation, not apply.
- This exception comes with **conditions**: researchers must, in the situation where consent withdrawal occurs, be able to **demonstrate** that the processing is **necessary** for a **scientific research** purpose (which should not be a high bar for scientific researchers), and that **erasing**

[43] Art. 7(3) GDPR.

[44] Art. 7(3) GDPR.

[45] Art. 7(3) GDPR.

[46] Art. 7(3) GDPR.

[47] Art. 7(3) GDPR.

[48] Art. 17(1)(b) GDPR.

the participant's data **likely** renders achieving the research purpose **impossible**, or that such erasure can **seriously impairs** the research purpose. In other words, the researcher must **motivate** why they process data of a participant that exercised their right to consent withdrawal.

3.5.7 Practical questions to consider when drafting a privacy policy and consent form

Prior to a researcher's filling the privacy policy template and the template for the consent form, answering the following **questions** may be helpful:

1. What information is needed to inform participants about your intent to process their personal data for your **specified research purpose**?
2. Where do you intend to **store** the **consent forms**?
3. **How** and where can the participant **withdraw consent** at a **later date**?
4. Does the **processing** provide **opportunities** for data subjects (participants) to **request/view/edit/delete** their personal data **themselves** (think of **self-service functionalities** or procedures)? How are these functionalities made **comprehensible** and **manageable** for **participants** to convey them some **actual control** over aspects of the processing of their personal data?
5. Are the personal data also used for **other processes** or scientific research **purposes** than those for which participants initially gave their consent? Or do you **expect** that this **could happen**?
6. Do you as a scientific researcher consider using participant data **for follow-up research**? If that applies, the researcher must inform the participant.

For the privacy policy, researchers must check whether they provided the information described in §3.5.2 (to comply with Art. 13 GDPR).

4. Further reading

- Article 29 Data Protection Working Party (WP29) Opinion 15/211 on the definition of consent of 13 July 2011 (WP 187).
  < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf>

- European Data Protection Board (EDPB) Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted 4 May 2020
  <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>

- European Data Protection Supervisor (EDPS) A preliminary opinion on data protection and scientific research. Adopted 6 January 2020, p. 18 – 20.
  < https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf>

Annex 1 Template privacy policy

Privacy policy for participants

[Title research project]

Dear participant,

You are going to participate in the research project [research project title] conducted [optional: by name researcher] at the Faculty of [XXX] of the University of [XXX] [optional: in collaboration with XXX].

Before the research project can start, it is important that you take note of the procedures we will apply. Please read this brochure carefully. If anything is unclear to you, feel free to ask [option 1: the University representative at [e-mail DPO or ERB]] [option 2: the researcher, through e-mail [e-mail address]] [option 3: [organization XXX] at [e-mail XXX] and [telephone number]. Note: in a few words make crystal clear in the privacy policy what the role of this organization is].

The researcher [option: the researcher's representative [XXX] at [e-mail] and [telephone number]] will be happy to answer any questions you may have.

Purpose of the research project

[Description of the purpose of the research project, this should be understandable to non-experts, so avoid jargon.
**Example purpose*: The goal of the study is to form a clearer idea of the confrontations that smokers who live in Amsterdam encounter in social interactions (with family, friends, acquaintances and in public spaces) and how they deal with them*].

[If it is necessary to slightly 'mislead' participants to prevent the information from influencing the outcome of the *study*, the following text can be used]. At this stage of the project, we cannot give further information about the factors we will investigate. You will receive more details after the research is completed.

[If it is necessary to slightly 'mislead' the participants to prevent the information from influencing the *methodology*, the following text can be used]. At this stage of the project, we cannot give you further information about the research method(s) we use for our investigation. You will receive more details about the research methods after the research is completed.

Instructions and procedure

[*If not applicable, leave one or more of the following aspects out*: Give a description of the procedure so that participants know what will happen, what exactly is expected of them, the questions that will

be asked, will there be a publication, more measuring moments, research method, how long it will take, etc. Explain only what is intended, not what is not intended.
**Example of procedure:* During this study you will be shown images of animals in rapid succession. When you see a mammal, use your left index finger to press the button intended for that purpose. When you see a bird, use your right index finger to press the button intended for that purpose. Try to react as quickly and as accurately as possible.*].

Other aspects that might apply:
This study takes approximately [duration of participation in the study].
If the study comprises multiple sessions, specify that, including the duration of each session.
If participants receive compensation, add: After participating in the study, you will receive [amount/credits] [in your bank account/in cash].

1) Data controller in this study
The [name university] is the data controller for this study; you can contact the data controller via [e-mail@uni.nl].

2) GDPR compliance
We process your personal data [specify type of data, specify particular category of data if relevant] on the basis of your consent, in accordance with the General Data Protection Regulation (AVG) and the General Data Protection Regulation Implementation Act (UAVG).

Personal data are data that can be traced back to you individually, either directly or indirectly. When working with (personal) data, researchers may use external parties, for instance when administering online surveys. In that case, appropriate contracts with these parties are in place to warrant your privacy.

3) Voluntary participation
You are participating in this research project on a voluntary basis. This means that you are free to withdraw your consent without giving reasons. This does not affect you and you are not obliged to complete the procedures described earlier. There are no consequences to stopping, other than you not receiving (full) compensation. You can decide to withdraw your consent at any stage of the study. If you decide to withdraw your consent, all information collected by the researcher up to that point will have been lawfully processed. From the moment your consent is withdrawn, your data can only be processed in an anonymised form.

You can withdraw your consent by contacting [the data controller] mentioned under 1).

4) Access to your data by third parties
Your personal data will not be accessed by third parties without your explicit consent.

Collaborations
If you collaborate and/or share data during your research project (with other universities or commercial parties), this must be made explicit in your privacy policy. If you did not close an agreement for the collaboration but are working with an alternative instead, such as a Privacy

Statement, please include this in the informed consent. In that case you do not have to use the options below.

5) Confidential treatment and storage of your personal data

The information collected during this study will only be used for further analysis and publication in scientific journals. Your personal data will not be used in these publications, and we guarantee that you will remain anonymous under all circumstances in any published output, unless you explicitly consent to the sharing of your personal data.

The data collected during the study will be encrypted and stored separately from personal data. This personal data and the encryption key can only be accessed by members of the research staff. Anonymised data will be kept for a period of [standard period in the humanities is 10 years].

6) Data subject request

As a data subject, you have the right to make a request, and have access to the personal data processed about you. You can have your data corrected, erased or object to the processing of (certain) data. You can submit the request to [the data controller] mentioned under 1).

7) Discomfort, risk and insurance

[describe any advantages and disadvantages of the study for the participant. Sample text at D3I:]
The risks of participating in this research are no greater than in everyday situations at home. Previous experience with similar research has shown that participants experienced little or no discomfort. Standard liability insurance applies to all research at the University of [...].

8) Compensation for participation

[Compensation or a small gift may be given; please describe the type of compensation and indicate whether compensation is given based on participation in specific research phases, or whether it is released after the research is completed].

9. Further information

This research has been approved by the Ethics Committee of the Faculty [...] of the University of [...]. For complaints about the research project, please contact the secretary of the Ethics Committee of the Faculty [...] of the University of [...], (telephone number [XXXXXXXXXXXX]; e-mail [XXX.XXX@XXX.XX]).

Confidential treatment of your complaint is guaranteed. You also have the right to lodge a complaint about the handling of your personal data with the Data Protection Authority, in the Netherlands see www.autoriteitpersoonsgegevens.nl).

Annex 2 Template consent form

Participant consent form

I herewith declare that I have been clearly informed about the research project [research project title] at the University of […; name department; capacity group; research school] conducted [optional: by name researcher] at the Faculty of [XXX] of the University of [XXX] [optional: in collaboration with XXX] as described in the privacy policy.

I realise that participation in this research is on an entirely voluntary basis. I retain the right to revoke this consent without having to provide any reasons for my decision. I am aware that I am entitled to withdraw my consent at any time, including after the termination of the research.

My personal information will not be viewed by third parties unless I have given my express permission. My personal data can only be used in scientific publications or made public in any other way under the condition that this happens in an anonymised form.

This research was approved by the Ethics Committee of the Faculty of [XXX] of the University of [XXX]. If I have any complaints regarding the research project, I can contact the secretary of the Ethics Committee of the Faculty of the [XXX] of the University of [XXX], (phone number [XXXXXXXXXX]; e-mail [XXX.XXX@XXX.XX]).

I understand the above text and consent to:
[for the researcher: please delete if not applicable and be aware of that each activity must be clearly and accurately explained in the privacy policy]

- participate in this research yes/no
- that video/audio recordings are being made or used for the research yes/no
- my personal data will be stored for a period of [XXX years/months] yes/no
- my personal data will be transferred to third parties yes/no

Signed:

Name participant Date [Tick box for consent] [X]

Annex 3 Relevant GDPR texts

Here we introduce the relevant texts – the **GDPR Articles** and the **Recitals** researchers must **comply** with whenever they seek to obtain **consent** from the **participants** envisaged in their **study**.

We advise you to **take note** of them. To make the reading of the Articles and Recitals a bit more **accessible**, we highlighted the **most relevant bits** of each Article and Recital.

In the **manual**, we explain what these mean for researchers **in practice**.

Relevant GDPR-elements outside informed consent are elaborated in the **Background document on Scientific Research**.

1.1 Relevant articles

Article 4(11) GDPR - Definition of consent

'consent' of the data subject means 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;

Article 6(1)(a) GDPR - Consent as lawful ground for data processing

Processing shall be lawful only if and to the extent that […] the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Article 7 GDPR Conditions for consent

1. Where processing is based on **consent**, the **controller** shall be **able to demonstrate** that the **data subject** has **consented** to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to **withdraw his or her consent at any time**. The withdrawal of consent shall **not** affect the **lawfulness** of processing **based on consent before its withdrawal**. Prior to giving consent, **the data subject shall be informed thereof**. It shall be **as easy to withdraw** as **to give consent**.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 9(2)(a) – Processing of special categories of personal data

1. **Processing** of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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 shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:
    a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, […];
    b. […]

Article 12 – Transparent information, communication and modalities for the data rights exercises

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 […] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Article 13 GDPR - Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are **collected from the data subject**, the **controller shall**, at the time when personal data are obtained, **provide the data subject** with **all** of the **following information**:

a) the **identity** and the **contact details** of the **controller** and, where applicable, of the **controller's representative**;
b) the **contact details** of the **data protection officer**, where applicable;
c) the **purposes** of the processing for which the personal data are intended as well as the legal basis for the processing;
d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
e) the **recipients** or **categories of recipients of the personal data**, if any;
f) where applicable, the fact that the controller intends to **transfer personal data to a third country** or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the **controller shall**, **at the time when personal data are obtained**, provide the data subject with the **following further information necessary** to **ensure fair** and **transparent** processing:

a) the **period** for which the personal data will be **stored**, or **if that is not possible**, the **criteria used** to **determine that period**;
b) the **existence** of the **right** to **request** from the controller **access to** and **rectification or erasure** of **personal data** or **restriction of processing** concerning the data subject or to **object** to processing as well as the right to data portability;

c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the **existence** of the **right** to **withdraw consent at any time**, **without** affecting the **lawfulness** of **processing based on consent before its withdrawal**;
d) the right to **lodge a complaint** with a **supervisory authority**;
e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
f) the **existence** of **automated decision-making**, **including profiling**, referred to in Article 22(1) and (4) and, at least **in those cases**, **meaningful information** about the **logic involved**, as well as the **significance** and **the envisaged consequences** of such processing **for** the **data subject**.

3. Where the controller intends to **further process** the personal data for a purpose other than that for which the personal data were collected, the **controller** shall provide the data subject **prior to that further processing** with **information** on **that other purpose** and with **any relevant further information** as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 15 GDPR – Right of access by the data subject

1. The data subject shall have the right to **obtain** from the controller **confirmation** as to **whether or not** personal data concerning him or her are being processed, and, where that is the case, **access** to the persona data and the following information:

a) the **purposes** of the processing;
b) the **categories** of personal data concerned;
c) the **recipients** or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged **period** for which the personal data will be **stored**, or, if not possible, the criteria used to determine that period;
e) the **existence** of the right to request from the controller **rectification** or **erasure** of personal data or **restriction** of processing of personal data concerning the data subject or to **object** to such processing;
f) the right to lodge a **complaint** with a **supervisory authority**;
g) where the personal data are not collected from the data subject, any available information as to their **source**;
h) the existence of **automated decision-making**, including **profiling**, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the **logic** involved, as well as the **significance** and the **envisaged consequences** of such processing for the data subject.

2. Where personal data are transferred to a **third country** or to an **international organisation**, the data subject shall have the right to be informed of the appropriate **safeguards** pursuant to Article 46 relating to the transfer.

3. The controller shall provide a **copy** of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.

Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a **commonly used electronic form**.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Article 17 GDPR – Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
c) […].

2. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

d) for […] **scientific** […] **research** purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is **likely** to render **impossible** or **seriously impair** the achievement of the **objectives** of that processing; […].

1.2 Relevant recitals

Recitals are part of the GDPR. Recitals do **not give additional rules**. They **aim** to give the reader – and the researcher – **information** and **background** to how the GDPR articles should be **read** and **interpreted**. Here are the **most relevant Recitals** that relate to **consent**, which can give **researchers** more **handhold** when they are looking for a **proper reading** of the **consent-related articles**:

32
Consent should be given by a **clear affirmative act** establishing a **freely given, specific, informed and unambiguous indication** of the data subject's **agreement** to the **processing** of **personal data** relating to him or her, such as by a **written statement**, including **by electronic means**, or an **oral statement**. This could include **ticking a bo**x when visiting an **internet website**, choosing **technical settings** for information society services or another statement or **conduct which clearly indicates** in this context the data subject's acceptance of the proposed processing of his or her personal data. **Silence**, **pre-ticked boxes** or **inactivity** should **not** therefore constitute consent. **Consent** should **cover all processing activities carried out for the same purpose or purposes**. When the processing has **multiple purposes**, consent should be given for **all of them**. If the data subject's **consent** is to be given **following a request by electronic means**, the request must be **clear**, **concise** and **not unnecessarily disruptive** to the use of the service for which it is provided.

33
It is often **not** possible to **fully** identify the purpose of personal data processing for **scientific purposes** at the time of data collection. Therefore, data subjects should be allowed to give their consent to **certain areas** of scientific research when in keeping with recognised **ethical standards** for scientific research.

Data subjects should have the opportunity to give their **consent only to certain areas of research** or parts of research projects to the extent allowed by the intended purpose.

38
Children merit specific protection with regard to their personal data, as they may be **less aware of the risks**, **consequences** and **safeguards** concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the **purposes of marketing** or **creating personality** or **user profiles** and the collection of personal data with regard to children when using services offered directly to a child. The consent of the **holder of parental responsibility** should not be necessary in the context of preventive or counselling services offered directly to a child.

40
In order for **processing** to be **lawful**, personal data should be processed on the **basis** of the **consent** of the data subject concerned […]

42
Where processing is based on the data subject's consent, the **controller** should be **able to demonstrate** that the data subject **has given consent to the processing operation**. In particular in the context of a written declaration on another matter, safeguards should ensure that the **data subject** is **aware** of the **fact** that and **the extent to which consent is given**. In accordance with Council Directive 93/13/EEC (1) a **declaration of consent pre-formulated by the controller** should be provided in an **intelligible** and **easily accessible form**, using **clear and plain language** and it should **not contain unfair terms**. For consent to be **informed**, the data subject should be aware at least of the **identity of the controller** and the **purposes** of the **processing** for which the **personal data are intended**. Consent should **not** be regarded as **freely given** if the **data subject** has no **genuine** or **free choice** or is **unable** to **refuse** or **withdraw consent without detriment**.

43
In order to ensure that consent is **freely given**, **consent** should **not** provide a valid legal ground for the processing of personal data in a specific case where there is a **clear imbalance between** the **data subject** and the **controller**, in particular where the controller is a **public authority** and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. **Consent** is presumed **not** to be **freely given** if it does **not allow separate consent** to be given to **different** personal **data processing operations** despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.