CELSI Data Protection and GDPR Compliance Guideline

Table of contents

Overall information about data protection....2
Sensitive vs. Non-Sensitive Data....2
How to work with the data (Interviews with Sensitive Information)....4
Annexes....6
Reminders....9
Answers to your questions:....10

Overall information about data protection

CELSI, as a research organization, regularly processes personal data in the context of academic and policy research. It is essential that all members of our team understand the **fundamental principles of data protection (Annex 1)** and our responsibilities under relevant data protection laws, including GDPR and Slovak national data protection legislation.

The **first step** in responsible data handling is understanding what kinds of data we collect and when GDPR applies.
Depending on the project, CELSI may collect various types of personal data. If **individuals are identifiable,** the processing of such **data is subject to the General Data Protection Regulation (GDPR)**. This data may include, but is not limited to:

- Interviews (audio, transcripts, notes)
- Surveys and questionnaires
- Focus groups and workshops (often recorded or transcribed)
- Case studies and field notes (narrative accounts or observations by researchers)
- Audio and video recordings
- Administrative data (contact lists, participant logs)
- Photographs from events

If your data category is not listed above and you are unsure whether the GDPR applies, ask yourself: **Can the individual be identified, either directly or indirectly, through the data or its context (Annex 2)?** If the answer is yes, the data should be treated as personal data under the GDPR.

Sensitive vs. Non-Sensitive Data

Once you have determined that the GDPR applies, the next step is to assess whether the data is classified as sensitive or non-sensitive.
In general, personal data that can be found in public sources and is not inherently private or sensitive is considered non-sensitive personal data.

Examples of **non-sensitive personal data** include, but are not limited to:

- Names

- Email addresses
- Job titles or organizational roles
- Audio recordings (if the speaker is identifiable and the content does not reveal sensitive information)

To process non-sensitive data, CELSI must have a lawful basis for processing, such as **consent, contract, or legitimate interest.** Non-sensitive personal data **does not require special safeguards** unless it is combined with sensitive data (Annex 3).

The second category is **the sensitive data,** the following types of information are classified as **sensitive**:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data used for identification
- Data concerning health
- Data concerning a person's sex life or sexual orientation

CELSI may process **sensitive data** only if one of the following conditions applies:

- **Explicit Consent -** the data subject has given **clear and informed consent** for the processing of their sensitive data for one or more specific purposes. **Example**: A participant agrees to speak about their union membership or political beliefs during an interview.
- **Public Interest Research -** the processing is necessary for **scientific or historical research** purposes and is carried out with appropriate safeguards. This may apply in certain **EU-funded projects**, where legal or ethical justifications exist. **Example**: Research project funded under EU Horizon grants.

- **Data Made Public by the Subject -** the individual has **clearly made the information public** themselves, for example, through a speech, article, or public role. **Example**: A politician publicly expressing views.
- **Legal Claims or Obligations -** the processing is necessary for the **establishment or defence of legal claims**, or to meet specific obligations under Slovak or EU law. **Example**: Personal data processed in the context of legal proceedings or compliance with national laws.

But overall recommendation is always **obtaining a consent!**

How to know if data is sensitive:

- Is it about a person's identity or belief system?
- Could misuse of this data harm them personally, socially, or professionally?
- Would this information usually be treated as private?

If yes - treat it as sensitive.

Working with sensitive data

If sensitive data is likely to be collected CELSI must:

- Obtain **explicit, documented consent** from the participant
- Inform the participant clearly and in writing about how the data will be used
- Apply **technical and organisational safeguards** (e.g. limited access, pseudonymisation, 2FA, VPN)
- And do **Data Protection Impact Assessment (DPIA)** (template – you can use other, the GDPR does not have a required template)

How to work with the data (Interviews with Sensitive Information)

Before the start of the interview, provide the participant with a **signed consent form** (annex 4) and make sure they fully understand what they are agreeing to. After obtaining their consent, proceed with the interview. During the interview, only ask questions that are directly relevant to the purpose of the interview.

Once the interview data is collected, transfer the data to **Dropbox** as soon as possible. Before transferring the data, **pseudonymize** the participant's information to protect their identity. To do this securely, you must use a **VPN connection** during the transfer.

Once the data is safely stored in **Dropbox**, confirm that the folder is secured with **two-factor authentication (2FA)**. After transferring the data, be sure to delete all local copies of the files from your computer. This includes removing the files from the **Recycle Bin** and, if possible, clearing any **cached data** to avoid leaving any trace of personal information on your device.

Also, make sure to **dispose of any paper notes** that contain identifiable information, particularly if these notes could link back to individuals. All personnel working with this data, including **translators**, must sign a **confidentiality agreement** acknowledging their responsibility to protect the data. This guarantees that everyone understands their role in keeping the data secure and private.

When handling the data, always use **VPN** for secure access. This safeguards the data from potential threats and makes certain that only authorized individuals can access the personal information.

Also, store the contact information, such as email, phone, **separately**, for purposes of contacting.

Regularly monitor the data to ensure it is up to date and monitor to ensure continued compliance with GDPR.

Annexes

Annex 1

Principles of Data Processing

Each CELSI staff member involved in processing personal data must ensure that the following GDPR principles are upheld:

- **Lawfulness, fairness, and transparency** – Processing must be fair and based on a legal basis; individuals must be clearly informed.
- **Purpose limitation** – Data may only be collected for specific, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.
- **Data minimisation** – Only data that is necessary for the intended purpose shall be collected and processed.
- **Accuracy** – All personal data must be kept accurate and up-to-date.
- **Storage limitation** – Personal data must be kept only as long as necessary and securely deleted or anonymised after that.
- **Integrity and confidentiality** – Appropriate security measures (technical and organisational) must be in place to protect data from loss, alteration, or unauthorised access.

Wherever possible, CELSI uses **anonymised data**, meaning the person is no longer identifiable by any means reasonably likely to be used. Anonymised data is **no longer subject to GDPR**. If full anonymisation is not possible, **pseudonymisation** should be applied, in which identifying elements are replaced with pseudonyms. This still falls under GDPR.

Annex 2

Even if a person's name or email is not explicitly collected, **they can still be identified** based on combinations of other details. This is known as **indirect identification**, and it still qualifies as personal data under the GDPR.

Examples:

“The chief accountant of the union in Trenčín mentioned that...”
— There may be only one person with that role in that city → identifiable → GDPR applies

“One participant said they had previously worked for the SIS and left due to political pressure.”
— Even without a name, the statement could make the person identifiable → GDPR applies

Annex 3

For CELSI’s research activities, the most relevant lawful bases under Article 6 are:

- **Consent** – when participants voluntarily agree to provide data for a specific purpose.
  Example: A participant signs a consent form before being interviewed or recorded.
- **Legitimate interest** – when data is processed for research purposes in a way that does not override individuals’ rights.
  Example: Analysing anonymised expert statements from a public panel discussion.
- **Public task** – when data is processed as part of publicly funded projects serving the public interest.
  Example: Conducting interviews for a Horizon Europe project funded by the European Commission.

Annex 4

How to structure a consent form for the participants:

- outline the research objectives, intended purposes,
- the identity and contact details of CELSI as data controller,
- who is funding the research,
- the voluntary nature of participation,
- assurance of confidentiality and anonymity,
- potentially expected benefit & burdens of participation,

- details on data use, processing and storage including who will have access (for example other project partners),
- how findings will be published,
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,
- the rights of the data subject (Annex 5)
- any international transfers and applicable safeguards.
- and the right to withdraw from the research at any time without facing any consequences and without any reasons given

If CELSI intends to process **the data for a new purpose**, the data subject must **be informed in advance.**

Annex 5

Data Subject Rights

Under the GDPR, individuals whose data is processed have the right to:

- **Access** – request to see what data is held about them.
- **Rectification** – request correction of inaccurate or outdated data.
- **Erasure** – request deletion of their data ("right to be forgotten").
- **Restriction of processing** – request to limit how their data is used.
- **Data portability** – receive their data in a structured, commonly used format.
- **Object** – refuse processing based on legitimate interests or public interest.
- **Withdraw consent** – revoke consent at any time (where consent is the basis for processing).

Requests must be responded to within **one month**.

Reminders to those working with data

1. Informing data subjects about data transfer to CELSI

Please remind all project partners to inform data subjects that their personal data will be transferred to CELSI for research purposes. For example, they can include a line in their consent form stating that project partners (including CELSI) will have access to the data and clarify that this is part of an international project with multiple partners.

2. DPIA (Data Protection Impact Assessment)

We need to conduct a DPIA before starting interviews. If we later discover that the data processing may lead to high risk, even after we implemented safety measures, we are required to consult the supervisory authority in line with GDPR Article 36.
In the JCA in 10.2: *The parties shall consult the supervisory authority/authorities prior to processing in accordance with GDPR Article 36 where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the parties.*

But I think that it is not necessary to contact Slovak authorities, because, we are going to use safety tools like VPN, pseudonymisation, and two-factor authentication and I think it would be enough, but we could clarify it with the partners.

3. Use of external platforms

If we use third-party tools like Survey Monkey or similar during data collection, we must double-check that their servers and systems are GDPR compliant.

4. Encryption

Encryption means converting personal data into a secure format that can only be read with a decryption key. According to GDPR Article 32, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk—*including, inter alia as appropriate*:

1. the pseudonymisation and encryption of personal data.

So, the way I understand it, encryption is recommended, if we think it's necessary, based on the risk. But, since we're already planning to use VPN and 2FA, that might be enough.

Also, our partners didn’t mention encryption in the JCA, so maybe it's not expected from us, but we can keep it in mind just in case.

5. NDAs (non-disclosure agreements) for all people working with data

We should prepare and sign NDAs before anyone starts working with data, including interpreters or external people.

6. Appoint a Data Protection Officer (DPO) at CELSI

It is necessary to assign someone as a Data Protection Officer (DPO) at CELSI who understands GDPR and can support with DPIA and related questions. It could be also person from CELSI.