# A Primer on the Use of Personal Data from the European Union

The European Union's General Data Protection Regulation (GDPR) regulates the use, access, collection, and processing of all personal data throughout the European Union. The European Commission boasts that the GDPR sets out "some of the highest standards of data protection in the world."[1] It is important for USU investigators conducting human subjects research projects abroad to know what responsibilities they have to citizens of the European Union while collecting or handling their data.

## I. Personal & Sensitive Data

Any research project which uses **personal data** from the European Union must abide by the requirements of the GDPR. **Personal data** is defined as "any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, constitute personal data." The European Commission lists the following examples of personal data:

- A name and surname;
- A home address;
- An email address;
- Income;
- An identification card number;
- An Internet Protocol (IP) address;
- A cookie ID;
- Phone identifiers; or
- Data held by a hospital or doctor which could uniquely identify a person.

If you have data which has been rendered anonymous in such a way that the individual is not identifiable, it is no longer considered personal data. For data to be truly anonymized under the GDPR, the anonymization must be "*irreversible*."

If personal data is also **sensitive data**, it requires "special protection," meaning that you must obtain explicit consent to be collect or use it. This means that the receipt of sensitive data that originates in the European Union must always be accompanied by the explicit consent of the individual, and for a specified purpose (i.e. "passive consent," or a Letter of Information, is not sufficient). **Sensitive data** is data concerning "one's health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, biometric data, or data concerning a natural person's sex life."

## II. Children

The GDPR defines a **child** (for the purposes of using or accessing personal data) as an individual **under the age of 16**. For any personal data collected regarding a child under the age of 16, the "holder of parental responsibility" must explicitly consent to the collection or use of that child's data. Note, however, that individual member states are given the latitude to lower that age within their own jurisdiction, but can never go below age 13.

- Protis Tip: Use the "Submit" section in the protocol to provide documentation relating to the age limits for your particular jurisdiction if you plan to utilize 13-15 year olds without seeking parental consent.

[1] European Commission. *Communication from the Commission to the European Parliament and the Council: Stronger Protection, New Opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018*. January 1, 2018.

## III. Data Collection & Access Requirements

There are particular pieces of information which must be provided to an individual when their personal data is being collected, used, or accessed. If **sensitive data** is being collected, used, or accessed, please remember that you must use the full informed consent process, with translation as appropriate. You are required to ensure that you are collecting only the minimum necessary information for your defined purpose.

- Protis Tip: It is best to wait until the English version of your Informed Consent document has been labeled "Ready for Translation" in Protis before you translate it into another language. This way, you are certain that your translation encompasses all of the possible edits needed throughout the review process.

Below is the information that must be provided to an individual in the European Union whose personal data is being collected, used, or accessed for research by a USU researcher:

- The specific purpose for the use of the data
- The legal basis for using the data
- How long the data will be stored
- Who will view or use the data
- The data protection rights available (see IV., below)
- Whether the data will be removed from the EU
- Where one could lodge a complaint about their data use or protection
- How to withdraw consent for use of the data once it has been given (and it must be "as easy" as the process for giving consent in the first place)
- Contact information for USU and the relevant Data Protection Officer

Protis Tip: Consider incorporating these bulleted points in a new subsection of your informed consent document titled "EU General Data Protection Regulation Information," rather than working to incorporate them into established headers within that document.

According to the GDPR, personal data can only be collected and processed for "a well-defined purpose." This essentially negates our ability to approve deception research in the European Union at this time; member states are working on further definition of the GDPR as it relates to research in particular locales.

## IV. Data Storage & Maintenance Requirements

Once you possess the personal data of an individual from the European Union, they are entitled to certain rights regarding how the data is handled. This means that you must store their information in a way that permits them to take advantage of the following rights:

- The right to access the data, free of charge, in an accessible format.
- The right to object to a particular use of that data.
- The right to correct the data in the event the individual feels that it is incorrect, incomplete, or inaccurate.
- The right to "be forgotten," or to erase all data relating back to that person in an irreversible fashion. Parents of children and children each individually hold this right, so *either* of those parties can require a child's data to be deleted.
- The right to move data; this means that the individual can ask you to transfer it to them, or to another party, in a commonly-used and machine-readable format.

The GDPR permits the retention of personal data for only as long as is necessary to achieve the specific purpose for which it was collected. It must be deleted after that time. If there is a data breach which could pose any risk to your participants, you must inform your participants of the breach.