General Data Protection Regulation (GDPR)
Frequently Asked Questions

GENERAL

What is GDPR?

The General Data Protection Regulation (GDPR) is a European law that establishes protections for the privacy and security of personal data about individuals in European Economic Area (EEA) countries. It applies to the collection and use of personal information:

1. Through activities within the borders of EEA countries,
2. That is related to offering of goods and services to EEA residents, or
3. That involves monitoring the behavior of EEA residents.

GDPR is in effect as of May 25, 2018.

What countries are adopting GDPR?

The countries making up the European Economic Area (EEA) are all adopting GDPR. This includes all European Union (EU) countries, as well as a few others: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

Note: The United Kingdom will still abide by GDPR after it leaves the EU.

This is a European regulation. Does it affect me in the US?

Yes. Personal data collected in, or transferred from, any of the above-listed countries is subject to the GDPR.

Why should I care about the GDPR?

Researchers are required to abide by all regulations and policies covering your research. Failure to do so puts the university and yourself at risk of noncompliance, monetary fines, and reputational harm. Fines associated with noncompliance under the GDPR are particularly hefty. Fines can be up to 20 million Euros or 4% of the university's prior financial year worldwide annual revenue.

How does the GDPR define 'personal data'?

GDPR defines '**personal data**' as "any information relating to an identified or identifiable natural person ('data subject')."

An '**identifiable person**' is defined as "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Under the GDPR, personal data also includes: racial or ethnic origin, political opinions, religious beliefs, trade union membership, health (physical or mental), genetic data, and sexual orientation/activity.

RESEARCH ACTIVITIES

How does the GDPR relate to research in general?

1. It establishes the circumstances under which it is lawful to collect, use, disclose, destroy, or otherwise process 'personal data.'
2. It establishes certain rights of individuals in the EEA, including rights to access, amendment, and erasure (i.e., right to be forgotten).
3. It requires researchers to implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk of the data.
4. It requires notification to data protection authorities and affected individuals within 72 hours following the discovery of a personal data breach, which is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

What activities are subject to the GDPR?

1. Activities involving identifiable information if personal data is being collected from one or more research participants **physically located** in the EEA at the time of data collection (even if the participant is not an EEA resident).
2. Activities involving the **transfer of personal data collected under the GDPR from an EEA country to a non-EEA country**.

What are examples of activities that are NOT subject to the GDPR?

Activities involving collection of identifiable personal data from individuals who are **physically located within the United States** at the time of data collection (even if the participant is an EEA citizen).

What steps can I take to help ensure my project will be GDPR-compliant?

Researchers:

1. Should **collect only the absolute minimum personal/demographic data** needed to complete the study. If a study can be completed using only de-identified data that is strongly encouraged. (Note: Many online survey sites collect personal information, including IP addresses, by default. Ensure you setup your study to receive only the information you are seeking.)
2. Must only use **active ("opt-in") informed consent**. Consent must be freely given, specific, informed, unambiguous, and explicit. A description of the data processing and transfer activities to be performed, if applicable, must be included in the informed consent document. Following an informed consent description, a "Click next to proceed to the survey" button or equivalent is sufficient for "active" consent for online data

collection. Silence, pre-ticked boxes, and inactivity do not constitute "active" consent.

3. To the extent possible, must verify any **third-party** website or app being used for data collection is GDPR-compliant.
4. Must include a **privacy statement** as part of the informed consent document. ORCI is currently working to draft template language to include for any study involving internet-mediated research and/or collection of information from individuals in the EEA.
5. Must indicate in the **informed consent that a data breach is a potential risk** of the study.
6. For activities in which identifiable data is collected, must have an **executable plan in place to remove data in the event a participant requests to have their data removed**. (Note: The informed consent document requires that the participant be notified that their participation is voluntary and that they may leave the study at any point; the informed consent document does not require the researcher to document *how* the data erasure will take place if requested.)
7. Must **notify the university immediately in the event of a data breach**.

HUMAN RESEARCH REVIEW COMMITTEE (HRRC) STUDIES

Does the GDPR only apply to projects that are reviewed and approved by GVSU's Human Research Review Committee (HRRC)?

No. The GDPR is a completely separate regulation from the regulations that oversee human subjects research. There may be instances where a project may not fall under HRRC review, but would still need to abide by the GDPR.

My project was previously approved by the HRRC. Do I need to do anything further to be in compliance with the GDPR?

Possibly. Further action would depend on who and how you are recruiting participants and the data being collected. Please contact the Office of Research Compliance and Integrity (rci@gvsu.edu; 616-331-3197) to discuss your protocol if your research will involve any of the following after May 24, 2018:

1. Recruitment through social media site(s)
2. Use of a third-party internet site (such as Qualtrics, Skype, etc.) or app to collect data
3. Direct receipt of data from individuals (participants, research collaborators, etc.) in an EEA country.

If after discussing your protocol with ORCI it is determined that protocol changes are necessary, these changes will need to be formally submitted via a Change in Approved Protocol Form and approved by the HRRC. The ORCI will work with the HRRC to expedite the review of changes to GDPR-affected protocols as quickly as possible, in an effort to avoid any delays in your research.

DATA COLLECTION & MANAGEMENT

Are there special consent requirements for the GDPR?
Yes. Participants having their data collected or transferred must actively "opt-in" for all GDPR-covered research. This means they must sign a form, check a box, or in some other way *actively* indicate they will allow their data to be used for the proposed research activity. "Opt-out" consent is not permissible for collection of GDPR-covered data. Silence, pre-ticked boxes, and inactivity do not constitute consent.

My study involves data collection from EEA participants, but the data being collected is not private identifiable information. Is my project still subject to GDPR?
No, so long as the collected data cannot be used to directly or indirectly identify participants. Note, however, that some third-party data collection sites (such as survey hosting sites) might collect personal data covered by the GDPR, even if this information is not passed along to you as the researcher. When using third-party sites, you as the researcher (and person obtaining consent from the research participant) are responsible for ensuring the third-party site being used is operating in a GDPR-compliant way. This can be done by vetting (to the extent possible) the privacy and security policies of the site you are using.

I will be traveling to a country covered by the GDPR and will be sending data to the United States while on the trip. Is this affected by the GDPR?
Yes, if you are sending any 'personal data' as defined by the GDPR. Any personal data you send when physically located in an EEA country falls under the GDPR, even if you are a US citizen. Any data falling under the GDPR requires the data subject to provide consent to allow the data transfer to occur. Therefore, if this consent was not obtained, the data cannot be transferred.

My research project involves recruiting participants and/or collecting data through internet sites. Does this fall under the GDPR?
Possibly. Since online surveys/interviews can be completed from any location with internet access, a participant may be engaging in your research project from an EEA location without your knowledge. As such, all activities involving online collection of personally identifiable information should be designed to be GDPR-compliant.

You are **strongly encouraged** to add a question to the beginning of your survey to determine if the individual is participating from an EEA location. The response to this question is a simple way to determine if any participants in your activity are covered under the GDPR. Alternatively, you could use this question to remove EEA participants from the participant pool prior to collecting any identifiable data, thereby ensuring your activity does not fall under the GDPR.

I am contacting study participants in the EEA directly to obtain information for my research. Does this fall under the GDPR?
Yes, if the participants are providing you 'personal data' as defined by the GDPR. Please contact the Office of Research Compliance and Integrity (rci@gvsu.edu; 616-331-3197) to discuss your specific project.

What is the best way to secure GDPR-covered data?
According to the GDPR, appropriate technical and organizational measures must be in place to ensure a level of security appropriate to the risk. The HRRC already requires similar measures to be in place for human subjects research studies. (See HRRC Policy 730 for more information: https://www.gvsu.edu/hrrc/hrrc-policies-procedures-guidance-17.htm.) Additionally, GVSU has secure servers available for researchers who are collecting private identifiable information; researchers are encourage to use those secure servers for storage of their project data for any project involving personal or sensitive data. Where possible, researchers should also convert identifiable data to de-identifiable data at the earliest possible point in the project and destroy personal identifying data when possible. (Note: if data destruction is to be a part of the research plan, the participant must be notified of this in the informed consent document.) Using these servers can help ensure data is properly destroyed in the event data removal is requested. Please contact Matt Hodgman (hodgmanm@gvsu.edu; 616-331-2441) for more information about accessing and using the secure servers.

What is "right to erasure"?
Under the GDPR individuals have the right to request that their previously provided data be erased. If an individual covered by the GDPR contacts you at any point after data collection asking for their data to be erased, please contact the Office of Research Compliance and Integrity (rci@gvsu.edu; 616-331-3197).

GVSU has secure servers available for researchers who are collecting private identifiable information; researchers are encourage to use those secure servers for storage of their project data. Using these servers can help ensure data is properly destroyed in the event data removal is requested. Please contact Matt Hodgman (hodgmanm@gvsu.edu; 616-331-2441) for more information about accessing and using the secure servers.

If there is a data breach for research subject to GDPR, what needs to happen?
The GDPR has strict rules and timelines regarding the report of data breaches. As such, any data breach occurring on a project involving GDPR-covered research **must be reported within 24 hours upon identification of the breach to the Vice Provost for Research Administration** (Robert Smart, smartr@gvsu.edu; 616-331-) **and the Office of Research Compliance and Integrity** (rci@gvsu.edu; 616-331-3197). The following information should be communicated:

1. Type of breach
2. Nature, sensitivity and volume of personal data
3. Severity of consequences for individuals
4. Number and characteristics of affected individuals
5. Ease of identification of individuals
6. HRRC protocol number, if applicable

The Vice Provost for Research Administration will assess the situation and take the appropriate next steps. Researchers should not contact the affected individuals directly about a data breach, unless explicitly directed to do so by the Vice Provost for Research Administration.

If the breach occurs on an HRRC protocol, it must also be reported to the HRRC via the Unanticipated Problem/Serious Adverse Event Reporting Form within 7 calendar days.

FURTHER INFORMATION

Whom can I contact with further questions?

Please contact the Office of Research Compliance and Integrity (rci@gvsu.edu; 616-331-3197) regarding any questions related to research and the GDPR.