**Overview**

The *General Data Protection Regulation (GDPR)* implements strict rules regarding the processing and movement of personal data for any resident located in the [European Economic Area (EEA)](https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:European_Economic_Area_(EEA)). This will impact research studies at Rutgers which collect/process personal data from the EEA regardless if they will conduct their research from inside the EEA or remotely from the USA.

To address any potential GDPR requirements from an IRB perspective, complete *HRP-335 - WORKSHEET - GDPR IRB Compliance - Data Protection And Privacy* to determine if GDPR applies to your research [LINK <https://research.rutgers.edu/researcher-support/research-compliance/human-subjects-protection-program-toolkit> ].

If GDPR does apply to your research:

1. Review this guidance page.
2. Use the GDPR Special Consent Passage [LINK <https://research.rutgers.edu/researcher-support/research-compliance/human-subjects-protection-program-toolkit> ] to address any additional GDPR consent requirements.

\*\*\*Please note that GDPR has additional requirements which are outside the scope of the IRB. For assistance with these other requirements, contact Rutgers University Ethics and Compliance-Privacy Department [LINK]. <https://uec.rutgers.edu/contact-us/staff-directory/>

**FAQ**

**Q. What is GDPR?**

1. A set of regulations designed to give individuals more control over how their personal data is collected, used, and protected online. It also binds organizations to strict new rules about using and securing the personal data they collect from people, including the mandatory use of technical safeguards like encryption and higher legal thresholds to justify data collection. Organizations that don’t comply will face heavy penalties of up to 4 percent of their global annual revenue or €20 million, whichever is higher ([gdpr.eu](https://gdpr.eu/companies-outside-of-europe/)). A list of countries in the EEA and EU governed by GDPR can be found [here](https://www.gov.uk/eu-eea).

**Q. Does GDPR apply to a non-EU based organization like Rutgers University?**

1. Yes, when Rutgers University Researchers process the personal data of EU citizens. This includes transfers of the data back to the USA (see GDPR Article 44) [LINK <https://gdpr-info.eu/art-44-gdpr/>], when you process data as a Data Controller and Data Processor (see [GDPR Art. 3.1](https://gdpr-info.eu/art-3-gdpr/)), and applies to organizations who are not present in the EU (see [GDPR Art. 3.2](https://gdpr-info.eu/art-3-gdpr/)).

**Q. I’m not conducting research in person in the European Union, does GDPR affect me as a researcher in the USA?**

1. Yes, if you are processing personal data from EU residents. According to GDPR Art. 3: “This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not ([GDPR Art. 3](https://gdpr-info.eu/art-3-gdpr/)).

**Q. Can I conduct international research using personal data from residents in the European Union without the need to adhere to GDPR?**

1. Yes, but you must only collect and process anonymous data as defined in GDPR. This does not include coded data as defined in US regulations.

**Q. How does GDPR impact my research?**

1. If your research is governed by GDPR, you will need to make sure it is designed in a way which meets the data privacy standards in GDPR as described in your research protocol. You must also have a GDPR compliant consent form (when applicable) which must include all the features and subject rights which GDPR provides to EEA residents. There may also be additional GDPR requirements which are outside the scope of the IRB and those are managed by Rutgers UEC.

**Q. Aren’t the data privacy laws in the USA enough the meet the requirements of GDPR?**

1. No. GDPR Data Privacy laws are much stricter and extensive compared to the USA. **The USA is not currently on the list** of “*Secure third countries*” for which the European Commission has confirmed a suitable level of data protection on the basis of an adequacy decision.

**Q. My project only involves processing GDPR “Personal Data” on behalf of others. Do I still need to comply with the GDPR?**

1. Yes. Your role under GDPR would be a “Data Processor” as defined under [GDPR Art. 4.8.](https://gdpr-info.eu/art-4-gdpr/) It requires GDPR compliance. Data Controllers are only able to utilize a Data Processor if “... sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject” ([GDPR Art. 28](https://gdpr-info.eu/art-28-gdpr/)).

**Q. Does GDPR still apply if I am transferring data out of the EU?**

1. Yes. You are only able to transfer GDPR Private Data out of the EU if you have a lawful reason and you must maintain the same data protections as if the data remained in the EU ([see GDPR Chap. 5](https://gdpr-info.eu/chapter-5/)). If not, the outgoing transfer will be unlawful.

**Q. Does GDPR still apply if I recruit citizens from the European Union who are in the USA?**

1. No. The location of the processing of data is more important than the citizenship of the person ([see GDPR Art. 3](https://gdpr-info.eu/art-3-gdpr/)). In this situation, the data processing is not taking place in the EEA.

**Q. If my research does not include EEA residents and GDPR does not apply, would any other data privacy regulations still be a concern for me conducting research in the USA or internationally?**

1. Yes. Data privacy laws vary across different US States and international countries. Many are working on implementing new stricter data privacy regulations as well. It is important to check your local laws and addressing these regulations in your protocol and consent form.

**Q. How do I get my GDPR data from the EEA back to the USA as part of my research project?**

1. GDPR restricts (does not allow) transfers of personal data outside the EEA because individuals risk losing the protections afforded by the regulation except under the following circumstances:
   * 1. Transfers of personal data to Non-EEA/EU countries which have the same level of data protections ([GDPR Art 45](https://gdpr-info.eu/art-45-gdpr/)) are allowed. [*The USA does not have the same level of data protections as GDPR affords. As such, Exception a. does apply to research projects proposing to transfer personal data to the USA collected from the EEA/EU countries.*]
     2. Transfers of anonymous data to Non-EEA/EU countries ([GDPR Art 49](https://gdpr-info.eu/art-49-gdpr/)). [If you collect only anonymous data or collect personal data that you have anonymized in a way that makes it no longer possible to identify individuals—even when combined with other information which is available to receiver—it is no longer considered personal data protected under GDPR. You are free to transfer the anonymous or anonymized data outside the EEA.]
     3. Subject has consented to the transfer of their personal data collected for the research to a Non-EEA/EU country which does not have the same level of data protections. [Design your study to obtain consent from subjects. Add GDPR passages to outline the details about data collection and transfer to the USA [LINK to our templates page https://research.rutgers.edu/researcher-support/research-compliance/human-subjects-protection-program-irbs]. as been obtained. If the study does not plan to consent subjects or was conducted without disclosure about transfer of personal data to the USA, either (a.) anonymize the data before transfer, or (b) re-consent subjects to obtain their permission to transfer personal data to the USA.

NOTE: When Exceptions apply allowing for transfer of personal data to Non-EEA/EU countries with lower levels of data protection, the data controller and data user must still have adequate plans to protect the data consistent with GDAP Appropriate Safeguards ([GDPR Art 46(2)](https://gdpr-info.eu/art-46-gdpr/).

**Q. I am a Rutgers PI managing one local site in the USA, as part of an international study with other sites located in the European Union. Is GDPR compliance required if my site is only sending data to the EU and not receiving any EU Personal data?**

1. The answer to this question varies depends on whether any EU personal data is being received by the USA site, who is being targeted for recruitment, where participants are residing when receiving any study follow-up, and other considerations. For multisite studies, or any unique considerations not addressed in this guidance, contact your IRB and/or University Ethics and Compliance for assistance.

**GDPR Requirements**

The following are IRB related requirements. Please include all items as applicable in your research:

**Protocol Requirements** *(not an exhaustive list)*

|  |  |
| --- | --- |
| **Requirement** | **Regulatory Reference** |
| Provide a legal reason why data is being processed using GDPR’s list of allowable reasons. If your purpose is not on the list, your data processing activity is not lawful and cannot commence. | Includes a **legal basis** for data processing was identified for each type of data collection situation ([*GDPR Art 6*](https://gdpr-info.eu/art-6-gdpr/)). All Studies are required to select and document a valid legal basis for data collection/processing (specific legal basis scenarios provided by GDPR) and must include a justification for why the researcher believe it applies. For studies involving Secondary Data (use of data that was previously collected for another purpose), the legal basis provided must be compatible with the original legal basis when it was originally collected. (Note: you usually cannot swap from consent to a different basis). Rutgers University recommends the selection of “Consent” as the legal basis. If the PI has not selected “Consent” or has additionally selected any of the other of the six valid reasons (legal basis) as allowed under GDPR (includes contract, legal obligation, vital interest, for official authority, or legitimate interest) STOP: contact the IRB for assistance. Consent: All data subjects involved in this study will give consent to the processing of their personal data for one or more specific purposes. |
| Provide an additional legal reason which confirms why “Special Category Data” is being processed using GDPR’s list of allowable reasons. Also include why you selected that reason. | Includes a separate **legal basis** for studies which contain ***Special Category Data***, was selected and documented as required in ([*GDPR Art 9.2*](https://gdpr-info.eu/art-9-gdpr/)) identifying why the processing of special category data is allowed and includes a justification for why the researcher believe it applies ([*GDPR Art 9.2*](https://gdpr-info.eu/art-9-gdpr/)). Rutgers University recommends the selection of “Consent” as the legal basis. |
| Provide an additional legal reason which confirms why “Secondary Data” is being processed using GDPR’s list of allowable reasons. Also include why you selected that reason. | If you will be using **Secondary Data** and collecting new data, you will need a separate legal basis for each. If the PI has not selected “Consent” or has additionally selected any of the other of the six valid reasons (legal basis) as allowed under GDPR (includes contract, legal obligation, vital interest, for official authority, or legitimate interest) **STOP**: Contact the IRB for assistance. Consent: All data subjects involved in this study will give consent to the processing of their personal data for one or more specific purposes. |
| If you are collecting non-sensitive data from the internet (e.g. social media sites), you will need to get consent from each user. | If the study involves **Secondary Data Collection** (non-sensitive data only) from a public online source (e.g. social media websites, public databases). [Publicly Accessibility Does Not Equal Consent] ([*GDPR Art 14*](https://gdpr-info.eu/art-14-gdpr/)). Rutgers University requires “Consent” as the legal basis to collect secondary data from online sources. The Term and Conditions of a website are not sufficient to demonstrate consent. (**Note**: For publicly accessible social media data which contains “Sensitive Data”, consent cannot be inferred and must be explicit.)**.** For further guidance, contact Rutgers University Ethics and Compliance. |
| Provide the details of the data’s transfer from the EU to the USA. | Provides details of data transfer including: how data will be transferred, to whom (identify countries and recipients), method and security of data storage, and how transfer meets GDPR data protection standard’s approved codes of conduct ([*Art. 40 GDPR*](https://gdpr-info.eu/art-40-gdpr/)). **Rutgers University assumes that all data will always be transferred back to the USA.** |
| Explain your reason to collect each type of data with a focus on minimizing the amount of data needed. | The data to be collected is the minimum necessary to achieve the research objectives. |
| Confirm that you considered using anonymized or coded data to reduce data risks. | The potential for using anonymized or pseudo-anonymized (coded) data has been considered. |
| Confirm your data security plan. | All data will be collected, transmitted, and stored securely. |
| Confirm your data security plan’s level of security, matches the risk level of your data (more risk, more security). | Provides a data security plan whose level of data security is appropriate to the risks represented by the processing. |
| Confirm how your study’s data security plan will be regularly tested to ensure its security. | PI provides a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. (Must be documented but can be delegated to your organization’s IT Department) |
| Confirm your plan to destroy the data when if it no longer required. | Plans are in place for the secure disposal and/or destruction of personal data when no longer required. Note: data retention must be compliant with the *Rutgers University Data Retention Policy*, which stipulates that research data and records should be retained for a minimum of 3 years after the end of the research or longer if required by research funders, regulators, or state/local laws. For RU policies see “Record Keeping and Record Retention”: https://research.rutgers.edu/researcher-support/research-compliance/human-subjects-protection-program-irbs/hspp-guidance-topics |
| Explain why you will be keeping the data for the length of time you specified. | Provides a detailed procedure which includes a clear rationale for the length of time data will be kept as fully identifiable data (data in fully identifiable must be stored for the shortest time possible). |
| Confirm your data breach plan. | Provides a plan for the Data Controller’s Data Protection Officer (DPO) to notify all stakeholders, should a data breach occur. Includes plan to contact the Supervisory Authority ([*GDPR Art 55*](https://gdpr-info.eu/art-55-gdpr/)), and how the Data Processor notifies the Data Controller ([*GDPR Art 33*](https://gdpr-info.eu/art-33-gdpr/)), and if breach is high risk, the data subjects ([*GDPR Art 34*](https://gdpr-info.eu/art-34-gdpr/)) as applicable. With a deadline of no later than 72 hours after having become aware of it. (Note: this is a separate requirement compared to an IRB Reportable Event and a Rutgers University Ethics and Compliance (UEC) report). |
| Confirm how your study addresses subject vulnerability to coercion and undue influence (e.g. subjects recruited by employer) | Consent Process takes into consideration and addresses any imbalance between the parties during the consent process i.e. employee/employer, doctor/patient, teacher/student, etc. and it is included in consent process ([*GDPR-Consent*](https://gdpr-info.eu/issues/consent/)). |
| Confirm your plan for utilizing external databases. | If research data will be added into an external database (e.g. CT.gov, GWAS, dbGap, or other U.S. or international public access database), protocol documents where and what data will be submitted. **☐ N/A** |
| Confirm the details of each Data Controller. | Clearly identifies each Data Controller (role which determines the purposes and means of the processing of personal data) including the PI and their responsibilities and obligations under GDPR ([*GPDR Chap 4*](https://gdpr-info.eu/chapter-4/)). |
| Confirm the details of each Data Processor, if applicable. | Clearly identifies each Data Processor (role which processes personal data on behalf of the controller) and their responsibilities and obligations under GDPR ([*GPDR Chap 4*](https://gdpr-info.eu/chapter-4/)). **☐ N/A** |
| Confirm the details of your Data Processing Agreement (DPA), if applicable. | Data Processing Agreement (DPA) ([*GDPR Art 28.3*](https://gdpr.algolia.com/gdpr-article-28)): A legally binding *Data Processing Agreement* (DPA) or commissioned data processing clause exists between the controller and each processor (and/or their sub-processors) whenever a data processor carries out any processing on behalf of a Data Controller. It documents the Data Processor’s role, responsibilities, how they will ensure the security of personal data, and their assurances to adhere to all GDPR regulations. (Note: All data processing agreements (DPA) must be approved by the Rutgers Research Contract Services and then uploaded into eIRB.) **☐ N/A** |
| Confirm your Data Protection Officer (DPO). | Data Protection Officer (DPO) ([*GDPR Art 37*](https://gdpr-info.eu/art-37-gdpr/)) has been identified and documented with contact information (usually the Principal Investigator). |
| Confirm how you investigated local EEA member laws to see if there are any additional local requirements to conduct GDPR compliant research. | Protocol confirms and documents compliance to any GDPR “open causes” which allow individual members states to implement stricter local rules (e.g. stricter local rules for sensitive data involving health or genetics, for the designation of a data protection officer, the age of consent of children, data protection in the context of employment, and data breach notification obligations). |
| Confirm how you addressed GDPR Subject Rights. | GDPR Subject Rights ([*GDPR Art 12.2*](https://gdpr-info.eu/art-12-gdpr/)) (includes all required GDPR Subject Rights and deadlines when organization will comply, usually one month, if more time is required, subject must be notified) (Applies when data is in identifiable form). Explains how PI will address each right and provides procedures. |

**Consent Requirements** *(not an exhaustive list)*

Consent includes *Rutgers IRB GDPR Section* added before the signature line of your consent document. The section must include the following informational elements:

|  |  |
| --- | --- |
| **Requirement** | **Regulatory Reference** |
| Explain all legal GDPR reasons for using each type of data or action. | Documents all applicable legal basis(s) as described in the protocol: processing data, processing special category data, transferring data outside the EEA ([*GDPR Chap 5*](https://gdpr-info.eu/chapter-5/)). |
| Explain data transfer details. | Documents whether data will be transferred outside the EEA and all details as explained in the protocol. |
| Address each GDPR Subject Rights | GDPR Subject Rights ([*GDPR Art 12.2*](https://gdpr-info.eu/art-12-gdpr/)) (includes all required GDPR Subject Rights and deadlines when organization will comply, usually one month, if more time is required, subject must be notified) (Applies when data is in identifiable form). |
| Provide GDPR Subject Rights deadlines. | Consent procedures include specific deadlines for completing any subject rights requests (normally 30 days). |
| Provide details about each Controller. | Clearly identifies each Data Controller (role which determines the purposes and means of the processing of personal data) including the PI and their responsibilities and obligations under GDPR ([*GPDR Chap 4*](https://gdpr-info.eu/chapter-4/)). |
| Provide details about each Processor. | Clearly identifies each Data Processor (role which processes personal data on behalf of the controller) and their responsibilities and obligations under GDPR ([*GPDR Chap 4*](https://gdpr-info.eu/chapter-4/)). **☐ N/A** |
| Provide details about Data Protection Officer (DPO) | Data Protection Officer (DPO) ([*GDPR Art 37*](https://gdpr-info.eu/art-37-gdpr/)) has been identified and documented with contact information (usually the Principal Investigator). |
| Provide details of data transfer. | Provides details of data transfer including: how data will be transferred, to whom (identify countries and recipients), method and security of data storage, and how transfer meets GDPR data protection standards approved codes of conduct ([*Art. 40 GDPR*](https://gdpr-info.eu/art-40-gdpr/)). **Rutgers University assumes that data will always be transferred back to the USA.** |
| Provide purpose for using each type of data. | The purposes for which the personal data or special category data will be processed. Each purpose must be listed separately, and all items must be accepted for any subject participating in the study. E.g. personal data is being collected to conduct a particular study. |
| Explain data anonymization/destruction plan. | Contains details specifying when the personal data or special category data will be anonymized and/or destroyed. |
| Explain how long data will be stored. | Time period for which personal data will be stored or criteria used to determine length of time data will be stored. |
| Provide subject complaint procedures. | Contains detailed procedure for receiving and addressing complaints from research participants. |

**Additional Points to Consider**

* Explicit Consent, (Explicit consent - an individual's explicitly indicates their consent, for example by signature, recorded oral consent or a two-step verification system of consent. ) may be required because the study involves ‘Special Category’ Data ([*GDPR Art. 9*](https://gdpr-info.eu/art-9-gdpr/)) and/or is it being transferred outside the EEA. Acceptable Explicit Consent examples include: hand-written signature, electronic signature, or a two-step electronic verification process ([*11/28/17 Article 29 Consent Guidance*](https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030)).
* **Research with Minors** ([*GDPR Art 8*](https://gdpr-info.eu/art-8-gdpr/)): “Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child”. **NOTE** EEA local state laws may also apply around research involving minors ([*GDPR Art 8*](https://gdpr-info.eu/art-8-gdpr/)).
* **Broad Consent:** At Rutgers University, Broad Consent Is Not Permitted When Rutgers Is the IRB Of Record.
* **Data Protection Impact Assessment (DPIA)**: ([*GDPR Art 35*](https://gdpr-info.eu/art-35-gdpr/)): A DPIA is required “Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.” If your study meets these requirements, contact the Rutgers IRB for assistance.
* **Processing Personal Data About Criminal Convictions Or Offences** is only lawful if it meets all of the GDPR requirements as described in the regulations ([*GDPR Art 10*](https://gdpr-info.eu/art-10-gdpr/)).

**Common GDPR Definitions**

* **Personal Data**: Any information relating to an identified or identifiable natural person (‘data  
  subject’); an identifiable natural person is 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. It can include anything from a name, a photo, an email address, bank details, posts on social  
  networking websites, medical information, or a computer IP address.
* **Processing**: Any operation or set of operations which is performed on personal data or on  
  sets of personal data, whether or not by automated means, such as collection, recording,  
  organization, structuring, storage, adaptation or alteration, retrieval, consultation, use,  
  disclosure by transmission, dissemination or otherwise making available, alignment or  
  combination, restriction, erasure or destruction
* **Controller**: The person, agency or other body which, alone or jointly with others, determines  
  the purposes and means of the processing of personal data
* **Processor**: The person, agency or other body which processes personal data on behalf of the  
  controller

**Help**

For IRB related GDPR issues, contact your local IRB.

For GDPR inquires related to subject rights or all other Non-IRB GDPR compliance issues, contact Rutgers University Ethics and Compliance-Privacy Department. <https://uec.rutgers.edu/contact-us/staff-directory/>

If you like to see your GDPR question added to the GDPR FAQ, please email your local IRB. https://research.rutgers.edu/researcher-support/research-compliance/human-subjects-protection-program-irbs/identify-your-irb