The European Union (EU) General Data Protection Regulation (GDPR)

What is the GDPR?

The General Data Protection Regulation (GDPR) applies broadly to the processing of personal information of individuals while they are in the European Union (EU) and European Economic Area (EEA) and to the processing of information by an EU organization regardless of where the processing takes place. (Note that, in addition to EU Member states, the GDPR also applies to Iceland, Norway, Liechtenstein, and Switzerland). Generally speaking, the regulation applies to all personally identifiable data that is collected, used, stored, or otherwise processed about individuals in the EU by any method, including electronic and paper records.

What is "personal data" under GDPR?

"Personal data" refers to any information that relates to an identified or identifiable natural person, i.e., a living individual, not a company or organization. Under GDPR, the term "personal data" covers a broader spectrum of personally identifiable information than other U.S. regulations such as FERPA, HIPAA or the Common Rule. Examples of personal data under GDPR include names, email addresses, IP addresses, Internet cookies, voice or image recordings, dates unique to an individual (e.g., birthdates, employment appointment dates), and locations (e.g., physical address, GPS information). Other examples include combinations of information that may be used to identify an individual, such as combining information about a person's place of employment, amount of education, marital status, and place of birth.

Does the GDPR apply to data that includes keys to directly identifiable data store elsewhere?

The GDPR uses the term "pseudonymized" to refer to data that can no longer be attributed to a specific individual without use of additional information; this can be achieved by the process of removing identifiers directly from data and linking the data to identifiers via keys or codes, provided that appropriate measures are in place to ensure that individuals cannot be re-identified. Under GDPR, pseudonymized data is still considered personally identifiable data and must comply with GDPR, even if the data receiver does not have access to the coding system or set of identifiers.

Does the GDPR apply to Anonymized Data?

GDPR does not apply to data that have been fully anonymized (i.e. not pseudonymized). Anonymized data is defined as information that is "rendered anonymous in such a manner that the data subject is not or no longer identifiable" based on "whether means are reasonably likely to be used to identify" the individual. This is a fact-specific inquiry that takes into account available technology and the cost and time required to identify the individual.

Do some categories of data require special attention?

The GDPR considers the following information to be "special categories" of data:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership
- Genetic or biometric data
- Data concerning health, sex life, or sexual orientation

Special care is required when collecting data from these categories and one must have a clear legal basis to collect this data or NYU must obtain the explicit consent of the subjects to collect this information. Please contact gdpr-info@nyu.edu if you have questions about the legal basis for collecting data and whether subject consent is needed.

In addition, note that processing of personal data relating to criminal convictions and offenses is prohibited under the GDPR unless it is being carried out by a public authority or as authorized under EU or member state law.

What is NYU Doing to Address the GDPR?

NYU has crafted a university-wide, institutional approach to the GDPR which includes a series of privacy notices for staff, faculty, and students in the EU. Information about NYU's approach to the GDPR including links to NYU's notices can be found on the GDPR webpage: www.nyu.edu/it/gdpr.

GDPR impacts a number of activities at NYU has taken a risk-based approach, targeting the areas of greatest exposure: EU based employees, alumni/donors in the EU, prospective students from the EU, and students studying at one of our six EU sites.

NYU also updated its Data Breach Notification Policy to conform to GDPR requirements. NYU must notify EU authorities within 72 hours of a data breach and may also be required to notify affected individuals.

The failure to comply with GDPR could result in significant penalties or legal claims against NYU.

What should I do if somebody wants to exercise their rights under the GDPR, e.g., rights to access, transmission, amendment, or erasure?

You should advise the person to contact the GDPR team at: gdpr-info@nyu.edu

What should I do if there is a breach of personal data?

The GDPR has strict rules regarding reports of data breaches. In some cases, NYU must report potential data breaches to the EU GDPR supervisory authorities within 72 hours of discovery of the incident and may also be required to notify affected individuals. If you discover a breach or a possibility of a breach, *immediately notify* gdpr-info@nyu.edu.

Include the following information:

- Description of the breach, e.g., What happened? How did the data breach occur?
- Description of the personal data, e.g., nature of data, volume/amount of data, number of subjects involved.
- Assessment of risks and consequences to subjects.
- Proposed measures to address breach, including, where appropriate, measures to mitigate possible risks or consequences. These measures should NOT be implemented until further notification from the Data Protection Officer.

What if I have additional questions about GDPR?

Contact: gdpr-info@nyu.edu