CUNY HRPP Guidance: Application of European General Data Protection Regulation (GDPR) to Human Subject Research in Which CUNY is Engaged

I. Purpose and Overview

The General Data Protection Regulation (GDPR) is a European Law that establishes protections for personal data collected about individuals within the European Economic Area (EEA) (EU countries plus Lichtenstein, Iceland and Norway). If you are engaged in a research project that collects or processes any information from individuals located within the EEA, then you should include the GDPR consent supplement provided as an attachment to this Guidance in your research consent forms.

II. Basic principles of the GDPR

The GDPR's goal is to protect individuals with regard to the processing of their personal data by ensuring that it is: processed lawfully, fairly and in a transparent manner; collected for specified, explicit and legitimate purposes; accurate and when necessary kept up to date, kept in a form which permits identification of individuals only for as long as required for the purposes for which it is processed; and processed in a manner that ensures appropriate security.

III. Countries covered by GDPR

GDPR has been adopted in the following countries:

Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom, Norway, Iceland, Lichtenstein.

IV. Type of information covered by GDPR

GDPR broadly defines "Personal data" as any information relating to an identified or identifiable natural person (one who can be identified directly or indirectly), 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.

Examples of personal data include:

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Personal data that has been de-identified, encrypted or pseudonymized but can be used to re-identify a person remains personal data and falls within the scope of the law.

The law protects personal data **regardless of the technology used for processing that data** – it is technology neutral and applies to both automated and manual processing, provided the data is organized in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

V. Anonymized data and de-identified data

Personal data that has been rendered **anonymous** in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymized, the anonymization must be irreversible.

VI. Application of GDPR to research involving data collection and processing

The GDPR applies when information is collected or processed from individuals while they are physically located in an EEA country. It also applies when personal data collected under the GDPR is transferred from an EEA country to a country outside of the EEA.

VII. Lawful processing of special categories of Personal Data

There are special safeguard requirements when research involves the collection or processing of information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Processing of this information is prohibited except when the individual has given explicit consent or under a series of limited exceptions such as:

- Processing is necessary to protect the vital interests of the individual or another where the subject is incapable of giving consent;
- Processing relates to personal data manifestly made public by the individual;
- Processing is necessary for legal claims;
- Processing is necessary for reasons of substantial public interest;
- Processing is necessary for purposes of preventive or occupational medicine and health care or treatment or for reasons of public interest in the area of public health.

NOTE: Additional explicit consent may be required for collection or processing of data involving criminal convictions and offenses.

VIII. Required Language for Informed Consent Forms

See "CUNY HRPP Policy: Required Language for Inclusion in Research Informed Consent Form for Research to which GDPR is Applicable" for language to be included in consent forms. For oral or internet consents, this required language should be included as an appendix to the main consent.

IX. References

European Commission web page on personal data: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en