جامعة نيويورك أبوظبي

NYU | ABU DHABI

Things you need to know about the EU General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).

If a researcher intends to conduct human subjects research in the EU, or will obtain data from a company or institution located in the EU, this regulation will apply. The IRB will work with you to ensure that the protocol is in compliance with this regulation.

What constitutes personal data?

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier (e.g. IP address), reflecting changes in technology and the way organizations collect, transmit and store information about people.

Personal data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g., name and first name, date of birth, biometrics data, fingerprints, DNA, etc.).

Personal data can be data that are not associated with the name of a person but can easily be used to identify him/her and to know his/her habits and tastes. For instance, "the holder of line number 01 53 73 22 00 often makes calls to Senegal", or "the owner of vehicle 3636AB75 subscribes to such and such magazine", or "social security beneficiary 16000530189196 sees the doctor more than once per month".

Who does the GDPR effect?

The GDPR not only applies to organizations located within the EU but it also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the EU, regardless of the company's location.

———

The main changes include (but are not limited to):

Consent: consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and

provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Breach notification: Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Rights to Access: The right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten: The right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability: GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

___

Penalties for Non-Compliance

Organizations found to be in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements, e.g., not having sufficient consent to process data or violating the core of the Privacy by Design concepts.

Content taken from: https://www.eugdpr.org/.

Full text of GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

Please contact the NYUAD IRB at irbnyuad@nyu.edu for further guidance