The European Economic Area General Data Protection Regulation (EEA GDPR) and the United Kingdom General Data Protection Regulation (UK GDPR)

Frequently Asked Questions

I. General

1. *What is the GDPR?*

   There are now two General Data Protection Regulations: in the European Economic Area (the EEA GDPR) and in the United Kingdom (as tailored by the Data Protection Act, the UK GDPR). Both the EEA GDPR and the UK GDPR regulate the collection, use, transfer, storing, and other processing of personal data of persons in their respective jurisdictions.

2. *When did the EEA GDPR and UK GDPR go into effect?*

   The EEA GDPR became effective on May 25, 2018. The UK GDPR became effective on January 1, 2021.

3. *Why did the EU adopt the EEA GDPR?*

   Protecting how personal data is used and otherwise processed is considered a fundamental human right in the EU. It is even included in the Charter of Fundamental Rights of the EU.

4. *To what countries does the EEA GDPR apply? What are the EU and the EEA?*

   The GDPR applies to all 27 member countries of the European Union (EU). It also applies to all countries in the European Economic Area (the EEA). The EEA is an area larger than the EU and includes Iceland, Norway and Liechtenstein.

II. Understanding when the EEA GDPR and UK GDPR apply

1. *When do the EEA GDPR and UK GDPR apply?*

   There are three types of situations that are subject to the EEA GDPR and the UK GDPR:

   A. *If a person is present in the EEA or the UK*, any personal data collected from them in connection with the offering of a good or

service is protected by that area's GDPR, even if the organization offering the good or service is not established in that area. Protection for the personal data continues after the person leaves the EEA or the UK.

B. *Establishments in the EEA or UK.* If personal data is collected or otherwise processed *in the context of the activities of any establishment in the EEA or UK,* then the personal data is protected by that area's GDPR, even if the processing occurs outside the EEA or the UK.

C. *If a person is present in the EEA or UK*, any personal data collected from them in connection with the *monitoring of their behavior* where the behavior takes place within the EEA or the UK.

2. *What are some examples of situations that might be subject to the EEA GDPR or UK GDPR?*

   For persons when they are in the EEA or the UK:

   - Applicants (and their family members)
   - Students, Employees, Faculty, and Consultants
   - Donors, Prospective Donors, Alumni
   - Website visitors
   - Clinical trial subjects

   Programs occurring in the EEA or UK:

   - Study Abroad programs
   - Talloires programs
   - Research, including as human subjects in clinical trials

3. *To which persons does it apply?*

   The EEA GDPR and UK GDPR apply to all persons. There is no requirement that a person be an EEA or UK citizen or an EEA or UK resident.

   There are special protections for children under age 18. For processing of information for online services, the default age of consent is 16.

4. *To what data do they apply?*

   The EEA GDPR and UK apply to all "personal data," which includes any information relating to an identified or identifiable person.

Examples include: Name – SSN – Other identification number – Location data – IP addresses – Online cookies – Images – Email addresses – Content generated by the data subject.

Generally, personal data is protected even if it has been otherwise publicly disclosed.

The EEA GDPR and UK GDPR include more stringent protections for special categories of personal data. These are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health data
- Sex life and sexual orientation
- Genetic and biometric data

The EEA GDPR and UK GDPR also impose limitations on the processing of personal data relating to criminal convictions and offenses.

III. What are the EEA GDPR and UK GDPR's Requirements?

1. *When is collecting, using and otherwise processing personal data permitted under the EEA GDPR and UK GDPR?*

   There must be a documented, *lawful basis* for collecting, using or otherwise processing any personal data. Generally, there are three options for a lawful basis: consent, necessity for a legitimate interest, and in connection with a contract. The lawful basis must be selected and documented before the information is first collected. If the initial lawful basis becomes unavailable after the information is collected, the holder of the information cannot rely on a new lawful basis.

   A. *Consent.* In the US, it is common practice to rely on consents given by an individual. In the EEA and UK, on the other hand, consent is treated differently and is often not considered effective. The EEA GDPR and UK GDPR impose several significant restrictions on consent. Therefore, Tufts' approach is often to leverage either the legitimate interest or the contract legal basis for our GDPR activities whenever possible.

      To rely on consent under the EEA GDPR or UK GDPR, consent must be freely and actively given, without any imbalance of power

between the giver of the consent and the recipient. For example, a consent by an employee to an employer will often be considered compelled and therefore not effective. Generally, there cannot be any penalty for withholding consent, such as a denial of access to a service.

If consent is selected as the lawful basis for collecting personal information, the consent will need to be accompanied by a clear statement of the intended use of the information. That original scope of use cannot be expanded later.

Under the EEA GDPR and UK GDPR, some consents may need to be regularly renewed. In most cases, a person giving consent may withdraw the consent at any time with respect to future activities.

B. *Necessary for a legitimate interest* is a broader basis for use, and covers many activities in the standard course of business, such as direct marketing, human resources purposes, research, and nonprofit fundraising.

Compliance with US law is generally not considered to be a legitimate interest.

What constitutes a legitimate interest is strictly construed, and it must be a lawful, real, and present need, balanced against the privacy rights of the subject. The balancing analysis must be documented.

C. *In connection with a contract* applies when the processing is necessary for the performance of a contract with the data subject, or where necessary to take steps the data subject requests prior to entering into the contract. Necessity is construed narrowly.

This basis may also apply to uses necessary for providing a service; this basis might apply for arranging for study abroad and processing applications for admission or employment.

2. *What do the EEA GDPR and UK GDPR require for handling and other processing of the information?*

All processing of personal data must be documented from collection through destruction. Data should only be kept while it is needed and promptly securely disposed of when it is not.

The amount of data collected must be minimized. Whenever possible, data should be collected in a manner that is not subject to the EEA GDPR and UK GDPR to reduce the administrative work required.

Data should not be shared with any person unless the person has a need for the information and that need is consistent with the lawful basis initially established.

The EEA GDPR and UK GDPR impose additional requirements for ensuring the data is protected. Data is to be collected, used, stored and otherwise processed in a manner that takes into account state of the art security practices.

3. *Do we have to meet any requirements when we use a vendor?*

   Yes. All vendors that process personal data subject to the EEA GDPR or UK GDPR will be obligated to comply with the regulation. Contracts with these vendors will need to include new provisions that address the regulation's requirements.

4. *What rights will data subjects have?*

   - Transparency: the right to be told what data is being collected, who will have access to it, and what will be done with it.
   - Access and review: the right to be given access to, and to review, their personal data upon request.
   - Rectification: the right to have any inaccuracies in their personal data corrected.
   - Erasure, right to be forgotten: the right in many situations, to require that an organization delete all of their personal data.

IV. How are the EEA GDPR and UK GDPR enforced?

Reports of unauthorized use or disclosure of personal data are required to be made within 72 hours.

The maximum fine for breach under the EEA GDPR is the larger of €20,000,000 or 4% of an organization's worldwide annual "turnover," or revenue. The UK GDPR also provides for substantial fines. Both the EEA GDPR and UK GDPR also provide a private right of action for individuals.

V. Who can I contact with questions?

Questions can be sent to Tufts' Data Privacy Team at dataprivacy@tufts.edu.