European Union - Data Privacy and Protection
The GDPR) governs how personal data of individuals in the EU may be processed and transferred.

European Union - Data Privacy and Protection

European Union - Data Privacy and Protection

The EU General Data Protection Regulation (GDPR), which governs how personal data of individuals in the EU may be processed and transferred, went into effect on May 25, 2018. GDPR is a comprehensive privacy legislation that applies across sectors and to companies of all sizes. It replaces the Data Protection Directive 1995/46. The overall objectives of the measures are the same – laying down the rules for the protection of personal data and for the movement of data.

Note, see Commerce's July 16, 2020 press release on the Schrems II Ruling and Importance of EU-U.S. data Flows. According to the release, "The Department of Commerce will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List."

Key Provisions:

GDPR is broad in scope and uses broad definitions. "Personal data" is any information that relates to an identified or identifiable living individual (data subject) such as a name, email address, tax ID number, online identifier, etc. "Processing" data includes actions such as collecting, recording, storing and transferring data.

A company that is not established in the Union may have to comply with the Regulation when processing personal data of EU and EEA residents (EEA countries are Norway, Lichtenstein and Switzerland):

a) If the company offers goods or services to data subjects in the EU; or,
b) If the company is monitoring data subjects' behavior taking place within the EU.

The mere accessibility of a company's website in the EU is insufficient to subject a company to GDPR, but other evidence of the intent to offer goods or services in the EU would be relevant.

As a general rule, companies that are not established in the EU but that are subject to GDPR must designate in writing an EU representative for purposes of GDPR compliance. There is an exception to this requirement for small scale, occasional processing of non-sensitive data.

Fines in case of non-compliance can reach up to 4% of the annual worldwide revenue or 20 million euros – whichever is higher. Companies of all sizes and sectors should consider GDPR as part of their overall compliance effort with assistance of legal counsel.

The European Commission and Data Protection Authorities are releasing official guidelines to help companies with their compliance process. These documents relate, for instance, to the role of the data protection officer, personal data breach notification, data protection impact assessment.

Note: the EU is currently updating its e-privacy legislation governing confidentiality of communications. This legislative instrument once enacted will add several requirements in addition to the GDPR. We encourage U.S. exporters to monitor this situation as it evolves through the EU legislative process.

For More Information:

Full GDP Text
Official Press Release

European Commission guidance:

- https://ec.europa.eu/info/law/law-topic/data-protection_en

- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://edpb.europa.eu/edpb_en
  https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

Transferring Customer Data to Countries Outside the EU

The General Data Protection Regulation (GDPR) provides for the free flow of personal data within the EU but also for its protection when it leaves the region's borders.

- GDPR sets out obligations on data controllers (those in charge of deciding what personal data is collected and how/why it is processed), on data processors (those who act on behalf of the controller) and gives rights to data subjects (the individuals to whom the data relates).

- These (above) rules were designed to provide a high level of privacy protection for personal data and were complemented by measures to ensure the protection is maintained when data leaves the region, whether it is transferred to controllers, processors or to third parties (e.g. subcontractors).
- EU legislators put restrictions on transfers of personal data outside of the EU, specifying that such data could only be exported if "adequate protection" is provided.

The European Commission (EC) is responsible for assessing whether a country outside the EU has a legal framework that provides enough protection for it to issue an "adequacy finding" to that country. The U.S. has never sought to be found adequate by the EC. This means that U.S. companies can only receive personal data from the EU if they:

- Join the EU-U.S. Privacy Shield program, or
- Provide appropriate safeguards (e.g. standard contractual clauses, binding corporate rules), or,
- Refer to one of the GDPR's derogations.

For more information, consult the European Commission's webpage on data transfers outside the EU.

Important note: The legal environment for data transfers to the United States continues to evolve. Companies that transfer EU citizen data to the United States as part of a commercial transaction should consult with an attorney, who specializes in EU data privacy law, to determine what options may be available for a transaction.

About the EU-U.S. Privacy Shield

The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

EU-U.S. Privacy Shield

For more information about other mechanisms of transfer, please refer to:
https://www.export.gov/article?id=European-Union-Transferring-Personal-Data-From-the-EU-to-the-US
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en