The **General Data Protection Regulation** [(EU) 2016/679](https://eur-lex.europa.eu/eli/reg/2016/679/oj) ("GDPR") is a [regulation](https://en.wikipedia.org/wiki/Regulation_(European_Union)) in [EU law](https://en.wikipedia.org/wiki/EU_law) on [data protection](https://en.wikipedia.org/wiki/Data_protection) and privacy for all individuals within the [European Union](https://en.wikipedia.org/wiki/European_Union) (EU) and the [European Economic Area](https://en.wikipedia.org/wiki/European_Economic_Area) (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for [international business](https://en.wikipedia.org/wiki/International_business) by unifying the regulation within the EU.[[1]](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#cite_note-1) Superseding the [Data Protection Directive](https://en.wikipedia.org/wiki/Data_Protection_Directive) 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of [personal data](https://en.wikipedia.org/wiki/Personal_data) of individuals (formally called *data subjects* in the GDPR) inside the EEA, and applies to an enterprise established in the EEA or—regardless of its location and the data subjects' citizenship—that is processing the personal information of data subjects inside the EEA.

Controllers of personal data must put in place *appropriate technical and organisational measures* to implement the data protection principles. Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data (for example, using [pseudonymization](https://en.wikipedia.org/wiki/Pseudonymization" \o "Pseudonymization) or full [anonymization](https://en.wikipedia.org/wiki/Data_anonymization" \o "Data anonymization) where appropriate), and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit, informed [consent](https://en.wikipedia.org/wiki/Consent), and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it is done under a lawful basis specified by the regulation, or unless the data controller or processor has received an unambiguous and individualized affirmation of consent from the data subject. The data subject has the right to revoke this consent at any time.

A processor of personal data must clearly disclose any [data collection](https://en.wikipedia.org/wiki/Data_collection), declare the lawful basis and purpose for data processing, and state how long data is being retained and if it is being shared with any third parties or outside of the EEA. Data subjects have the right to request a [portable](https://en.wikipedia.org/wiki/Data_portability) copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances. Public authorities, and businesses whose core activities centre around regular or systematic processing of personal data, are required to employ a *data protection officer* (DPO), who is responsible for managing compliance with the GDPR. Businesses must report any [data breaches](https://en.wikipedia.org/wiki/Data_breach) within 72 hours if they have an adverse effect on user privacy. In some cases, violators of the GDPR may be fined up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

The GDPR was adopted on 14 April 2016, and became enforceable beginning 25 May 2018. As the GDPR is a regulation, not a [directive](https://en.wikipedia.org/wiki/Directive_(European_Union)), it is directly binding and applicable.

In November 2018, Google was accused of GDPR privacy violations by 7 countries.[[](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#cite_note-2)