

Fines of up to 4% of annual global revenue or €20 million, whichever is greater



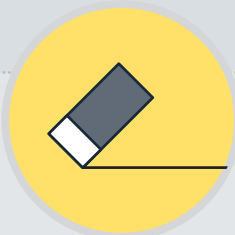
The regulation applies to **non-EU companies** that process personal data of individuals in the EU. The **international transfer of data** will continue to be governed under EU GDPR rules.



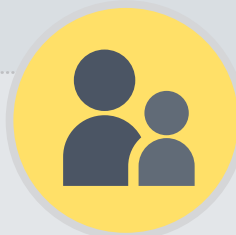
The **definition of personal data** is now broader and includes such identifiers as genetic, mental, cultural, economic, and social identity



Obtaining consent for processing personal data must be clear and must seek an affirmative response



Data subjects have the **right to be forgotten** and erased from records



Parental consent is required for processing of **personal data of children** under age 16



Users may request a copy of personal **data held by companies in a portable format**



Controllers must **report a data breach** no later than 72 hours after becoming aware of the breach, unless the breach has a low risk to the individual's rights



The appointment of a **data protection officer (DPO)** will be mandatory for companies processing high volumes of personal data and good practice for others



Privacy risk assessment will be required for projects where privacy risks are high



Products, systems and processes must consider **privacy-by-design** concepts during development



Data controllers must ensure adequate contracts are in place to **govern data processors**



Data processors can be held **directly liable** for the security of personal data



Controllers must have a **legal basis for processing** and collecting data



One stop shop: international companies will only have to deal with one supervisory data protection authority

YOU HAVE TO COMPLY WITH EU GDPR BY MAY 2018