



News

EU Boosts Cyber Defenses With Stricter Security Rules

The regulations are the latest in a series of efforts by the EU to strengthen cybersecurity across its 27 member states

The European Union approved a [new set of cybersecurity standards](#) this week aimed at better protecting sensitive data and critical infrastructure across the bloc. The rules, which will take effect next year, mandate increased digital defenses for government agencies, companies that supply critical infrastructure like energy grids, and "essential services" such as hospitals and transportation networks.

"Cybersecurity is a political and operational priority for the EU, and this Regulation is a milestone in this respect. More cooperation, certainty and efficiency will create a climate of collaboration and trust where people, data and networks can operate and interact safely" said Johannes Hahn, Commissioner for Budget and Administration on behalf of the [EU Commission](#).

The regulations require government entities and companies in critical sectors to conduct regular risk assessments, implement safeguards like multi-factor authentication, and report major cyber incidents within 24 hours. Firms that fail to comply could face fines of up to 10 million euros or 2% of global revenue, whichever is higher.

The bloc has taken an increasingly active role in cyber policy in recent years amid a rise in attacks on governments and infrastructure worldwide. The new rules aim to close security gaps, reduce vulnerabilities, and improve coordination in the event of major incidents. They will apply to an estimated 10,000 public and private entities across the EU.

Read more:

[The EU Cybersecurity Act](#)
[Cybersecurity Policies](#)

--

Ramin Aryaie: cc by-nc-sa

