Cisco Webex

Security always matters.

GDPR and why security always matters

The European Union's (EU's) General Data Protection Regulation (GDPR) foresees severe financial penalties for data breaches and mishandling of personal data—because security always matters. It's vitally important to know the latest regulations and mandates and how they may impact you. The following list of important issues will help keep you safer out there.

GDPR applies to companies beyond the EU.

GDPR applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. Non-EU businesses processing the data of EU citizens are also subject to GDPR and must appoint a representative in the EU.

Under GDPR, breach notifications are mandatory.

Breach notifications to the appropriate supervisory authority are mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals." Notifications must be submitted within 72 hours of first awareness.

Data subjects can have their personal data erased.

The right to be forgotten entitles data subjects to have the data controller erase his or her personal data, cease further dissemination of the data, and potentially require third parties to halt processing of the data.

Data protection is required from the onset of designing systems.

Privacy by design calls for the inclusion of data protection measures from the **onset** of the designing of systems. Controllers must hold and process only the data necessary for the completion of their duties and limit access to personal data to those needing to carry out the processing.

There is a tiered approach to GDPR fines.

A company can be fined as much as 2 percent for not having its records in order, for not notifying the supervising authority and data subject about a breach, and for not conducting impact assessment. "Clouds" are not exempt from GDPR enforcement, among other events.

Source: https://eugdpr.org/the-regulation/

IP phone calls that are not properly secured can expose an individual's personal data, including:

- The content of the voice conversation
- Identification of the entities involved in the call, including phone numbers and URLs
- Call history, including frequency and duration of calls
- Missed calls and transfers

What's next

The collaboration environment, including software, voice endpoints, and video endpoints, should be updated to support Transport Layer Security 1.2 (TLS 1.2) protocol.

Violations on certain articles of GDPR can carry fines of up to 20 million euros or as much as 4 percent of an organization's total global revenue for the preceding year.

Learn more to find out if this regulation could be impacting your business.

cisco.com/go/voipcompliance