TrustArc

EU Cloud Code of Conduct

Frequently Asked Questions

What is the scope of the EU Cloud Code of Conduct?

The EU Cloud Code of Conduct is a self-regulation instrument that makes it easier to demonstrate compliance with the EU GDPR. It translates the legal requirements of the Regulation into operational controls that organisations can implement. The Code covers all aspects of the GDPR, from individual rights to data security, and also includes a governance section that is designed to support the effective and transparent implementation, management, and evolution of the Code.

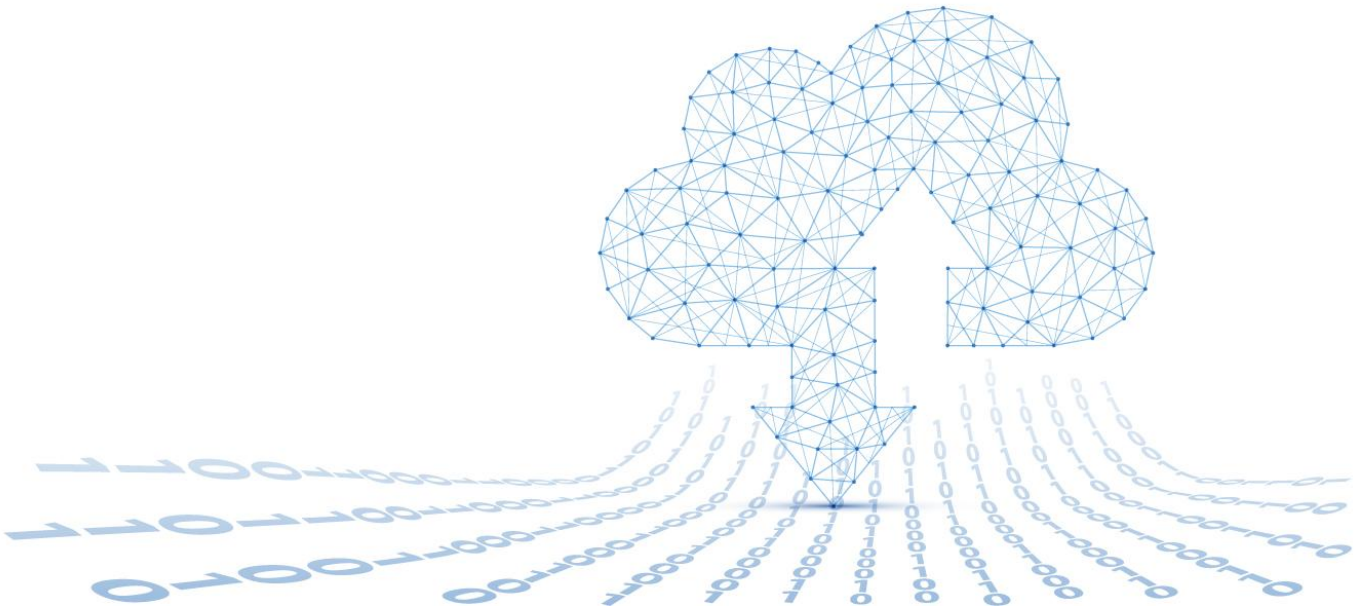
The intention of the EU Cloud Code of Conduct is to make it easier for cloud customers (particularly small and medium enterprises and public entities) to determine whether certain cloud services are appropriate for their designated purpose. In addition, the transparency created by the Code will contribute to an environment of trust and create a high default level of data protection in the European cloud computing market.

Who does the EU Cloud Code of Conduct apply to?

The Code applies to all Cloud Service Providers (CSPs) that have completed a declaration of adherence to the Code of Conduct, and have submitted themselves to the oversight of an independent monitoring body. It covers the full spectrum of cloud services: software (SaaS) and platform (PaaS) as well as infrastructure (IaaS).

What does this mean for international data transfers?

Nothing at this time. The Code has not yet been approved as an instrument to facilitate international transfers. However, the General Assembly of the EU Cloud Code of Conduct has tasked a working group with the creation of a so-called third country module, that could create the legal basis for international transfers from the EU to a non-EU CSP. The third country module will be drafted in such a way that it meets the 'essential equivalence' test as explained by the Court of Justice of the European Union in the Schrems-II decision. That means it will also include an overview of so-called supplementary measures that can be adopted to make up for a lack of legislative safeguards in a third country of destination. Given that these supplementary measures are subject to approval by the European Data Protection Board, once approved the third country module will become a safe way to transfer personal data from the EU. TrustArc is a member of the working group preparing this module.



What companies are adherent to the EU Cloud Code of Conduct?

The full overview of companies currently adhering to the Code is available in a public register. TrustArc is in the process of finalising its declaration of adherence and will be added to the register in the coming weeks.

What are the benefits to adherence?

Adherence to the Code shows that organisations take the implementation of a privacy and security management programme seriously. It provides for an independent verification of the controls put in place that should offer trust to organisations doing business with a certain CSP. In addition, organisations can rely on the fact that the data practices of a CSP will be monitored on an ongoing basis.

How is adherence demonstrated?

For every control, the CSP will need to demonstrate how they have implemented the requirements within their organisation and/or cloud service. The required evidence, which could for example include all kinds of policies and procedures in use in the organisation, should be submitted to the monitoring body for review. The monitoring body will assess the information provided by each CSP. For each service that is being declared adherent, the monitoring body will confirm that the information provided is complete and relevant. It will also request additional documentation and samples which underpin the effective implementation of the measures mentioned within the explanation.

Once the initial assessment is successfully completed and adherence to the Code is confirmed, subsequent assessments will take place on an annual basis, as well as ad hoc, should there be a complaint, a suspicion of non-compliance or if the cloud service itself changes.

EU Cloud Code of Conduct in the TrustArc Platform

PrivacyCentral now offers additional guidance to its users specific to the EU Cloud Code of Conduct, and will soon offer a validation program for organizations that need support in demonstrating compliance with the EU Cloud Code of Conduct before submitting adherence to SCOPE Europe, its monitoring body.

The EU Cloud Code of Conduct PrivacyCentral solution incorporates the controls catalogue developed as part of the Code as well as alignment with ISO 27001, GDPR, UK GDPR, APEC CBPRs and PRPs, the TrustArc Privacy and Data Governance Framework, Nymity Privacy Management Accountability Framework, CCPA, LGPD, and HIPAA so that organizations can leverage the standards they already have in place to demonstrate their adherence to the Code. To learn more, visit www.trustarc.com/privacycentral.