UpCloud

# Maintaining Cloud Compliance

## Best Practices

1 **Define compliance requirements internally** □

Organisations should establish clear compliance requirements based on industry regulations, legal obligations, and internal policies. This ensures a structured approach to maintaining security and regulatory adherence in the cloud.

2 **Choose a cloud service provider that aligns with your cloud compliance requirements** □

Organisations should evaluate CSPs based on their certifications, security controls, and ability to support regulatory requirements relevant to their industry.

3 **Data residency awareness** □

Understanding applicable data residency requirements is crucial when selecting cloud regions to ensure compliance with the data transfer restrictions imposed by data protection laws or your customer requirements. While most CSPs offer European cloud regions, it's important to ensure the whole supply chain, including possible sub-processors, comply with your data residency requirements.

4 **Regularly update policies and procedures** □

Cloud compliance is an ongoing process, not a one-time task. Organisations should frequently review and update their policies and procedures to reflect new regulatory changes, emerging threats, and evolving business needs.

5 **Work closely with cloud service providers** □

Building a strong relationship with the CSP ensures better communication and collaboration. Organisations should engage with their CSPs to stay informed about security updates, compliance practices, and shared responsibility expectations.

6 **Implement strong access controls** □

Because compliance involves data security, your organisation should set appropriate access controls, apply the principle of least privilege, enforce strong password policies, and implement multi-factor authentication to enhance user security and prevent unauthorised access.

7 **Encryption** □

By encrypting data at rest and in transit, your business can significantly reduce the risk of unauthorised access and data breaches.