Vultr DORA Compliance Customer Trust Statement

Date: July 18, 2025

In support of Vultr's commitment to its customers, BDO assessed Vultr's alignment with the European Union's Digital Operational Resilience Act (DORA). Our assessment reviewed Vultr's controls, resilience plans, incident management protocols, and governance structure to ascertain compliance with the Information Communication and Technology (ICT) provider requirements set out in DORA.

Assessment Approach

BDO's assessment utilized a unified control framework, mapping each DORA article to Vultr's existing ISO 27001 certification and SOC 2 Trust Services Criteria (Security, Confidentiality, and Availability). Our methodology included a review of Vultr's policy framework, resilience and response plans, incident notification protocols, operational resilience testing, and third-party risk management practices. This was further supported by interviews with key control owners to provide insight into current practices.

Vultr's Commitment to DORA Compliance

Vultr maintains a central control framework to address the DORA requirements of critical ICT providers, leveraging standards such as ISO 27001 and the SOC 2 Trust Services Criteria. This approach enables Vultr to maintain services that are secure, reliable, and compliant with regulatory expectations.

Key Elements of Vultr's DORA Compliance

- **Integrated Controls and Governance:** Vultr maintains a unified controls environment that streamlines the adoption of new regulatory requirements and supports ongoing compliance with DORA and other international standards.
- **Operational Resilience**: Vultr maintains central business continuity and incident response plans with periodic exercising and operational resilience testing.
- **Incident Management:** Vultr incident escalation, notification, and reporting protocols are defined to meet DORA expectations and timelines.
- **Third-Party Risk Management:** Vultr conducts ongoing third-party risk assessments for ICT providers directly and indirectly involved in the delivery, security, and uptime of its products and services.

Applicability of ISO 27001 and SOC 2 Controls

Vultr's ISO 27001 certification and SOC 2 attestation provide independent assurance of its information security, confidentiality, and availability controls. These frameworks support Vultr's alignment with DORA ICT requirements in several key areas:

- **Incident Response and Reporting:** Vultr's incident response program is designed to detect, escalate, and address cybersecurity threats. Documented procedures and communication protocols ensure incidents are managed promptly and reported to relevant stakeholders.
- **Third-Party Oversight:** Vultr maintains an inventory of third-party partners and subprocessors. Risk assessments are conducted based on data sensitivity and service criticality.
- **ICT Risk Management:** Vultr regularly identifies, assesses, and mitigates ICT-related risks. Controls and monitoring are in place to address evolving threats, supporting DORA's expectations for proactive risk management.
- **Operational Resilience:** Business continuity and disaster recovery plans are established and tested.
- **Governance and Accountability:** Governance structures define roles and responsibilities for ICT risk management and oversight.

Continuous Improvement and Customer Assurance

Vultr is committed to continuous enhancement of its controls and resilience capabilities. Ongoing initiatives include refining business impact analysis, expanding technical resilience testing of critical IT assets, and strengthening resilience planning with scenario-specific strategies and plans.

Assurance for Vultr Customers

BDO's independent assessment indicates Vultr's risk and resilience capabilities are designed to align with DORA and financial sector expectations. Vultr's ongoing investments and focus on transparency and improvement support its ability to deliver secure, reliable, and compliant services.

For additional information regarding BDO's assessment or Vultr's DORA compliance, please contact grc@vultr.com.