

The background of the page features a large, stylized red 'V' logo, which is the Vodafone brand mark. This logo is centered and surrounded by a series of concentric red circles of varying line weights, creating a ripple effect. The text is positioned in the center of the page, overlaid on the logo and circles.

# **Vodafone Supplier Policy – S1**

## **Payment Card Industry (PCI)**

### **Compliance**



## Scope

All Vodafone Procurement Company procurement agreements with Suppliers.

## Policy

### 1. Introduction

- 1.1. This VPC Supplier Policy on PCI Compliance:
  - (i) sets out Supplier's obligations for data security for account data; and
  - (ii) is additional to Supplier's obligations in relation to data processing and minimum security requirements.
- 1.2. In this VPC Supplier Policy on PCI Compliance:
  - (i) all obligations on Supplier shall be interpreted as being obligations not just on Supplier, but obligations on Supplier to procure compliance with the same obligations by its sub-contractors and agents;
  - (ii) where Supplier is under an obligation it shall bear all of the costs of compliance with the obligation; and
  - (iii) where Supplier has an obligation to provide information then it shall do so as soon as reasonably practicable.
- 1.3. You All references to "Vodafone" include the relevant contracting entity and all other Vodafone Group Companies that benefit from the goods and services being provided.

### 2. Definitions

- 2.1. In this VPC Supplier Policy on PCI Compliance and in its application, the followings words and expressions shall have the following meanings:

**"Account Data"** means Account data consists of cardholder data and/or sensitive authentication data. See Cardholder Data and Sensitive Authentication Data;

**"ASV"** means Approved Scanning Vendor (ASV), being a Company approved by the PCI SSC to conduct external vulnerability scanning services;

**"Attestation of Compliance (AOC)"** means a Statement of PCI compliance as completed by a Supplier in conjunction with either

  - (i) an ROC; or
  - (ii) an SelfAssessment Questionnaire (SAQ);

**"Cardholder Data (CHD)"** means, at a minimum, cardholder data consists of the full Primary Account Number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See Sensitive Authentication Data for additional data elements that might be transmitted or processed (but not stored) as part of a payment transaction.

**"Matrix of Responsibilities"** means a documented matrix which identifies which PCI DSS requirements and sub-requirements are the responsibility of the Supplier, which are the



responsibility of Vodafone, or if any responsibilities are shared between the Supplier and Vodafone;

**“PCI Standards”** means the standards published by the PCI Security Standards Council (PCI SSC) which covers the security of systems and networks that store, process, or transmit account data. (a list of such standards and guidance being available at <http://www.pcisecuritystandards.org>);

**“RoC”** means a Report on Compliance, being a detailed report containing information documenting an entity’s compliance status with the PCI Standards;

**“QSA”** means a Qualified Security Assessor. QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments.

**“SAQ”** means a Self-Assessment Questionnaire;

**“Service Provider Level”** means the appropriate accreditation level of a Supplier as defined by the PCI SSC who carries out the processing, storage, or transmission of account data.

**“Sensitive Authentication Data (SAD)”** means security-related information used to authenticate cardholders and/or authorize payment card transactions. This information includes, but is not limited to, card validation verification codes/values, full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks.

### **3. PCI Data Security**

#### **3.1. In this Supplier shall:**

- (i) handle and store account data in accordance with this VPC Supplier Policy on PCI Compliance;
- (ii) facilitate payment card transactions for no purpose other than those expressly agreed in writing by Vodafone;
- (iii) comply with the most current versions of the Payment Card Industry (PCI) Standards available from time to time at <http://www.pcisecuritystandards.org/>;
- (iv) ensure that its payment systems, networks, applications and payment transaction devices are compliant with the applicable PCI Standards;
- (v) not store any Sensitive Authentication Data (SAD) within their environment;
- (vi) comply with applicable PCI DSS requirements where their service or product could impact on the security of a Vodafone cardholder data environment.

#### **3.2. In the event that the Payment Card Industry (PCI) Standards provide for choices or alternatives as to compliance then Supplier shall comply with all reasonable requests made by Vodafone as to these choices or alternatives.**



#### **4. PCI Compliance Artefacts**

- 4.1. Supplier shall provide Vodafone with full copies of the following artefacts required under PCI (depending upon the appointed Service Provider Level):
  - 1) Annual Report on Compliance (ROC)
  - 2) Annual Attestation of Compliance (AOC)
  - 3) Annual Self-Assessment Questionnaire (which has been counter-signed by a QSA)
  - 4) Quarterly ASV (Approved Scanning Vendor) Network Scan
- 4.2. Supplier shall provide Vodafone with written information detailing all applicable PCI DSS requirements, to the extent the supplier handles, has access to, or otherwise stores, processes or transmits the Vodafone's cardholder data or sensitive authentication data, or manages the Vodafone's cardholder data environment. This shall be provided as a documented Matrix of Responsibilities on an annual basis or if the supplier's responsibilities change.
- 4.3. Vodafone shall have the right to perform a due diligence audit on the Supplier to validate the results of each of the above artefacts.
- 4.4. The supplier may be required to proactively participate in the following PCI activities :
  - Risk management workshops / activities
  - Incident management workshops / activities and annual testing of Vodafone's Incident response plan.
  - Cardholder data flow workshops to facilitate an end-to-end representation of the relevant solution/service for both Vodafone and Vodafone customers.

#### **5. Account Data Breach**

- 5.1. Supplier shall notify Vodafone in writing as soon as reasonably possible if it know or suspects that account data has been breached or used:
  - (i) without authorisation; or
  - (ii) contrary to its contractual arrangements with Vodafone including this VPC Supplier Policy on PCI Compliance. These matters are referred to in this VPC Supplier Policy on PCI Compliance as "**Incidents**".
- 5.2. In relation to each Incident, Supplier shall:
  - (i) provide, in a secure manner, to Vodafone, all relevant account data numbers;
  - (ii) undertake its own audit in relation to the Incident and ensure that such audit identifies the root cause of the Incident and confirms whether or not Supplier was in compliance with the PCI Standards at the time of the Incident;
  - (iii) provide to Vodafone copies of all relevant audit and other similar reports in relation to the Incident;
  - (iv) be responsible for and pay all reasonable costs associated with the engagement of forensic investigation services by Vodafone in accordance with the relevant Payment Card Industry and Vodafone's own forensic procedures;



- (v) provide Vodafone and its forensic investigators and auditors such waivers as are necessary to facilitate such forensic investigation services; and
- (vi) provide full cooperation and access to enable such forensic investigation services.

**5.3. Supplier shall:**

- (i) rectify all issues arising from an Incident;
- (ii) consult with Vodafone about Vodafone's communications to card holders affected by the Incident;
- (iii) provide to Vodafone all relevant information (and associated waivers) to verify Supplier's ability to prevent future data incidents in a manner consistent its contractual arrangements with Vodafone including this VPC Supplier Policy on PCI Compliance; and
- (iv) compensate Vodafone for any losses incurred by Vodafone arising from fraudulent transactions, to the extent that such transactions result from Supplier's non-compliance its contractual arrangements with Vodafone including this VPC Supplier Policy on PCI Compliance.

**6. Termination**

- 6.1.** Following termination of the relevant contractual arrangement with Vodafone, Supplier shall securely dispose of any account data in its possession in accordance with any reasonable request by Vodafone.