



Vodafone Procurement Company S.à r.l.

Supplier Policy - S1

Payment Card Industry Compliance

Version Number	Date	Vodafone Point of contact	Email
1.0	06.09.13	Charles Husbands	charles.husbands@vodafone.com

Scope

All Vodafone Procurement Company procurement agreements with Suppliers that involve payment cards.

Policy

1. Introduction

- 1.1 This VPC Supplier Policy on PCI Compliance: (i) sets out Supplier's obligations for data security for cardholder 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 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:

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

"Attestation of Compliance" means a Statement of PCI compliance as completed by a Supplier in conjunction with either (i) an ROC; or (ii) an

SAQ;

“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 cardholder 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;
“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 cardholder data.

3. PCI Data Security

- 3.1 Supplier shall: (i) handle and store cardholder 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.
- 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
 - 2) Annual Self-Assessment Questionnaire
 - 3) Attestation of Compliance
 - 4) Quarterly ASV Network Scan
- 4.2 Vodafone shall have the right to perform a due diligence audit on Supplier to validate the results of each of the above artefacts.

5. Cardholder Data Breach

- 5.1 Supplier shall notify Vodafone in writing as soon as reasonably possible if it know or suspects that cardholder 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 cardholder account 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 cardholder data in its possession in accordance with any reasonable request by Vodafone.