Security Standards Council®

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D – Service Providers

For use with PCI DSS Version 3.2

Revision 1.1
January 2017

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the service provider's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	Sysdat Turismo Srl		DBA (doing business as):	Sysdat Turismo Srl	
Contact Name:	Gandola Luca		Title:	Manager	
Telephone:	+39 02967181		E-mail:	gandola.luca@sigesgroup.it	
Business Address:	Via G. Ferrari 21c		City:	Saronno	
State/Province:	Varese	Country:	Italy	Zip:	21047
URL:	www.sysdat-turismo.it				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	SysHotel On Line Booking Engine & Channel Manager

Type of service(s) assessed:

Hosting Provider:

□ Applications / software
□ Hardware
□ Infrastructure / Network
□ Physical space (co-location)
□ Storage
□ Web
□ Security services
□ 3-D Secure Hosting Provider
□ Shared Hosting Provider
□ Other Hosting (specify):

Managed Services (specify):

□ Systems security services
□ IT support
□ Physical security
□ Terminal Management System
□ Other services (specify):

Payment Processing:

□ POS / card present
☒ Internet / e-commerce
□ MOTO / Call Center
□ ATM
□ Other processing (specify):

□ Account Management	□ Fraud and Chargeback	□ Payment Gateway/Switch
☒ Back-Office Services	□ Issuer Processing	□ Prepaid Services
□ Billing Management	□ Loyalty Programs	□ Records Management
□ Clearing and Settlement	□ Merchant Services	□ Tax/Government Payments
□ Network Provider		
□ Others (specify):		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others."*

If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) not assessed:	Software development; managed services for hotels

Type of service(s) not assessed:

Hosting Provider:

- □ Applications / software
- □ Hardware
- □ Infrastructure / Network
- □ Physical space (co-location)
- □ Storage
- □ Web
- □ Security services
- □ 3-D Secure Hosting Provider
- □ Shared Hosting Provider
- □ Other Hosting (specify):

Managed Services (specify):

- □ Systems security services
- ☒ IT support
- □ Physical security
- □ Terminal Management System
- □ Other services (specify):

Payment Processing:

- □ POS / card present
- □ Internet / e-commerce
- □ MOTO / Call Center
- □ ATM
- □ Other processing (specify):

□ Account Management	□ Fraud and Chargeback	□ Payment Gateway/Switch
☒ Back-Office Services	□ Issuer Processing	□ Prepaid Services
☒ Billing Management	□ Loyalty Programs	□ Records Management
□ Clearing and Settlement	□ Merchant Services	□ Tax/Government Payments
□ Network Provider		
☒ Others (specify): Software development; education & training		

Provide a brief explanation why any checked services were not included in the assessment:	These services aren't related to credit cards payment processing

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Sysdat Turismo stores the CHD on behalf of the hotels. Sysdat Turismo receives the data when a customer makes an hotel reservation and it maintains them on its systems until the customer's check-out. Sysdat Turismo never do credit card transaction. It archives the data and makes them available to the hotels. Sysdat Turismo estimates to store less than 300.000 credit card numbers per year.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Sysdat Turismo can impact the security of CHD because it receives, stores and transmits them to the hotels.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Example: Retail outlets	*3*	*Boston, MA, USA*

Corporate office	1	Saronno, VA, Italy
Data center	2	Milano, Italy

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? □ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment.

For example:

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

The CDE components are:

- a firewall provided by the ISP,

- 2 application servers,

- 2 database and backup systems in the internal network.

The internal network is a dedicated network, segmented from the office network, hosted by the ISP.

Sysdat Turismo receives the CHD from the hotels using a secure protocol during the reservation process. It stores the CHD on its database in a secure manner. The hotels can access the information in the database using a secure protocol and only after passing a two-level authentication process. When the CDE needs some maintenance, the Sysdat technicians connect it in a secure way and do their tasks.

Does your business use network segmentation to affect the scope of your PCI DSS environment?

(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

☒ Yes □ No

Part 2f. Third-Party Service Providers	
Does your company have a relationship with a Qualified Integrator Reseller (QIR) for the purpose of the services being validated? If Yes: Name of QIR Company: QIR Individual Name: Description of services provided by QIR:	☐ Yes ☒ No

Part 2f. Third-Party Service Providers (Continued)	
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No

If Yes:

Name of service provider:	Description of services provided:
KPNQwest	KPNQwest is the service provider hosting the internal network. It provides the facilities (secure building, electricity, internet connection) hosting the Sysdat network.

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- Full – The requirement and all sub-requirements were assessed for that Requirement, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the SAQ.
- Partial – One or more sub-requirements of that Requirement were marked as "Not Tested" or "Not Applicable" in the SAQ.
- None – All sub-requirements of that Requirement were marked as "Not Tested" and/or "Not Applicable" in the SAQ.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the SAQ
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Name of Service Assessed:	SysHotel On Line Booking Engine & Channel Manager

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	□	☒	□	**1.2.2: N.A because there are no routers in CDE** **1.2.3: N.A. because Wi-fi networks aren't in use** **1.4.a, 1.4.b: N.A. because there are a few number of dedicated station to access the CDE. These stations are hosted on a dedicated network and can't moved outside**
Requirement 2:	□	☒	□	**2.1.1.a, 2.1.1.b, 2.1.1.c, 2.1.1.d, 2.1.1.e: N.A. because Wi-fi networks aren't in use** **2.2.3, 2.2.3.a, 2.3.e: N.A. because un-secure protocols are not in use** **2.6: N.A. because Sysdat Turismo is not a shared hosting provider**
Requirement 3:	□	☒	□	**3.2.a, 3.2.b: N.A. because Sysdat Turismo is not an issuer** **3.2.c: N.A. because Sysdat Turismo doesn't make payment transaction, it only stores CHD on behalf of its customers** **3.2.1: N.A. because Sysdat Turismo is an e-commerce company, it doesn't handle magnetic cards**

				3.2.2, 3.2.3: N.A. because Sysdat Turismo doesn't make payment transaction, it only stores CHD on behalf of its customers 3.4.1.a, 3.4.1.b, 3.4.1.c: N.A. because disk encryption is not in use 3.5.1: N.A. because it's a future date requirement 3.6.b: N.A. because keys aren't shared with customers 3.6..: N.A. because manual clear-text key-management operations aren't in use
Requirement 4:	□	☒	□	4.1.f: N.A. because un-secure protocols are not in use 4.1.1: N.A. because CHD are not transmitted on wireless networks 4.2.b: N.A. because Sysdat can't access the PAN, so it can't send it using instant messaging technologies
Requirement 5:	☒	□	□	
Requirement 6:	□	☒	□	6.4.6: N.A. because it's a future date requirement
Requirement 7:	☒	□	□	
Requirement 8:	□	☒	□	8.1.6.b, 8.2.1.b, 8.2.3.b, 8.2.4.b, 8.2.5.b, : N.A. because Sysdat doesn't provide non-consumer customer's authentication credentials to its customers 8.3.1: N.A. because it's a future date requirement 8.3.2: N.A. because no remote access originating from outside Sysdat Turismo's network 8.5.1: N.A. because Sysdat Turismo doesn't remote access to its customer premises
Requirement 9:	□	☒	□	9.5, 9.5.1, 9.6.a, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1.a, 9.7.1.b, 9.8.a, 9.8.b, 9.8.1.a, 9.8.1.b, 9.8.2, : N.A. because Sysdat archives its backups on a network device, not on a removable media 9.9.a, 9.9.b, 9.9.c, 9.9.1.a, 9.9.1.b, 9.9.1.c, 9.9.2.a, 9.9.2.b, 9.9.3.a, 9.9.3.b: N.A. because Sysdat does not use POS POI terminals
Requirement 10:	□	☒	□	10.8.a, 10.8.1.a: N.A. because it's a future date requirement

Requirement 11:	□	☒	□	**11.1.c: N.A. because wireless scanning are not in use** **11.1.2.b: N.A. because unauthorized wireless access points are not found** **11.2.3.a: N.A. because no significant changes are made in the last year** **11.3.3: N.A. because no exploitable vulnerabilities are found** **11.3.4.1.a: N.A. because it's a future date requirement**
Requirement 12:	□	☒	□	**12.3.10.a: N.A. because nobody can access CHD remotely** **12.11.a, 12.11.b, 12.11.1: N.A. because it's a future date requirement**
Appendix A1:	□	□	☒	**Sysdat Turismo isn't a shared hosting provider**
Appendix A2:	□	□	☒	**2.1 Sysdat Turismo doesn't use POS POI terminals** **2.2 Sysdat Turismo doesn't use unsecure protocols**

Section 2: Self-Assessment Questionnaire D – Service Providers

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	15-09-2017	
Have compensating controls been used to meet any requirement in the SAQ?	☐ Yes	☒ No
Were any requirements in the SAQ identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements in the SAQ identified as being not tested?	☐ Yes	☒ No
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated *15-09-2017.*

Based on the results documented in the SAQ D noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document: (***check one):***

☒ **Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Sysdat Turismo Srl* has demonstrated full compliance with the PCI DSS.

□ **Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provide Company Name)* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*

□ **Compliant but with Legal exception:** One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.

If checked, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒ PCI DSS Self-Assessment Questionnaire D, Version *3.2, April 2016*, was completed according to the instructions therein.

☒ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.

□ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

☒ I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

☒ If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)

☐	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *CryptoNet Srl*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **15-09-2017**
Service Provider Executive Officer Name: **Gandola Luca**	*Title:* **Manager**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	n.a.

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* **n.a.**
Duly Authorized Officer Name: **n.a.**	*QSA Company:* **n.a.**

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	n.a.

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	□	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	□	
3	Protect stored cardholder data	☒	□	
4	Encrypt transmission of cardholder data across open, public networks	☒	□	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	□	
6	Develop and maintain secure systems and applications	☒	□	
7	Restrict access to cardholder data by business need to know	☒	□	
8	Identify and authenticate access to system components	☒	□	
9	Restrict physical access to cardholder data	☒	□	
10	Track and monitor all access to network resources and cardholder data	☒	□	
11	Regularly test security systems and processes	☒	□	
12	Maintain a policy that addresses information security for all personnel	☒	□	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	□	☒	Sysdat isn't a shared hosting provider
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	□	☒	Sysdat doesn't use POS POI terminals and unsecure protocols