



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:	C.E.E. Group Travelport a.s.	DBA (doing business as):	
Contact Name:	Martin Brandysky	Title:	sr. manager e-commerce & IT
Telephone:	+420222250670	E-mail:	martin.brandysky@travelportgds.cz
Business Address:	Sokolovská 685/136f	City:	
State/Province:		Country:	Czech Republic
		Zip:	18600
URL:			

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: GOL IBE

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):

B2B2C online e-shop GOL IBE for sale of tickets and other travel services. It is provided as a service, and the main pass through the search and reservation process is through
 a) Front Ends managed by us,
 or b) through an API that permits customization of the search process.

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:

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):
Other products that are managed by separate teams and/or on separate infrastructure such as Galileoterminal, GEM, etc. Compliance with PCI DSS is assessed separately for these products.

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):

- | | | |
|--|---|--|
| <input type="checkbox"/> Account Management | <input type="checkbox"/> Fraud and Chargeback | <input type="checkbox"/> Payment Gateway/Switch |
| <input type="checkbox"/> Back-Office Services | <input type="checkbox"/> Issuer Processing | <input type="checkbox"/> Prepaid Services |
| <input type="checkbox"/> Billing Management | <input type="checkbox"/> Loyalty Programs | <input type="checkbox"/> Records Management |
| <input type="checkbox"/> Clearing and Settlement | <input type="checkbox"/> Merchant Services | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Network Provider | | |

Others (specify):

Provide a brief explanation why any checked services were not included in the assessment:

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	We do not store any credit card data. Payments are made after redirecting to third-party payment pages.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	None

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)
<i>Example: Retail outlets</i>	3	Boston, MA, USA
Offices and testing infrastructure	1	Prague, CZ
Server hosting for production infrastructure	1	Prague, CZ

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)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> 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.*

GOL IBE uses external data sources to provide offers and make reservations. End customers are redirected to one of the external payment gateways to make a payment. Payment gateways are the external sites of payment gateways managed by banks or payment providers that are responsible for the security of payment cards handling.

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:

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: GOL IBE

PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach <small>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)</small>
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 - 2.6 The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Requirement 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Requirement 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Requirement 6:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.

Requirement 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.1.2, 8.1.4 - 8.1.8, 8.2.1 - 8.2.2, 8.2.4 - 8.2.6, 8.3 - 8.4, 8.6, 8.8 Reduced need to meet requirements - reduction according to SAQ A. (https://www.pcisecuritystandards.org/faqs/FAQ_1292) The product does not store, process, or transmit any cardholder data. 8.5 Compensation is used. 8.5.1 We don't need and use remote access to customer premises. 8.7 The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Requirement 9:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	There is no physical access to cardholder data. The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Requirement 10:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Requirement 11:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.1 - 12.7, 12.11 Reduced need to meet requirements - reduction according to SAQ A. (https://www.pcisecuritystandards.org/faqs/FAQ_1292) The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data. 12.8. Cardholder data are not used through any form of sharing. 12.10 The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The product accepts only card-not-present e-commerce transactions and does not

				store, process, or transmit any cardholder data.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The product accepts only card-not-present e-commerce transactions and does not store, process, or transmit any cardholder data.

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:	28.2.2018
Have compensating controls been used to meet any requirement in the SAQ?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the SAQ identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the SAQ identified as being not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the SAQ unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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 (28.2.2018).

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)**:

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby (C.E.E. Group Travelport a.s.) has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>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.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire D, Version (FEB18), was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
<input checked="" type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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)

<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor (<i>Qualys</i>)

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	Date: 28.2.2018
Service Provider Executive Officer Name: Martin Brandýský	Title: sr. manager e-commerce & IT

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

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

Signature of Duly Authorized Officer of QSA Company ↑	Date:
Duly Authorized Officer Name:	QSA Company:

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:	
---	--

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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	<input type="checkbox"/>	<input type="checkbox"/>	

