Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's 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:	Tecnes Milano s.r.l		DBA (doing business as):	Tecnes Milano s.r.l		
Contact Name:	Leopoldo Sergi		Title:	CEO		
Telephone:	+39 0267101036		E-mail:	l.sergi@tecnes.com		
Business Address:	Via Piranesi 26		City:	Milano		
State/Province:	MI	Country:	Italy		Zip:	20137
URL:	http://www.tecnes.com					

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Da Ros e Associati s.r.l				
Lead QSA Contact Name:	Giuseppe Citro		Title:	Security Consultant - QSA	
Telephone:	+390292979884		E-mail:	giuseppe.citro@daros-associati.it	
Business Address:	Via Calabiana, 6		City:	Milano	
State/Province:	MI	Country:	Italy	Zip:	20139
URL:	www.drea.it				

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:	Channel Manager Hotel Booking Engine	
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:	Web design, system integration	
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): ICT consultancy		
Provide a brief explanation why any checked services were not included in the assessment:	The services checked are non included in the assessment because they aren't related to CHD management	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Tecnes developed two tools for the accommodation market: a booking engine and a channel manager. The first is dedicated to the accommodation facilities that sell their services directly through their web sites; the second is dedicated to the accommodation facilities that sell their services trought third party portals. Tecnes sells the tools 'as a service'', so it's considered as a service provider. Both the tools collect and store the reservation data received by the accommodation facilities, including the CHD, if any. They manage 300.000 reservations at month. The reservation data are stored for management Purpose, the CHD are stored as guarantee for the accommodation facilities in case of the customers leaving the hotel w/o paying the accommodation, cancelling a non refundable reservation or not showing up without notice on the day established for the start of the stay, The booking engine receives the reservations data from the accommodation's facility web site using the iframe technology. The connection between the accommodation facilities' web saes and the booking engine is secured. The channel manager connects to each channel and gots the reservation data. This connection is secured, too. Both the booking engine and the channel manager store the reservation data on the same repository, In the repository the data are stored encrypted and removed at checkout after that accommodation facilities' confirm this by a ticketing system. In any case, if a ticket is not receved, at maximum the SAD are maintained until 3 days after the checkout of the accommodation facilities' customers The accommodation facilities can see the reservation data passing a two-level authentication process: using the first level account they can see the reservation data without the CHD, using the second level account they can see also the CHD
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Tecnes never uses the stored CHD to make payments. It has the ability to impact the security of the cardholder data because it

	receives, stores and transmits CHD, it develops the tools used to manage the CHD and it administers the infrastructure used for this purposes.

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*
Datacenter	2	c/o Google (Google Compute Engine) Via Piranesi 26, 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)
n.a	n.a	n.a	☐ Yes ☐ No	n.a
			☐ 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*	Tecnes build an Infrastructure based on two datacenter for business continuity purposes. The infrastructure is different in the datacenters (Google datacenter there is a virtual infrastructure that maintain the functioning of the services and the main DB while in the Via Piranesi datacenter there is

necessary payment components, as applicable.	a physical infrastructure just for the DB replication and the backup of the virtuals servers) , The two datacenters are connected thought an SSL tunnel that can be accessed only from selected users, authenticated by certificates and accessing from dedicated IP addresses. The CHD are received through the internet (accommodation facility's web site or connecting to the channel repository) over secured connections . The CHD are transmitted over the Internet (web Interface or API) using secure connections The CHD passes from the booking engine and the channel manager front ends (web based or API) In the repository (database) through API.
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?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	n.a
QIR Individual Name:	n.a
Description of services provided by QIR:	n.a
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:**
Google	Hosting Service Provider (it provides the Google Cloud Platform (GCP) technologies and infrastructure managed by Google)

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 of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

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 ROC
- 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:	Channell Manager Hotel Booking Engine			
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 the infrastructure doesn't contain routers 1.2.3: N.A. Tecnes doesn't build wireless networks
Requirement 2:	☐	☒	☐	2.1.1: N.A. because Tecnes doesn't build wireless networks 2.3.e.: N.A. because all non-console administrative access use strong cryptography 2.6: N.A. because Tecnes is note shared hosting providers.
Requirement 3:	☐	☒	☐	3.2.a, 3.2.b: N.A. because Tecnes is not an Issuer 3.4.e: N.A. because hashed and truncated version of the same PAN are not present In the environment. 3.4.1: N.A. because disk encryption Is not used 3.6.a: N.A. because Tecnes doesn't share keys with customers
Requirement 4:	☐	☒	☐	4.1.1: N.A. because Tecnes doesn't build wireless networks 4.2.a: N.A. because Tecnes, does not use end-user messaging technologies to send CHD

Requirement 5:	☐	☒	☐	5.1, 5.1.1, 5.2, 5.3 N.A. because the infrastructure is based on Linux systems, not commonly affected by malicious software.
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.3: N.A. because there aren't users terminated In the last six months. 8.1.4 N.A. because Tecnes' employees doesn't have users' accounts. Users accounts are only provided to the customers. 8.1.5: N.A. because third parties remote access isn't required. 8.1.8.b, 8.2.1.d, 8.2.1.e, 8.2.3.b, 8.2.4.b, 8.2.5.b: N.A. because Tecnes doesn't give non-consumer account to their customers 8.5.1: N.A. because Tecnes hasn't remote access to customer environments
Requirement 9:	☐	☒	☐	9.8.1: N.A. because Tecnes doesn't have hard-copy materials containing cardholder data 9.9: N.A. because Tecnes doesn't accept card-present transactions
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	11.2.1.b: N.A. because Tecnes Is still working to solve the vulnerabilities, the rescan is scheduled at the end of this activity 11.3.3: N.A. because the external penetration test doesn't loud exploitable vulnerabilities and Tecnes is still working to solve the ones found during the internal penetration test {the rescan Is scheduled at the end of this activity)
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	N.A. because Tacnes isn't a shared hosting provider
Appendix A2:	☐	☒	☐	A.2.1: N.A. because Tecnes doesn't collect credit card number using POS POI devices

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	30/11/2018	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC 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 the ROC dated 30/11/2018*.*

Based on the results documented in the ROC 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 ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Tecnes srl has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider 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 "Not in Place" 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)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC 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.

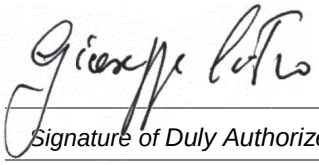
Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Comodo Ltd

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↗	*Date:* 30/11/2018
Service Provider Executive Officer Name: Leopoldo Sergi	*Title:* CEO

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

If a QSA was involved or assisted with this assessment, describe the role performed:	The QSA performed the audit, spending time both to the customer side, both doing remote assessing activities. Onsite the assessor interviewed the people, conducted observations at the office of Tecnes (administrative offices) and the datacenter, connected to the systems in order to verify the implementation of the requirements. Remotely the assessor analyzed the policies, the procedures and all other documents in order to evaluate the posture of Tecnes s.r.l.



Signature of Duly Authorized Officer of QSA Company ↗	*Date:* 30/11/2018
Duly Authorized Officer Name: Giuseppe Citro	*QSA Company:* Da Ros e Associati srl

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