



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:	VoiceSage Global Holdings DAC	DBA (doing business as):	VoiceSage		
Contact Name:	Glenn Sweeney	Title:	Chief Information Officer		
Telephone:	+353 1 969 5800	E-mail:	glenn.sweeney@voicesage.com		
Business Address:	15 Priory Office Park Stillorgan Road	City:	Blackrock		
State/Province:	Dublin	Country:	Ireland	Zip:	A94 R635
URL:	http://www.voicesage.com/				

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

Company Name:	Kyte Consultants				
Lead QSA Contact Name:	Francis Kyereh	Title:	Information Security Consultant		
Telephone:	+233207192236	E-mail:	francis@kyte.global		
Business Address:	170, Pater House, Psaila Street, Birkirkara, BKR 9077, Malta	City:	Birkirkara, Malta		
State/Province:	N/A	Country:	Malta	Zip:	N/A
URL:	https://kyte.global/				



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: VoiceSage

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: Not Applicable

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):

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

Not Applicable

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

VoiceSage's principal business is the development and provision of customer engagement solutions. VoiceSage send telephone calls, voice messages, SMS messages, email and Whatsapp/social media messages to consumers on behalf of their clients. VoiceSage provides an option to consumers to "auto pay" via channels (telephone, app, sms, etc) in which case the consumer is routed to a payment processor for payment processing. The consumer is transferred over a VoiceSage platform but payment is not processed by VoiceSage.

VoiceSage does not store or process cardholder data but cardholder data may be transmitted over VoiceSage networks when telephone payments are re-routed for processing. VoiceSage does not record any of the "auto pay" transactions which are rerouted in this manner. Payments are not processed by VoiceSage but are transferred to



	<p>third-party processors. Third parties that VoiceSage connects to include Encoded, PayPal, Stripe, WorldPay, PaySafe and Freeman Grathan Holdings for payment processing on behalf of VoiceSage clients.</p>
<p>Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.</p>	<p>Call data is provided to VoiceSage in XLS or CSV format in a secure FTP connection. VoiceSage use this input to make a call/SMS/communication to the consumer customer. The consumer customer receives the call and is asked to confirm their identity and are given the option to be connected to the acquiring bank or third-party processor.</p> <p>For payment transactions VoiceSage make a point to point connection between the consumer and the acquiring bank or the third-party processor, following which the acquiring bank takes over the client contact.</p> <p>Credit card data does not pass across the VoiceSage system and is not stored. The role of VoiceSage is to facilitate the customer engagement on behalf of its clients.</p>

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	<i>Boston, MA, USA</i>
Corporate Office	1	Blackrock, Co. Dublin, Ireland
Datacentre	1	PCI Compliant Cloud services at AWS EU West



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)
None	N/A	N/A	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Not 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.*

The cardholder data environment is limited to the network components, databases and application servers which integrate with the payment providers in a hosted session on their websites.

VoiceSage as a customer engagement solutions provider only facilitates the data capture of payment card details for onward authorisation by the payment provider that the customer is using for the transaction.

Clients of VoiceSage who are the merchants integrate their websites or apps with the VoiceSage platform. By this integration, VoiceSage makes it possible for the customers of VoiceSage client to interact with that entity via voice, SMS, RMM, e-mail, chatbots, and social media. Depending on the configuration choices of VoiceSage's client, payment transactions can be facilitated by VoiceSage in such manner that is transparent to the customer. VoiceSage integrates with the payment providers' payment gateways in such a manner that payment card details are collected directly by the payment provider and are not collected and stored in VoiceSage's technical environment.

Third parties that VoiceSage connects to are Encoded, PayPal, Stripe, WorldPay,



	<p>PaySafe and Global Payments for payment processing on behalf of clients.</p> <p>Critical system components:</p> <p>Databases: Microsoft SQL Server</p> <p>Firewall: Cloud VPC, Cloud NAT</p> <p>Anti-Malware: Trend Micro Deep Security</p> <p>Applications: VoiceSage Customer Engagement Platform.</p> <p>Logging: CloudWatch, Cloudtrail, Datadog, GuardDuty</p>
--	--

<p>Does your business use network segmentation to affect the scope of your PCI DSS environment?</p> <p><i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i></p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>
---	--



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:	Not Applicable
QIR Individual Name:	Not Applicable
Description of services provided by QIR:	Not Applicable

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:
Encoded Global Payments	facilitation of payment processing
Amazon Web Services (AWS)	Infrastructure/Network, Platform as a Service(PaaS), Container as a Service (CaaS)
WorldPay	facilitation of payment processing
PayPal	facilitation of payment processing
Stripe	facilitation of payment processing
PaySafe	facilitation of payment processing

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:		VoiceSage		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.3 Not applicable – No wireless environments are connected to the technical environment
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 There is no wireless environment connected to the technical environment 2.2.3 There is no need to implement additional security features for any required services, protocols, or daemons that are considered to be insecure 2.6 VoiceSage is not a shared hosting provider that hosts the cardholder data of other organizations.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.4.1 Disk encryption is not used and cardholder data is not written to removable media. 3.6 VoiceSage does not store cardholder data in its technical environment. 3.6.6 Manual clear-text cryptographic key-management operations are not used
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1 Cardholder data is not transmitted over open, public networks
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	



Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.5.1 Not applicable - VoiceSage does not have remote access to customer premises. 8.7 Not applicable. Cardholder data is not stored in the VoiceSage technical environment.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.6.2 Not applicable - VoiceSage does not send any media containing cardholder data outside of the facility. 9.7.1 Not Applicable. VoiceSage hosts the entire technical environment in the AWS Cloud. 9.9-9.9.3b Not applicable – VoiceSage does not manage Point of Interaction (POI) or Process Data Quickly (PDQ) devices as part of contact points for service portfolio.
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.1.1 Not applicable - No wireless environments are connected to the cardholder environment.
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	VoiceSage is not a shared hosting provider
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No early SSL/TLS in the environment



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:	20th October 2023
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC 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 the ROC dated (20th October 2023).

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**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby VoiceSage Global Holdings DAC) has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>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 () 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 “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.</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"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1), and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input 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 (Qualys) |

Part 3b. Service Provider Attestation

DocuSigned by:

84275D95885C444...

Signature of Service Provider Executive Officer ↑

Date: 24th October, 2023

Service Provider Executive Officer Name: Glenn Sweeney

Title: Chief Information Officer

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

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

Assessment review and certification

DocuSigned by:

DA9183992C8C4CD...

Signature of Duly Authorized Officer of QSA Company ↑

Date: 24th October, 2023

Duly Authorized Officer Name: Trevor Axiak

QSA Company: Kyte Consultants

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

