More information:
https://patronusec.com/pci

PATRONUSEC
Your Cyber Security Patronus

PCI DSS Assessment

Attestation of Compliance

PATRONUSEC SP. Z O.O. | UL. ŚWIĘTY MARCIN 29/8, POZNAŃ, POLAND | HELLO@PATRONUSEC.COM | +48 662 395 468

QUALIFIED SECURITY ASSESSOR™

QUALIFIED PIN ASSESSOR (QPA) PROGRAM

SECURE SOFTWARE ASSESSOR

SECURE SLC ASSESSOR

POINT-TO-POINT ENCRYPTION ASSESSOR

3DS ASSESSOR

Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 2

Publication Date: August 2023

PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Little Pond Ltd DBA Prommt

Assessment End Date: 19 July 2024

Date of Report as noted in the Report on Compliance: 24 July 2024

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* ("Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	*Little Pond Ltd.*
DBA (doing business as):	*Prommt*
Company mailing address:	*The Greenway, Ardilaun Court, St Stephens Green, Dublin D02 TD28 Republic of Ireland*
Company main website:	*https://www.prommt.com/*
Company contact name:	*Paul Healy*
Company contact title:	*Head of Engineering*
Contact phone number:	*+353 1 539 2300*
Contact e-mail address:	*paul.healy@prommt.com*

Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)	
ISA name(s):	*Not Applicable*
Qualified Security Assessor	
Company name:	*Patronusec Sp. z o.o.*
Company mailing address:	*Św. Marcin 29/8, 61-806 Poznań, Poland*
Company website:	*https://patronusec.com*
Lead Assessor name:	*Christopher Ince*

Assessor phone number:	*+44 7857851666*
Assessor e-mail address:	*PCIQA@patronusec.com*
Assessor certificate number:	*205-825*

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	*Prommt*

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☒ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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): *Payment integration provider*

Note: *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select 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-hosting services
- □ Security services
- □ 3-D Secure Hosting Provider
- □ Multi-Tenant Service Provider
- □ Other Hosting (specify):

Managed Services:

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

Payment Processing:

- □ POI / 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 Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.	*Little Pond Ltd., hereafter referred to as Prommt, is an e-commerce integration service provider.* *Prommt has developed a payment integration solution that sits between merchants and acquires providing prompts via SMS or email to customers to make payments via the acquirer(s) that the merchant has a relationship with.* *Processing:*

	Prommt connects to each PCI compliant Payment Service Provider directly via their specific API or iFrame solution. No processing of cardholder data occurs on the Prommt system. *Transmitting:* *Cardholder data is transmitted to each PCI compliant Payment Service Provider via TLS 1.2 session utilizing their native API to undertake the processing of cardholder data.* *Storing:* *Prommt stores tokenisedcustomer details in a MySQL database and stores it in encrypted and hash format. Hashes generated are used to search the database to verify if the card data is already in the database transaction.*
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	*Not Applicable*
Describe system components that could impact the security of account data.	*Prommt uses the following components in its CDE which are included in this assessment:* *For e-commerce payments:* • *Cloudflare* • *AWS Load Balancer* • *AWS Virtual Private Cloud* • *AWS EC2 Security Groups* • *Internet gateways* • *NAT gateways*

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	*Prommt, as a service provider, hosts its CDE on a PCI DSS compliant cloud-based Amazon Web Services (AWS) infrastructure.* *The following processes and procedures performed by Prommt can impact the security of cardholder data:* • *Protecting the AWS-based CDE from unauthorized access and operations.* • *Ensuring secure cardholder data transmission from the cardholder to the merchants' choice of PCI compliant payment service provider.* *Prommt services only card-not-present payment transactions.*

Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the “Segmentation” section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	**Total Number of Locations** (How many locations of this type are in scope)	**Location(s) of Facility** (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Amazon Web Service (AWS) Cloud Hosting provider	*1*	*Dublin, Republic of Ireland*

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions[♦]?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Not Applicable	*Not Applicable*	*Not Applicable*	*Not Applicable*	*Not Applicable*

[♦] For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2f. Third-Party Service Providers *(***ROC Section 4.4***)*	
For the services being validated, does the entity have relationships with one or more third-party service providers that:	
• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☒ Yes ☐ No
If Yes:	
Name of Service Provider:	**Description of Services Provided:**
Amazon Web Services	*Cloud Infrastructure Provider*
Note: *Requirement 12.8 applies to all entities in this list.*	

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

***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: *Prommt*

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	☒	☒	□	□	□	□
Requirement 2:	☒	☒	□	□	□	□
Requirement 3:	☒	☒	□	□	□	□
Requirement 4:	☒	☒	□	□	□	□
Requirement 5:	☒	☒	□	□	□	□
Requirement 6:	☒	☒	□	□	□	□
Requirement 7:	☒	☒	□	□	□	□
Requirement 8:	☒	☒	□	□	□	□
Requirement 9:	☒	☒	□	□	□	□
Requirement 10:	☒	☒	□	□	□	□
Requirement 11:	☒	☒	□	□	□	□
Requirement 12:	☒	☒	□	□	□	□
Appendix A1:	□	☒	□	□	□	□
Appendix A2:	□	☒	□	□	□	□

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	*1.2.6 – Not Applicable - Prommt is not using unsecured services or protocols* *2.2.5 – Not Applicable - Prommt is not using unsecured services or protocols* *2.3.1 – 2.3.2 Not Applicable – No wireless technology is in use or is connected to the CDE* *3.3.2- Not Applicable – Prommt does not sore and SAD* *3.3.3 – Not Applicable – Prommt is not an issuer and does not support issuing services* *3.4.2 – Not Applicable – Best practice before 31 March 2025* *3.5.1.1 – Not Applicable – Best practice before 31 March 2025* *3.5.1.2 -3.5.1.3 – Not Applicable – Prommt does not use disk encryption3.6.1 – Not Applicable – Prommt does not store full PAN* *3.6.1.1 – 3.6.1.4 – Not Applicable – Prommt does not store full PAN* *3.7.1 - Not Applicable - Prommt does not manage cryptographic keys used to protect PAN. All key management used for the protection of PAN is performed by PCI compliant TPSP* *3.7.2 - Not Applicable - Prommt does not distribute keys* *3.7.3 - Not Applicable - Prommt does not manage cryptographic keys used to protect PAN. All key management used for the protection of PAN is performed by PCI compliant TPSP* *3.7.4 - Not Applicable - Prommt does not manage key to protect PAN* *3.7.5 - 3.7.8 Not Applicable - Prommt does not manage cryptographic keys used to protect PAN. All key management used for the protection of PAN is performed by PCI compliant TPSP* *3.7.9 – Not Applicable - Prommt does not share keys with its customers* *4.2.1.1 – Not Applicable - Best practice before 31 March 2025* *4.2.1.2 – Not Applicable - No wireless networks transmitting cardholder data or connected to Prommt's CDE* *4.2.2 – Not Applicable – Prommt doesn't send PAN via end-user messaging technologies* *5.2.3.1 – Not Applicable - Best practice before 31 March 2025* *5.3.2.1 – Not Applicable - Best practice before 31 March 2025*

	5.3.3 – Not Applicable – Best practice before 31 March 2025 *5.4.1 - Not Applicable – Best practice before 31 March 2025* *6.2.3.1 - Not Applicable – Prommt is using automated code scanning solution* *6.3.2 – Not Applicable – Best practice before 31 March 2025* *6.4.2– 6.4.3 Not Applicable – Best practice before 31 March 2025* *6.5.2 - Not Applicable – No significant change occurred within the past 12 months.* *7.2.4 – 7.2.5 Not Applicable – Best practice before 31 March 2025* *7.2.5.1 – Not Applicable – Best practice before 31 March 2025* *8.2.3 - Not Applicable - Prommt does not have remote access to the customers` premises* *8.2.7 - Not Applicable - No vendors providing remote management services to Prommt.* *8.3.6 - Not Applicable – Best practice before 31 March 2025* *8.3.10 - Not Applicable – There is no customer user access to cardholder data.* *8.3.10.1 - Not Applicable – There is no customer user access to cardholder data.* *8.4.2 - Not Applicable – Best practice before 31 March 2025* *8.5.1 - Not Applicable – Best practice before 31 March 2025* *8.6.1 - 8.6.3 Not Applicable – Best practice before 31 March 2025* *9.5.1 - 9.5.1.3 Not Applicable – Prommt does not own any point-of-sale systems and is not responsible for the point-of-sale systems owned by customers at their sites.* *10.4.1.1 - Not Applicable – Best practice before 31 March 2025.* *10.4.2.1 - Not Applicable – Best practice before 31 March 2025* *10.7.2 - Not Applicable – Best practice before 31 March 2025* *11.3.1.1 - 11.3.1.3 Not Applicable – Best practice before 31 March 2025* *11.3.2.1 - Not Applicable – No significant change occurred within the past 12 months.*

	11.4.7 - Not Applicable – Best practice before 31 March 2025 *11.5.1.1 - Not Applicable – Best practice before 31 March 2025* *11.6.1 - Not Applicable – Best practice before 31 March 2025* *12.3.2 - Not Applicable - Prommt does not use Customized Approach for and requirement.* *12.3.3 - 12.3.4 - Not Applicable – Best practice before 31 March 2025* *12.5.2.1 - Not Applicable - Best practice before 31 March 2025* *12.5.3 - Not Applicable - Best practice before 31 March 2025* *12.6.2 Not Applicable – Best practice before 31 March 2025* *12.6.3.1 – 12.6.3.2 - Not Applicable - Best practice before 31 March 2025* *12.10.4.1 - Not Applicable - Best practice before 31 March 2025* *12.10.7 - Not Applicable – Best practice before 31 March 2025* *Appendix A1 - Not Applicable – Prommt is not multi-tenant Service Provider.* *Appendix A2 - Not Applicable – Prommt does not manage POI terminal nor is responsible for its configuration.* *Appendix A3 – Not Applicable - No additional validation of existing PCI DSS requirements is required.* *A2.1 - A2.1.3 - Not Applicable - Best practice before 31 March 2025*
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	*Not Applicable*

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*			13 May 2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*			19 July 2024
Were any requirements in the ROC unable to be met due to a legal constraint?			□ Yes ☒ No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:			☒ Yes □ No
• Examine documentation	☒ Yes	□ No	
• Interview personnel	□ Yes	☒ No	
• Examine/observe live data	□ Yes	☒ No	
• Observe process being performed	□ Yes	☒ No	
• Observe physical environment	□ Yes	☒ No	
• Interactive testing	□ Yes	☒ No	
• Other: N/A	□ Yes	□ No	

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 24 July 2024)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)***:**

☒ **Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT rating; thereby *Little Pond Ltd*. has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

☐ **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance: *YYYY-MM-DD*

An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.

☐ **Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this AOC will be submitted.

If selected, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement from being met
N/A	**N/A**

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

DocuSigned by: donal.mcguinness@prommt.com C53AFC1E612F46D...	
Signature of Service Provider Executive Officer ↑	Date: 25-Jul-2024
Service Provider Executive Officer Name: *Donal McGuinness*	Title: *CEO*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signed by: CFD062571035422...	
Signature of Lead QSA ↑	Date: 25-Jul-2024
Lead QSA Name: *Christopher Ince*	
DocuSigned by: Krzysztof S. Olejniczak BBC1171147D34F1...	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 25-Jul-2024
Duly Authorized Officer Name: *Krzysztof (Kris) Olejniczak*	QSA Company: *Patronusec Sp. z o.o.*

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

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 network security controls	□	□	
2	Apply secure configurations to all system components	□	□	
3	Protect stored account data	□	□	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	□	□	
5	Protect all systems and networks from malicious software	□	□	
6	Develop and maintain secure systems and software	□	□	
7	Restrict access to system components and cardholder data by business need to know	□	□	
8	Identify users and authenticate access to system components	□	□	
9	Restrict physical access to cardholder data	□	□	
10	Log and monitor all access to system components and cardholder data	□	□	
11	Test security systems and networks regularly	□	□	
12	Support information security with organizational policies and programs	□	□	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	□	□	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	□	□	