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 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Little Pond Ltd DBA Prommt

Date of Report as noted in the Report on Compliance: 24 July 2026

Date Assessment Ended: 09 July 2026

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 Stephen's Green,* *Dublin 2,* *D02 TD28,* *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:	*PCI DSS QSA 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:	**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):		

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 Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	*Little Pond Ltd., trading as Prommt, is an e-commerce payment integration service provider.* *Prommt provides a payment orchestration and payment-link service that enables merchants to request card-not-present payments from customers by SMS or email. The customer payment journey is integrated with PCI-compliant payment processors/acquirers using each*

	processor/acquirer's supported iframe, hosted-field, hosted-payment-page, or API integration method. ***Processing:*** *Full PAN and sensitive authentication data are captured and processed by the payment processor/acquirer payment component. Prommt does not process full PAN or SAD within its application environment.* ***Transmitting:*** *Full payment credentials are submitted to the payment processor/acquirer payment component over TLS. Prommt transmits payment requests, transaction instructions, and processor/acquirer API calls, and receives processor/acquirer responses containing tokenised transaction references, truncated card information where returned, authorisation status, and related metadata.* ***Storing:*** *Prommt stores processor/acquirer-returned tokens, transaction references, last four digits/truncated PAN where returned, expiry date/card type where returned, and related transaction metadata in the application database. These values are not full PAN and are not sufficient to reconstruct PAN. Access to the database is restricted and logged.*
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	*Prommt controls the merchant-facing payment orchestration flow used to request and manage card-not-present payments. Although payment-entry components are provided by PCI-compliant payment processors/acquirers, Prommt's configuration and operation of its platform, integrations, authentication controls, and supporting infrastructure can affect the confidentiality and integrity of payment-related communications and processor/acquirer-returned account data elements.* *Prommt can impact the security of account data through its management of public-facing application components, API integrations, TLS-protected communications under its control, administrative access, logging and monitoring, vulnerability management, change management, and database access controls. Weaknesses or misconfiguration in these areas could affect the secure handling of processor/acquirer-returned tokens, truncated card information where provided, transaction references, and related payment metadata.*

Describe system components that could impact the security of account data.	*Prommt uses the following components and services within, or supporting, the assessed environment:* • *AWS Virtual Private Cloud (VPC), public/private subnets, route tables, Internet gateways, and NAT gateways.* • *AWS Application Load Balancer and AWS WAF for public-facing web traffic.* • *AWS EC2 security groups and network access controls for segmentation and traffic restriction.* • *AWS IAM Identity Center for administrative authentication and role assignment.* • *AWS Systems Manager Fleet Manager and Session Manager for controlled administrative access.* • *Private bastion access for controlled database port-forwarding to Amazon RDS.* • *Amazon RDS for application database services.* • *Amazon EKS/RabbitMQ used for application messaging and supporting services.* • *AWS CloudWatch, CloudTrail, S3 log storage, and Athena for logging, monitoring, and historical log review.* • *AWS GuardDuty for threat detection and AWS Inspector for vulnerability detection.* • *AWS Backup for backup management.* • *GitLab, Linear, Vanta, JScrambler, and Amazon Bedrock/Claude Sonnet were used to support development, compliance, payment-page monitoring, and segmentation-test analysis.*

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.*	*Little Pond Ltd., trading as Prommt, operates an e-commerce payment integration environment hosted on Amazon Web Services (AWS) and supporting card-not-present transactions only.* *The assessed environment supports a payment-link orchestration service that enables merchants to request payments from customers by SMS or email. Customers are directed to payment pages where payment-entry components are provided by the relevant PCI-compliant payment processor/acquirer using supported iframe, hosted-field, hosted-payment-page, or API integration methods. Full PAN and sensitive authentication data are captured and processed by the payment processor/acquirer payment component, not within Prommt's application environment.* *The environment covered by this assessment includes the public-facing application and supporting infrastructure used to initiate payment requests, manage merchant and transaction workflows, transmit payment requests and transaction instructions, receive processor/acquirer responses, and store processor/acquirer-returned tokens, truncated card information where provided, transaction references, authorisation responses, and related transaction metadata.* *Connections into and out of the assessed environment include inbound HTTPS traffic to Prommt's public-facing services, outbound TLS-protected communications to payment processors/acquirers and supporting services, administrative access through controlled management channels, and logging and monitoring flows to centralised AWS logging and security services.* *Critical system components and supporting security-impacting components include AWS VPC, public and private subnets, route tables, Internet gateways, NAT gateways, AWS*

	Application Load Balancer, AWS WAF, EC2 security groups, network access controls, AWS IAM Identity Center, AWS Systems Manager Fleet Manager and Session Manager, private bastion access for controlled database port-forwarding, Amazon RDS, Amazon EKS, RabbitMQ, AWS CloudWatch, CloudTrail, S3 log storage, Athena, GuardDuty, Inspector, and AWS Backup.
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, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

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 hosting and managed services provider for the assessed environment, including infrastructure and supporting security services*
Barclaycard / Cybersource	*Payment processing / acquiring services*
Chase	*Payment processing / acquiring services*
Planet	*Payment processing / acquiring services*
Euronet	*Payment processing / acquiring services*
Fiserv / Cover / Carat	*Payment processing / acquiring services*
Global Payments	*Payment processing / acquiring services*
NatWest Tyl / First Data	*Payment processing / acquiring services*
Paysafe	*Payment processing / acquiring services*
PXP	*Payment processing / acquiring services*
Stripe	*Payment processing / acquiring services*
Adyen	*Payment processing / acquiring services*
AIBMS	*Payment processing / acquiring services*
Elavon / Opayo	*Payment processing / acquiring services*
Lloyds Cardnet	*Payment processing / acquiring services*
Worldpay	*Payment processing / acquiring services*
FreedomPay	*Payment processing / acquiring services*

Token.io	*Open banking payment services provider that could impact the security of the assessed environment; no account data shared*

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 a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
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.	*2.2.5 – Prommt do not use any insecure services, protocols or deamons within the CDE.* *2.3.1 – 2.3.2– No wireless technology is in use or is connected to the CDE.* *3.1.2 - 3.3.2– Prommt does not store or receive PAN and SAD within its systems.* *3.3.3 –Prommt is not an issuer and does not support issuing services.* *3.4.1 – 3.7.9– Prommt does not store or receive PAN and SAD within its systems.* *4.2.1.2 - No wireless networks transmitting cardholder data or connected to Prommt's CDE.* *4.2.2 – Prommt doesn't send PAN via end-user messaging technologies.* *5.2.3 - 5.2.3.1– Prommt considers all system components to be at risk for malware.* *5.3.3 – No removeable media in use.* *5.3.2.1 - Prommt employs continuous behavioral analysis via AWS GuardDuty for malware detection, providing real-time protection across all systems.* *6.2.3.1 – Prommt is using automated code scanning solution.* *6.4.1 - This requirement no longer applies as of 31 March 2025.* *7.2.6 - The environment stores only processor/acquirer-returned tokens, transaction references, truncated card information where returned, expiry date/card type where returned, and related transaction metadata, which are not repositories of stored CHD.* *8.2.3 - Prommt does not have remote access to the customers` premises* *8.2.7 - No vendors providing remote management services to Prommt.* *8.3.9 - Multi-factor authentication (MFA) is enforced for every interactive login to all in-scope system components, with password-only access disabled.* *8.3.10 – This requirement no longer applies as of 31 March 2025.* *8.3.10.1 – There is no customer user access to cardholder data.* *9.4.1 - 9.4.7 – Prommt does not generate, store, or back up cardholder data in any form or media.* *9.5.1 - 9.5.1.3 – 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.* *10.4.2.1 – Prommt uses Datadog for continuous real-time log monitoring with immediate SOC alerts,*

	eliminating the need for periodic reviews or risk analysis. *10.7.1 - This requirement no longer applies as of 31 March 2025.* *11.4.7 – Prommt is not a multi-tenant hosting provider.* *12.3.2 – Prommt does not use Customized Approach to meet any requirements.* *Appendix A1 – Prommt is not multi-tenant Service Provider.* *Appendix A2 – Prommt does not manage POI terminal nor is responsible for their configuration.*
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**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	*15 June 2026*
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	*09 July 2025*
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ 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 *24 July 2026*.

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

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 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of 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

Donal McGuinness

Signature of Service Provider Executive Officer ↑	Date: 27-Jul-2026 | 15:46:38 CEST
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:

Signature of Lead QSA ↑	Date: 27-Jul-2026 | 15:48:02 CEST
Lead QSA Name: *Christopher Ince*	

Signature of Duly Authorized Officer of QSA Company ↑	Date: 27-Jul-2026 | 15:56:00 CEST
Duly Authorized Officer Name: *Agnieszka Leszczyńska*	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	☐	☐	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/