Integrity360
your **security** in mind

CERTIFICATE OF
COMPLIANCE WITH PCI DSS

AWARDED TO

Quipu Gmbh

ASSESSED BY ADVANTIO LIMITED (AN INTEGRITY360 COMPANY) AND FOUND TO BE COMPLIANT WITH PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD V3.2.1

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

WEBSITE	http://www.quipu.de
CATEGORY	Service Provider
ASSESSMENT	Level 1

Alessandro Amalfitano

ALESSANDRO AMALFITANO
PAYMENTS COMPLIANCE PRACTICE MANAGER

COMPLIANCE DATE	28 March, 2024
EXPIRATION DATE	27 March, 2025

Advantio Limited (an Integrity360 company) has issued this certificate to indicate that the aforementioned company has been assessed against the objectives of Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures and were found to be compliant with PCI DSS, on the date of issue only, no other guarantees given. This certificate is to be used in conjunction with the Attestation of Compliance (AoC) for a detailed description of the services included in the scope of the PCI DSS Assessment. This certificate offers no guarantee or warranty to any third party that the company is invulnerable to attack or breaches in its security, integrity or availability, and Advantio Limited (an Integrity360 company) accordingly accepts no liability to any third party in the event of loss or damage of any description caused by any failure in or breach of customer's security.

Certificate ID: W1XZEitO6yAukax

INTEGRITY360.COM

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

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:	Quipu Gmbh		DBA (doing business as):	N/A	
Contact Name:	Gleb Stolyarov		Title:	Head of Information Security, Risk and Compliance Department	
Telephone:	+49 69 506990 212		E-mail:	stolyarov@quipugmbh.com	
Business Address:	Königsberger Str. 1		City:	Frankfurt am Main	
State/Province:	Hessen	Country:	Germany	Zip:	60487
URL:	http://www.quipu.de/				

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

Company Name:	Advantio Limited				
Lead QSA Contact Name:	Oleg Aksyonenko		Title:	Senior Security Consultant	
Telephone:	+380 67 7016691		E-mail:	oleg.aksyonenko@integrity360.com	
Business Address:	Termini, 3 Arkle Road, Sandyford Business Park, Sandyford		City:	Dublin	
State/Province:	N/A	Country:	Ireland	Zip:	D18 T6T7
URL:	https://www.advantio.com				

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:	QPC issuing and acquiring services	
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): 3D Secure, E-commerce Acquring
☒ 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:	N/A	
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:		

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	As a processing center, Quipu receives, stores, processes and transmits CHD and SAD as a part of authorization and clearing. Storage: data is in encrypted files (RSA-2048, clearing) and encrypted database (Oracle TDE, AES-256). Processing: All processing functionality is performed by TranzWare PA-DSS validated software suite. This software is currently undergoing Secure Software validation. Receiving and transmitting: through EFT (authorization) and secure file transfer (SFTP for clearing files). All CHD and SAD exchange is performed electronically through encrypted (TLS 1.2 with strong ciphers) channels from POS, ATM or e-commerce to authorization platform.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	N/A

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*
Data center	2	Equinix FR2 Kruppstrasse 121-127 Frankfurt Germany 60388 Equinix FR4 Lärchenstrasse 110 Frankfurt Germany 65933
Corporate office1	1	Königsberger Str. 1, 60487 Frankfurt/Main, Germany

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)
TranzWare Suite (TWS)	3.2	Compass Plus	☒ Yes ☐ No	TWO is a PA-DSS validated application, expired on 29 Oct 2022

				and valid for pre-existing deployments. Currently, the application is undergoing a PCI Secure Software assessment.
			☐ 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 necessary payment components, as applicable.*	QPC uses the PCI PA-DSS certified payment application TranzWare, developed by Compass Plus. Cardholder data is stored in a database encrypted with 256-bit AES and flat files encrypted with RSA 2048-bit encryption. The data transferred from and to the banks and card schemes over open public networks is secured with encrypted VPNs. The payment platform is operated by personnel located in Frankfurt/Main, Germany. The administrative communication from the office to the data center is secured by MFA. The Kososvo-based Quipu Sh.P.K. Card Personalisation Centre, involved in data preparation and card issuing business and serviced by QPC, is not part of the current assessment.
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:	
QIR Individual Name:	
Description of services provided by QIR:	

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:**
Compass Plus	Software supplier.
Oracle	Licenses & Support.
LichtBlick	Electricity.
Deutsche Telecom/Colt	ISP.
BSGWüst	Physical Security of Premises.
Primion HP Visa Axway Equinix	Security Systems. Hardware support. Edit Package. MasterCard file transfer. Data center & colocation provider.

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:	QPC issuing and acquiring services

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:	☒	□	□	
Requirement 2:	□	☒	□	**2.1.1 - There are no wireless networks in scope of this assessment;** **2.2.3 - There are no insecure services, daemons or protocols;** **2.6 - The assessed entity is not a shared hosting provider.**
Requirement 3:	□	☒	□	**3.4.1 - Disk encryption is not used;** **3.6.2 - The cryptographic key discribution is not performed.**
Requirement 4:	□	☒	□	**4.1.1 - There are no wireless networks in scope of this assessment.**
Requirement 5:	□	☒	□	**5.1.2 - Anti-malware is installed on all types of CDE components.**
Requirement 6:	□	☒	□	**6.3, 6.3.1, 6.3.2, 6.5 (6.5.1 - 6.5.10) - There is no internal application development;** **6.4.6 - There have been no significant changes within the past 12 months;**
Requirement 7:	☒	□	□	

Requirement 8:	☐	☒	☐	**8.1.5 - There are no third parties with remote access to the CDE;** **8.5.1 - Quipu does not have remote access to customer premises.**
Requirement 9:	☐	☒	☐	**9.6.2, 9.6.3 - Media is not sent outside of the Quipu facilities;** **9.8.1 - Quipu does not allow storage of any cardholder data in hardcopy format;** **9.9 (9.9.1 - 9.9.3) - Quipu does not manage any devices that capture card data via direct physical interaction with the card.**
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	**11.1.1 - There are no wireless networks in scope of this assessment;** **11.2.3 - There have been no significant changes within the past 12 months.**
Requirement 12:	☐	☒	☐	**12.3.9 - No vendors or business partners have access to Quipu CDE.**
Appendix A1:	☐	☐	☒	**The assessed entity is not a shared hosting provider.**
Appendix A2:	☐	☐	☒	**SSL / early TLS is not utilized.**

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:	*06 March 2024*	
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 *06 March 2024.*

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 *Quipu Gmbh* 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, CVN2, CVV2, or CID 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 *Qualys*

Part 3b. Service Provider Attestation

Dana Enache
Managing Director

Petru Jucovschi
Managing Director
Petru Jucovschi (Mar 28, 2024 12:28 GMT+1)

Signature of Service Provider Executive Officer ↑	*Date:* **28 March 2024**
Service Provider Executive Officer Name: procurement@quipu.de	*Title:*

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*QSA performed the assessment and completed the RoC for Quipu Gmbh.*

DocuSigned by:
ABA9DEC3FF57486...

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 28 March 2024*
Duly Authorized Officer Name: Martin Petrov	*QSA Company:* Advantio Limited

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