Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Merchants

- **Version 4.0**
- Revision 1
- Publication Date: December 2022

PCI DSS v4.0 Attestation of Compliance for Report on Compliance - Merchants

- **Entity Name: Buypass AS**
- **Assessment End Date: 30.05.24**
- **Date of Report as noted in the Report on Compliance: 30.05.24**

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

Section 1 Assessment Information

Instructions for Submission

- This Attestation of Compliance (AOC) must be completed as a declaration of the results of the merchant's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* ("Assessment"). Complete all sections. The merchant 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:	Buypass AS
DBA (doing business as):	Payment and Trustservices provider
Company mailing address:	Kundeservice@buypass.no
Company main website:	Buypass.no
Company contact name:	Ole Kristian Målbakken
Company contact title:	CISO
Contact phone number:	+47 91864334
Contact e-mail address:	ole.malbakken@buypass.no
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):	Ole Kristian Målbakken
Qualified Security Assessor	
Company name:	N/A
Company mailing address:	N/A
Company website:	N/A
Lead Assessor name:	N/A
Assessor phone number:	N/A
Assessor e-mail address:	N/A
Assessor certificate number:	N/A

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply):
(ROC Section 2.1)

Indicate all payment channels used by the business that are included in this Assessment.

- ☐ Mail order / telephone order (MOTO)
- ☒ E-Commerce
- ☐ Card-present

Are any payment channels not included in this Assessment?	☐ Yes ☒ No
If yes, indicate which channel(s) is not included in the Assessment and provide a brief explanation about why the channel was excluded.	

Note: *If the merchant has a payment channel that is not covered by this Assessment, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.*

Part 2b. Description of Role with Payment Cards
(ROC Section 2.1)

For each payment channel included in this Assessment as selected in Part 2a above, describe how the business stores, processes, and/or transmits account data.

Channel	How Business Stores, Processes, and/or Transmits Account Data
Card present channel	Card present / User present in mobile apps and web interfaces when amount is more than NOK 300 (3D-Secure via NetAxept, or Delegated SCA – Vipps, Apple Pay etc). PSD 2 requirements
Card-not-present channel	Card-not-present in mobile apps and web interfaces when amount less than NOK 300 (Low value, ref PSD 2 - Sofie SDI).

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.*	Buypass runs the operations in-house based on two datacenters located within a safe distance (Oslo and Gjøvik). The two datacenters are operating redundantly. Both datacenters are harmonized with Tier 3 requirements according to Uptime Institute as reference. During operations CHD is stored, processed and transmitted between these two datacenters. CHD exchanged between Buypass and end-users, and Buypass and B2B customers as Norsk Tipping and Norges Idrettsforbund are transmitted through API's and VPN solutions.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. Refer to "Segmentation" section of PCI DSS for guidance on segmentation.	☒ Yes ☐ No

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

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

List all types of physical locations/ facilities (for example, retail locations, 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: Retail locations	*3*	*Boston, MA, USA*
Data center	2	Gjøvik and Oslo, Norway

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
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

* 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

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

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)	
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 scope of the Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, 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 Service(s) Provided:**
Nets	Payment Authorization, 3D-secure, aquiring services.

Note: *Requirement 12.8 applies to all entities in this list.*

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

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

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

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 A2:	☐	☒	☐	☐	☐	☐

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

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.*		April 2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*		May 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:	☐ Yes	☐ No

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

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 2024-05.30)*.
- 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 *(Merchant Company Name)* 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 *(Merchant 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 *(Merchant 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

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

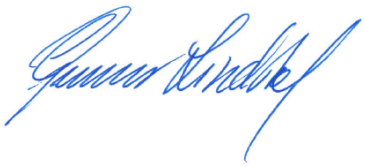
Part 3a. Merchant Acknowledgement

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. Merchant Attestation



Signature of Merchant Executive Officer ↗	Date: 2024-05-30
Merchant Executive Officer Name: Gunnar Lindstøl	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: YYYY-MM-DD
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company ↗	Date: YYYY-MM-DD
Duly Authorized Officer Name:	QSA Company:

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:

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

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 A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.