Payment Card Industry
Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D for Service Providers

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: December 2024

Section 1: Assessment Information

Instructions for Submission

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

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information	
Part 1a. Assessed Entity	
Company name:	Technogym S.p.A.
DBA (doing business as):	Technogym
Company mailing address:	Via Calcinaro 2861, 47521 - Cesena (FC), Italy
Company main website:	www.technogym.com
Company contact name:	Paolo Fiori
Company contact title:	Software Quality Manager – Digital R&D
Contact phone number:	+39 342 6446760
Contact e-mail address:	pfiori@technogym.com
Part 1b. Assessor	
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):	N/A
Qualified Security Assessor	
Company name:	Bl4ckswan S.r.l.
Company mailing address:	Via Vittor Pisani 10, 20124 - Milan (MI), Italy
Company website:	www.bl4ckswan.com
Lead Assessor Name:	Fabio Pacchiarotti
Assessor phone number:	+39 347 4884380
Assessor e-mail address:	fabio.pacchiarotti@bl4ckswan.com
Assessor certificate number:	205-320

Part 2. Executive Summary

Part 2a. Scope Verification

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

Name of service(s) assessed:	MyWellness platform payment services	
Type of service(s) 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): MyWellness platform payment services.		

***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 PCI DSS Assessment (select 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-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:	N/A

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	Technogym is a service provider that develops and manages the MyWellness platform, which includes a payment service that redirects users to a payment page generated and hosted by Stripe, a certified third-party payment gateway. The payment page where customers enter their cardholder data is entirely managed within Stripe's secure infrastructure. Technogym does not store, process, or transmit any cardholder or account data at any point in the transaction flow. All sensitive payment information is captured directly by Stripe, while Technogym only receives non-sensitive transaction metadata (such as payment status or confirmation) needed to complete service delivery.

	No cardholder data is handled or retained in any Technogym system.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Technogym can indirectly impact the security of cardholder data through its role in developing and managing the MyWellness application, which initiates payment requests and communicates with Stripe's APIs to generate secure payment pages. While Technogym never accesses or handles cardholder data, it is responsible for properly integrating Stripe's payment components, ensuring secure API communication, and maintaining application security in order to protect the integrity of the payment flow.
Describe system components that could impact the security of account data.	System components that could impact the security of account data include: - The MyWellness Pay application, which manages the integration with Stripe's APIs and orchestrates the redirection to the payment pages. Although it does not process cardholder data, its configuration ensures the integrity of payment requests. - The MyWellness and Technogym mobile applications, which present the Stripe-generated payment page to the users. - The MyWellness web application interface, which similarly displays the Stripe-hosted payment page. These components do not store, process, or transmit cardholder data themselves, but form the application environment in which the secure Stripe pages are invoked, and therefore contribute to protect the overall payment flow.

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.*	The environment covered by this assessment consists of the MyWellness platform payment services, designed and managed by Technogym. The scope includes the application components and interfaces that interact with Stripe to initiate and display payment pages. Specifically, the environment comprises: - The MyWellness Pay application component (pay.mywellness.com), which interacts with the MyWellness web front-end and the MyWellness and Technogym mobile applications to initiate the payment process, and manages the integration with Stripe's APIs by requesting the generation of Stripe-hosted payment pages to which users are redirected. - The MyWellness and Technogym mobile applications, which implement an embedded webview to load and display the Stripe-generated payment page for the purpose of processing payments. - The MyWellness web interface (pro.mywellness.com), which redirects users to the payment page generated and hosted by Stripe in order to process payments. The applications are developed by the service provider SPOT Software and are managed by Technogym. They are hosted within a dedicated AWS Virtual Private Cloud (VPC) that is logically and physically segregated from other Technogym environments. Applications and services outside this isolated VPC, including corporate networks and development and testing environments, are considered out of scope for this assessment. Network communications involving pro.mywellness.com (the web portal through which users manage and complete purchases) and pay.mywellness.com (used for system-to-system API communications with Stripe) are secured using HTTPS with enforced TLS encryption. None of the in-scope applications or system components store, process, or transmit cardholder data. All sensitive payment information is captured and managed exclusively by Stripe, including any cardholder data storage required for recurring payments.

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

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities—for example, corporate offices, data centers, call centers, and mail rooms—in scope for the PCI DSS 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*
AWS cloud hosted datacenter	1	Dublin, Ireland

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions

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)
-	-	-	-	-

[♦] 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

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 scope of the entity's PCI DSS 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:**
Stripe	- API integration - Generation and hosting of secure payment pages - Payment processing - Storage of cardholder data for recurring payments
Amazon AWS	- Cloud infrastructure services used to host Technogym applications
SPOT Software	- Development and maintenance of the in-scope MyWellness applications

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

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: MyWellness platform payment services

PCI DSS Requirement	**Requirement Responses** *More than one response may be selected for a given requirement. Indicate all responses that apply.*				
	In Place	In Place with CCW	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.	1.3.1, 1.3.2, 1.3.3, 1.4.4, 1.5.1: No CDE is present, as Technogym does not acquire, transmit, store, or process any form of cardholder data. 2.3.1, 2.3.2: No wireless technology is used by Technogym to transmit or receive cardholder data. 3.2.1, 3.3.1, 3.3.1.1, 3.3.1.2, 3.3.1.3, 3.3.2, 3.3.3, 3.4.1, 3.4.2, 3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.3, 3.6.1, 3.6.1.1, 3.6.1.2, 3.6.1.3, 3.6.1.4, 3.7.1, 3.7.2, 3.7.3, 3.7.4, 3.7.5, 3.7.6, 3.7.7, 3.7.8, 3.7.9: No CDE is present, as Technogym does not acquire, transmit, store, or process any form of cardholder data. 4.1.1, 4.1.2, 4.2.1, 4.2.1.1, 4.2.1.2, 4.2.2: No CDE is present, as Technogym does not acquire, transmit, store, or process any form of cardholder data. 6.4.1: This requirement is superseded as of 31 March 2025. 6.4.3: No public-facing application containing payment pages is managed by Technogym. 6.5.5: No CDE is present, as Technogym does not acquire, transmit, store, or process any form of cardholder data. 7.2.6: No CDE is present, as Technogym does not acquire, transmit, store, or process any form of cardholder data. 8.2.3: Technogym does not provide any remote access to customer premises. 8.3.10: This requirement is superseded as of 31 March 2025. 8.4.1, 8.4.2, 8.4.3, 8.5.1: No CDE is present, as Technogym does not acquire, transmit, store, or process any form of cardholder data. 9.1.1, 9.1.2, 9.2.1, 9.2.1.1, 9.2.2, 9.2.3, 9.2.4, 9.3.1, 9.3.1.1, 9.3.2, 9.3.3, 9.3.4, 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7: No CDE is present, as Technogym does not acquire, transmit, store, or process any form of cardholder data. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3: No POI devices are used by Technogym. 10.2.1.1: No CDE is present, as Technogym does not acquire, transmit, store, or process any form of cardholder data. 10.7.1: This requirement is superseded as of 31 March 2025. 11.2.1, 11.2.2: No wireless technology is used, as the in-scope system components are hosted by the AWS cloud infrastructure. 11.4.7: Technogym is not a multi-tenant service provider. 11.6.1: No public-facing application containing payment pages is managed by Technogym. 12.7.1: No CDE is present, as Technogym does not acquire, transmit, store, or process any form of cardholder data. A1.1.1, A1.1.2, A1.1.3, A1.1.4, A1.2.1, A1.2.2, A1.2.3: Technogym is not a multi-tenant service provider. A2.1.1, A2.1.2, A2.1.3: Technogym does not manage POS POI devices.

For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/A

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2025-12-19
Were any requirements in the SAQ 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 SAQ D (Section 2), dated (Self-assessment completion date *2025-12-19***).**

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

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

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

Based on the results documented in the SAQ D 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 SAQ are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *Technogym* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.
□	**Non-Compliant:** Not all sections of the PCI DSS SAQ 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 the PCI DSS requirements included in this SAQ. **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 PCI DSS SAQ 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 1) In Place, 2) In Place with CCW, or 3) 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 included in this SAQ 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 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	*PCI DSS Self-Assessment Questionnaire D, Version 4.0.1,* was completed according to the instructions therein.
☒	All information within the above-referenced SAQ and in this attestation fairly represents the results of the entity's 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

Firmato digitalmente da PIERLUIGI ALESSANDRI C: IT

Signature of Service Provider Executive Officer ↑	*Date:* 2025-12-19
Service Provider Executive Officer Name: **Pierluigi Alessandri**	*Title:* **Vicepresidente**

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: *Bl4ckswan performed a top-down analysis of Technogym services to confirm and validate the PCI DSS scope as defined by the client. The QSA clarified the purpose and intent of each PCI DSS requirement, explained their relevance within the Technogym context, and verified the consistency and adequacy of Technogym procedures and IT system configurations against the standard. No audits were conducted as part of the QSA engagement beyond a documentation review to evaluate the consistency and adequacy of Technogym's current processes and procedures.*

Signature of Lead QSA ↑	*Date: 2025-12-19*
Lead QSA Name: **Fabio Pacchiarotti**	

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 2025-12-19*
Duly Authorized Officer Name: **Francesco Morini**	*QSA Company:* **Bl4ckswan S.r.l.**

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 a Non-Compliant status 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 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 its program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/.*