Personify-Client Matrix of Shared PCI Responsibility

Wild Apricot

Personify

January 2025

Table of Contents

Purpose

Maintaining Payment Card Industry Data Security Standards (PCI DSS) is a responsibility shared between Personify and our Clients. The purpose of this document is to delineate those responsibilities belonging to Personify from those belonging to you, our Client.

Payment Card Industry Data Security Standard Requirements

Table 1, below, provides a matrix of the individual requirements set forth in the Payment Card Industry Data Security Standard v4.0.1 and which organization is responsible (Personify or Client) for each line item.

General PCI DSS Requirements

PCI DSS Requirement	Personify	Client
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 of Systems and Networks Regularly.	✓	✓
12. Support Information Security with Organizational Policies and Programs	✓	✓

Requirement Details

1. Install and Maintain Network Security Controls.

Servers hosted in Personify's private cloud and server instances hosted in Personify's public cloud environment are maintained by Personify. The network supporting these servers is also maintained by Personify. These separate network environments have stateful firewalls at Internet border ingress/egress and utilize micro segmentation, also known as Distributed Firewall, technologies to control connectivity inside the network.

2. Apply Secure Configurations to All System Components.

Personify is responsible for account security and passwords on devices and applications owned and operated by Personify. This includes ensuring no default password or other vendor default settings are used. The WA application is provided by Personify as a service for Customers. Clients create an account when first signing up for the service and are responsible for ensuring proper account protection practices are followed, including provisioning accounts for each unique user, as well as maintaining strong passwords and utilizing MFA.

3. Protect Stored Account Data.

The WA application is not designed to nor does it store cardholder data as defined by the PCI council.

4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.

Personify is responsible for configuring servers and websites to use strong cryptography. Personify is responsible for configuring the WA hosted application to use strong cryptography.

5. Protect All Systems and Networks from Malicious Software.

Personify is responsible for maintaining and updating anti-malware mechanisms on the hosted application servers, including performing regular antimalware scanning, receiving and responding to alerts, and resolving incidents.

6. Develop and Maintain Secure Systems and Software.

Personify is responsible for secure development and deployment of the WA application and the related system components. This includes ensuring that all system components have all appropriate software patches, as well as applying software lifecycle (SLC) processes and secure coding techniques.

7. Restrict Access to System Components and Cardholder Data by Business Need to Know.

Personify is responsible for controlling access to all system components hosted within the Personify cloud environments, the authorization of access requests, and granting an appropriate level of access based on level of need.

8. Identify Users and Authenticate Access to System Components.

Personify is responsible for user and process identification and authentication procedures and protocols for all backend access to system components. The Client is responsible for creating and using individualized accounts for anyone accessing their WA services, as well as appropriately maintaining their accounts.

9. Restrict Physical Access to Cardholder Data.

This responsibility is formally delegated to our payment gateway providers. Personify is responsible for monitoring PCI compliance of hosting and gateway providers, and documenting that they acknowledge that they are providing coverage for PCI DSS Requirement 9. Wherever Client takes in-person card payments from their constituents, Client is responsible for ensuring secure handling of cardholder data.

10. Log and Monitor All Access to System Components and Cardholder Data.

Personify is responsible for logging and monitoring usage on all system components. Personify is responsible for alert monitoring, log review, and incident response to log events.

11. Test Security of Systems and Networks Regularly.

Personify is responsible for regularly testing the security of our systems and networks, including all WA-provided widgets and editing tools. This includes penetration testing, vulnerability scanning, and segmentation verification. Personify contracts with a PCI Council Approved Scanning Vendor (ASV) to perform regular network scans. Personify regularly performs additional tests such as incident response testing, and any network intrusions, unexpected files changes, or unauthorized changes to payment pages are detected and responded to. Due to the nature of WA and its customizability, it is recommended that clients test any customizations made outside the scope of provided widgets and editing tools. Clients may reach out to WA support for more information if they intend to execute their own tests against their WA site(s).

12. Support Information Security with Organizational Policies and Programs.

Personify maintains an internal Policies and Procedures document guiding our implementation of PCI DSS requirements. This document is distributed to all Personify personnel to ensure they are aware of the sensitivity of cardholder data and their responsibilities for protecting it. We maintain that our Third Party Service Providers (TPSPs) are also compliant to PCI DSS requirements we trust to them. It is the responsibility of our clients to ensure that their TPSPs (including Personify) are properly engaged, and that they maintain PCI DSS compliance.

SAQ-A Requirements

Requirement	Defined Approach	Personify	Client	Comments
2.2.2	Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	✓	✓	Wild Apricot does not provide a “Vendor default” account. Personify is responsible for removing, disabling or changing default vendor accounts in their environment. Personify customers are responsible for removing, disabling or changing default vendor accounts in their environment. Customers are not provided with default accounts.
3.1.1	All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	✓	✓	Personify is responsible for ensuring that their policies and procedures are documented, up to date and made known to all affected parties. Personify customers are responsible for ensuring that their policies and procedures are documented, up to date and made known to all affected parties.
3.2.1	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that define length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.		✓	Wild Apricot does not store account data. Personify does not store account data. Personify customers are responsible for maintaining data retention and deletion policy and procedures towards CHD transmitted or stored within their CDE.

Requirement	Defined Approach	Personify	Client	Comments
	• A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.			
6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	✓		Personify is responsible for maintaining and implementing a process to identify security vulnerabilities and assign risk rankings. Personify customers are responsible for reporting confirmed findings to Personify.
6.3.3	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	✓		Personify is responsible for ensuring system assets are protected against known vulnerabilities by installing applicable vendor patches.
6.4.3	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary.	✓		Personify is responsible for maintaining a secure software development program to support their assets that may impact the CDE. Personify is responsible for maintaining scripts loaded and executed as part of the payment page.
8.2.1	All users are assigned a unique ID before access to system components or cardholder data is allowed.	✓	✓	Wild Apricot allows for the creation of unique users with unique IDs. Personify is responsible for implementing and monitoring user identification controls, assigning unique user IDs. Personify customers are responsible for

Requirement	Defined Approach	Personify	Client	Comments
				implementing and monitoring user identification controls, assigning unique user IDs.
8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary, on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	✓	✓	Wild Apricot allows for the creation of unique users with unique IDs and does not recommend sharing accounts. Personify is responsible for implementing and monitoring user identification controls, assigning unique user IDs. Personify customers are responsible for implementing and monitoring user identification controls, assigning unique user IDs.
8.2.5	Access for terminated users is immediately revoked.	✓	✓	Personify is responsible for implementing and monitoring user identification controls, revoking user access when no longer necessary. Personify customers are responsible for implementing and monitoring user identification controls, revoking user access when no longer necessary.
8.3.1	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric element.	✓	✓	Wild Apricot provides customers with the ability to utilize MFA. Personify is responsible for implementing and monitoring user identification controls, assigning multi-factor authentication mechanisms. Personify customers are responsible for implementing and monitoring user identification controls, assigning multi-factor authentication mechanisms.

Requirement	Defined Approach	Personify	Client	Comments
8.3.5	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.	✓	✓	Wild Apricot enforces new password creation for new accounts. Personify is responsible for maintaining user identification controls. Personify customers are responsible for maintaining user identification controls.
8.3.6	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.	✓	✓	Passwords to access the Wild Apricot frontend require: • A minimum length of 12 characters • numeric, alphabetic, and special characters Personify is responsible for maintaining a password policy compliant with PCI DSS requirements. Personify customers are responsible for maintaining a password policy compliant with PCI DSS requirements.
8.3.7	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	✓	✓	Wild Apricot enforces a password history of 4. Personify is responsible for maintaining a password policy compliant with PCI DSS requirements. Personify customers are responsible for maintaining a password policy compliant with PCI DSS requirements.
8.3.9	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	✓	✓	Wild Apricot enforces 365-day password reset requirements and provides the option to utilize MFA. Personify is responsible for maintaining a password policy compliant with PCI DSS requirements.

Requirement	Defined Approach	Personify	Client	Comments
				Personify customers are responsible for maintaining a password policy compliant with PCI DSS requirements.
9.4.1	All media with cardholder data is physically secured.		✓	Personify does not store cardholder data. Personify customers are responsible for storage of media in their own CDE, if applicable.
9.4.1.1	Offline media backups with cardholder data are stored in a secure location.		✓	See 9.4.1
9.4.1.2	The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.		✓	See 9.4.1
9.4.2	All media with cardholder data is classified in accordance with the sensitivity of the data.		✓	See 9.4.1
9.4.3	Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.		✓	See 9.4.1
9.4.4	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).		✓	See 9.4.1
9.4.6	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.		✓	See 9.4.1
11.3.2	External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	✓	✓	Personify contracts an ASV to perform quarterly external vulnerability scans against the standard pages and widgets available to customers. Personify customers are responsible for performing external vulnerability scans against any customizations not supported by Wild Apricot.

Requirement	Defined Approach	Personify	Client	Comments
11.3.2.1	External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	✓		Personify performs regular external vulnerability scans against the standard pages and widgets available to customers.
11.6.1	A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	✓	✓	Wild Apricot provides a payment page option. Personify is responsible for maintaining change- and tamper- detection for the provided payment page. Personify customers are responsible for any alternative payment pages used.
12.8.1	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	✓	✓	Personify monitors their TPSPs for PCI compliance. Personify customers are responsible for monitoring PCI compliance for service providers with whom cardholder data is shared.
12.8.2	Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	✓	✓	Personify maintains agreements with their TPSPs. Personify customers are responsible for maintaining agreements with their own service providers.
12.8.3	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	✓	✓	Personify maintains established processes, including following due diligence with TPSP. Personify customers maintain established processes, including following due diligence with their TPSP.
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	✓	✓	Personify monitors their TPSPs for PCI compliance.

Requirement	Defined Approach	Personify	Client	Comments
				Personify customers are responsible for monitoring PCI compliance for service providers with whom cardholder data is shared.
12.8.5	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	✓	✓	Personify is responsible for maintaining information on PCI requirements and responsibilities managed by their service providers and those that are shared. Personify customers are responsible for maintaining information on PCI requirements and responsibilities managed by Personify and any other service provider.
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	✓	✓	Personify is responsible for maintaining incident response policies and processes supporting their applications and infrastructure. Personify customers are responsible to maintain incident response policies and processes for their own business.