Publishing Concepts General Data Protection Regulation Compliance Overview

Overview

This document outlines how Publishing Concepts LP, (PCI) complies with the European Union General Data Protection Regulation (GDPR).

PCI's data protection program safeguards Personal Data (defined below) according to the GDPR requirements. This document outlines the program elements pursuant to which PCI intends to:

- Ensure the security and confidentiality of Personal Data
- Protect against any anticipated threats or hazards to the security of Personal Data, and
- Protect against the unauthorized access or use of Personal Data in ways that could result in substantial harm to PCI's clients and their respective constituents

PCI takes data security matters seriously and as custodians of your data, we are devoted to matters of privacy, security and transparency. You can read our privacy policy at this link: PublishingConcepts.com/default.aspx?page=PrivacyPolicy.

Network Design and Perimeter Protection

Publishing Concepts' (PCI) network consists of four physical locations – the PCI corporate environment and the PCI Datacenter facility located at the QTS DFW1 Datacenter, Irving TX. Two branch offices are also maintained: one in Virginia Beach, VA and one in San Antonio, TX. The QTS Datacenter location acts as the network hub, while the three remaining locations connect via Private Metro Ethernet.

Cisco Firewall appliances provide Outside, DMZ and internal LAN sub-networks. External application interfaces, i.e. web servers and SFTP servers, reside within the DMZ. Client secure databases reside within the internal network. The DMZ is allowed access to secure databases via PCI controlled applications on strict port rules. The DMZ is also secured from the public Internet via strict port access rules.

System Hardening

Software firewalls are utilized on applicable systems in addition to the already mentioned network level firewalls. Unneeded services are disabled and default vendor passwords are removed/changed out of the box.

Storage of Sensitive Data

Production data is secured on the internal network and access is granted on the principal of least privilege. All backups are stored in an industry-leading cloud based system. PCI will maintain a production copy of biographical information for up to six months after project completion. This is necessary to deal with post-production tasks. PCI will maintain minimal order information indefinitely for buyers, which can include name, address, phone and email. The electronic version of the published uses 448-bit Blowfish encryption to obfuscate Personally Identifiable Information.

Encryption of Data in Transit

Sensitive data leaving or entering the PCI network is encrypted. All PCI web based applications for data entry and reporting are accessed over TLS 1.2. Batch data is transferred via industry standard SSH either through public/private key authentication or standard interactive authentication.

IT Security/Secured Systems

ESET's Deslock (remote lock/wipe, remote access, device full encryption) for all associates who have access to databases

ESET Antivirus software installed on all employee computers with regular updates.

Anti-virus software is deployed throughout the enterprise on all user machines and servers, where applicable. Anti-virus/malware application also provides safe internet browsing. Email entering the network is scanned for SPAM, Phishing and malware.

Vulnerability scans are completed on a quarterly basis via 3rd party organizations. Penetration testing is completed on an annual basis via 3rd party organizations.

Software Development

All PCI production systems are patched on a monthly basis and out of band critical patches will be applied as needed. Desktops automatically apply patches per policy. Code is reviewed for accuracy, security, and performance on all changes and the software development life cycle is maintained in three environments:

- Development - located at the PCI Datacenter and includes source control and build machines to which developers have full access.
- Staging – located at PCI Datacenter. Staging provides a production-like environment for clients and PCI to review and test pending code changes. Developers have limited access.
- Production – located at PCI Datacenter. This is a pure production environment in which developers have read-access only.

Physical Access Security

PCI Server room access is limited to only the Manager of Information Technology and specified network engineers and officers of the company.

PCI has its own dedicated physical cabinets within the QTS Datacenter. Access to co-location facility/cabinets is limited to designated network engineers and officers of the company and the Executive Director of Information Technology. Access to the QTS data center is restricted by two factor authentication barriers plus continually monitored closed-circuit cameras trained on all entrances and common areas 24x7x365. Unauthorized access prevention measures also include - Northern Proximity security badge entry/exit on all doors, fingerprint scanners, retina scanners, and motion sensitive cameras throughout all facilities.

Access Control and User Management includes:

- All PCI associates are granted permissions based on the principle of least privilege and are assigned a unique ID
- Access to PCI's main office is controlled by keycard
- No guests are allowed in secured areas without signing in
- No guests are allowed unescorted access to any PCI office areas
- Associates are trained to secure any equipment not in use
- Secure passcodes are required on any equipment that has access to secure information
- Password-protected screensavers are required on computers when staff leave their computers unattended in the office
- Password Storage must be via secured systems; PCI uses LastPass for secure credential storage and is accessible only to site administrators

PCI reviews access lists monthly.

Information Security Policy

PCI's official information security policy is on file internally. All associates are required to sign an Acceptable Use Policy and other specialized policies depending on the job description. Extensive background checks are completed for all potential associates prior to date of hire.

Security Training

Security awareness training is provided to all staff during the onboarding process with supplemental training provided semi-annually.

PCI DSS

PCI contracts with Digital Defense for quarterly external scans. PCI requires that all credit card transactions go through a reputable and PCI DSS compliant online gateway in real time. PCI does not store credit card numbers to be processed manually by the client at a later date. Proof of PCI DSS compliance can be requested through Compliance@publishingconcepts.com.

Availability

All production systems are located at a PCI datacenter which provides infrastructure redundancy in regards to power, connectivity, etc. PCI uses a series of hot and warm redundant hardware in the event of equipment failure. Backups are performed daily using a secure cloud based platform. System maintenance and code upgrades are performed during off peak hours. Clients are notified in advance of maintenance needed during off peak hours.

Disaster Recovery Plan

PCI has a disaster recovery plan in place that utilizes log shipping of our databases. In the event of a full failure, we can restore services within a 24-hour period from our remote datacenter QTS. During this time necessary associates have been equipped with remote access and are trained how to work remotely from home or other safe environment with secure access the network.

Vulnerability Management

PCI utilizes multiple tools to alert the appropriate team members of vulnerabilities via distribution groups. Tools utilized include but are not limited to Digital Defense Inc. IDS/IPS, ZScalar, and SolarWinds LEM.

Data Breach Notifications

In the event that a data breach is suspected, PCI has developed and implemented a data breach policy that outlines and provides guidance to employees and contractors on the appropriate processes for reporting the event. Default action for any suspected breach is to report immediately to the Information Security Officer/Computer Emergency Response Team. Once escalated, a risk analysis of all suspected breach points and data will be completed to determine mitigation and remediation actions to be taken.

In the event of unauthorized access to client data, PCI will immediately notify the effected client(s) per state and federal laws.

Key GDPR Requirement	**PCI Capabilities**
Encryption-at-rest of Personal Data	PCI uses encryption transparent to applications provided by column-level encryption and driver-level encryption.
Encryption-in-transit of Personal Data	All data is encrypted in transit, both to our servers, server-to-server, and server-to-end users.
Data Mapping/Data Inventory	As a processor of our clients' constituent data, we store personal information on individuals passed on to us via a securely uploaded file provided by our clients, or

	entered into our CRM application by the client or individual. Personal information (listed below) is for the purposes of a) validating the information on file with the organization is up-to-date and b) inclusion in the physical and digital publications. The client defines the data that is to be printed in the book on a field-by- field basis. PCI provides the opportunity to the individual to opt out of the publication, omit certain fields from inclusion, and remove information from their record all together, provided the individual contacts PCI prior to the publication's deadline. PI includes name, phone numbers, addresses, email addresses, job title, spouse/partner name, children names, and date of birth. For projects in the educational market, PCI also stores and prints class years and degrees. Military association projects can include awards, conflicts served. For projects in the educational market, PCI also stores and prints class years and degrees. Military association projects can include awards, conflicts served. In certain projects, PCI allows the individual to provide photos and narrative text for inclusion in the publication. Photo and narratives are opt-in only fields, with all the content provided by the user. All contact related personal information used by PCI in the marketing phases of the project is to make outreach to the constituents and can include email, phone, and mailing address channels. PCI uses personal information in its predictive analytic models to identify marketing outreach.
Individual's Right – Data Retention	PCI provides a portal where clients can remove data on a constituent when they decide it is necessary.
Data Backups	PCI keeps data backups for a 5-day period.
Privacy by Design	PCI's development processes include data privacy reviews during architecture, design, implementation, and testing.
Individual's Right – Update Data	Individual users can update profile data via the self-update site, unless the project is published and thereby considered finished.

Individual's Right – Data Portability	Clients can request PCI provide the data stored on a constituent by sending their account manager the ID of the record.
Individual's Right – Commonly Used Format	Clients can request PCI provide a .pdf document of the data stored on a constituent by sending their account manager the ID of the record.
Individual's Right – Erasure	PCI provides a portal where clients can stop further marketing outreach and remove records from inclusion in the printed publication. In addition, clients can request PCI perform a full deletion of a constituent's record by sending their account manager the ID of the record to remove.
Individual's Right – Consent	PCI provides functionality to require consent to a terms and conditions screen before using the self-update site.
Cookies Consent	Upon login to the self-update site, users are notified that PCI uses cookies to maintain their logged in state.

Contact Us

For all inquiries, please contact your Account Manager if you are a current client, or alternatively, you can contact our Information Security Officer:

David Smith

4835 Lyndon B Johnson Freeway

Suite 1100

Dallas, TX 75244

informationsecurity@publishingconcepts.com