PCM UK GDPR Compliance Documentation	**Asset ID**	
	Document Name	PCM GDPR Compliance Statement
	Revision	v1.2
	Date	01/03/2018
	Document Owner	Kyle Tackley
	Document Author	Kyle Tackley
	Document Classification	External

PCM GDPR Compliance Statement

Introduction: The *EU General Data Protection Regulation ("GDPR")* comes into force across the European Union on 25th May 2018 and brings with it significant changes to data protection law. The new Regulation aims to standardise data protection laws and the processing of Personal Data (as defined under the applicable laws implementing the Data Protection Directive 95/46/EC as amended or replaced from time to time or equivalent legislation in other countries ("Data Protection Laws")) across the European Union (the "EU"), thus affording individuals stronger, more consistent rights to access and control their Personal Data.

Our commitment: We are committed to having security measures and procedures in place designed to protect the Personal Data we process. We have always had a data protection program in place which complies with existing law and abides by the then current data protection principles. We, therefore, recognise our obligation and have taken appropriate measures to update and expand our data protection program to meet the additional requirements of the GDPR for the protection of Personal Data we process.

Framework: PCM UK has implemented a proprietary GDPR Privacy Management Framework that ensures that all stakeholders processing Personal Data (1) adhere to the on-going compliance obligations required under the GDPR and (2) manage Personal Data in accordance with accepted industry standards, including ISO 27001 and PCI-DSS. This framework has been approved at the PCM Board level so to ensure there is an organization-wide approach in place to implement this framework, particularly in our data protection programme.

Programme: PCM UK's GDPR Privacy Programme Framework focuses on the following core areas in designing its data protection programme:

- Accountability & Governance
- Data Discovery, Data Flow Mapping and Information Life Cycle Management
- Third Party, Supply Chain and Outsourcing Arrangements
- Data Breach Detection, Defence & Response
- Data Privacy by Design (DPbD) & Data Privacy Impact Assessments (DPIA)
- Awareness, Training & Communications
- GDPR Principles including on-going Audit & Assurance
- Rights of Data Subjects

Project Plan: We already have security measures in place across our organisation to protect the Personal Data we process, and we are on track to be in an acceptable state of GDPR compliance by 25th of May 2018. Our project plan to be in an acceptable state for GDPR compliance, which has been underway since August 2017, includes:

- ***Information Audit*** – undertaking a company-wide information audit to identify and assess what Personal Data we hold, where it comes from, and how and why it is processed.
- ***Policies & Procedures –*** revising data protection policies and procedures to meet the requirements and standards of the GDPR.
- ***Data Protection* and Data Privacy Policy** – implementing a policy that drives up accountability and governance measures for all stakeholders, with a key emphasis on privacy by design and the rights of individuals.
- ***Data Retention & Erasure*** – updating our retention policy to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that Personal Data is stored, archived and destroyed compliantly. We will have erasure procedures in place to meet the new *'Right to Erasure'* obligation and will be poised to respond to other data subject's rights, along with any exemptions, response timeframes and notification responsibilities.
- ***Data Breaches*** – implementing safeguards and measures designed to identify, assess, investigate and report any Personal Data breach at the earliest possible time.
- ***International Data Transfers & Third-Party Disclosures*** – where we store or transfer Personal Data outside the EU, having international data transfer mechanisms in place designed to secure, encrypt and maintain the integrity of the data.
- ***Subject Access Request (SAR)*** – revising our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for doing so free of charge.
- ***Legal Basis for Processing*** –reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- ***Privacy Notice/Policy*** – revising our Privacy Notice(s) to comply with the GDPR so that all individuals whose Personal Data we process are informed of why we need their Personal Data, how their Personal Data is used, what their rights are, who their Personal Data is disclosed to, and what safeguarding measures are in place to protect their Personal Data.
- ***Obtaining Consent for Marketing Activities*** –developing stringent processes for recording an individual's consent to certain marketing activities; making sure that we can evidence an affirmative opt-in including time and date records of such opt-in; and having in place an easy to see and access-way for individuals to withdraw their opt-in consent at any time.
- ***Direct Marketing*** – revising the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions, a clear notice and method for opting out, and the provision of unsubscribe features on all subsequent marketing materials.
- ***Processor Agreements*** – where we use any third-party to process Personal Data on our behalf (including, but not limited to, Payroll, Recruitment, and Payment Processing), drafting compliant Processor Agreements and due diligence procedures for ensuring that they as well as we meet and understand their and our GDPR obligations.

- ***Data Subject Rights*** **–** In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, providing an individual easy to access information via our website of an individual's right to (1) access any Personal Data that we process about them and (2) request information pertaining to their rights as Data Subjects (as defined under the Data Protection Laws).

Information Security, Technical and Organisational Measures

We take the privacy and security of individuals and their Personal Data very seriously and take reasonable measures and precautions to protect and secure the Personal Data that we process. To that end, we have information security policies and procedures in place designed to protect Personal Data from unauthorised access, alteration, disclosure or destruction. We also have the required security measures in place, including, but not limited to, an implementation of the ISMS / ISO 27001:2013 certification.

GDPR Roles and Employees

We understand that continuous employee awareness and understanding is vital to our continued compliance with the GDPR's requirements, and to that end we have involved our employees in our preparation plans by implementing an employee training program specific to the GDPR. We will provide this training to our existing employees prior to May 25, 2018 and will incorporate this training into our induction process and annual training program.

Work with External EU Privacy and GDPR Experts

We recognize the importance of GDPR and work hand in hand with leading GDPR consulting firms and advisors to validate our programme and ensure our policies and procedures for data protection are aligned with those recommended by the Information Commissioner's Office and other related governing organizations for the protection of Personal Data.

If you have any further questions about our GDPR compliance, please contact our Data Protection Officer, Kyle Tackley (kyle.tackley@pcm.com).