PMS Ltd GDPR Statement v1.1 Document Draft

Introduction

The EU General Data Protection Regulation (GDPR) came into force on 25th May 2018 which impacts on every organisation which processes personal data of EU citizens. It introduces new responsibilities, empowers businesses to be accountable for their processing of personal data as well as enabling EU citizens to protect their privacy and control the way their data is processed. Even though the UK due to leave the European Union, the GDPR will still apply and will replace the UK's Data Protection Act 1998.

Data protection definitions

Personal data: is any information that relates to a living individual. It also includes any data that can be used with other sets of data to identify an individual. Typical examples of personal data are: name, identification number, location data, online identifier, email address, etc.

Data Processing: relates to any operation carried out on personal data including collection, recording, organising, structuring, storing, using, etc. Processing also doesn't have to be by automated means which means that processing includes paper-based, non-digital systems.

A Data Subject: is the individual whose personal data is being processed.

A Data Controller: is the organisation which determines how personal data is processed.

A Data Processor: is an organisation which processes data on behalf of a Controller. This typically means a third party who is used by the Controller to process their data (such as, a marketing company used to send out marketing materials).

For detailed information about GDPR and data protection, visit the Information Commissioner's Office website:https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Your GDPR responsibilities

When you use our services to store or process your personal data (including customer's or user's data), you are the Data Controller and we are a Data Processor. This will be true for any personal data you place in our application and on our servers either directly, via a hosted website or by use of any of our other services, meetings, training or seminars.

The GDPR requires you, as a Data Controller, to ensure that any Data Processor services you use to process personal data are GDPR compliant. This means that when you use any of our services to process your personal data you need to carry out due diligence on our services and ensure certain contractual terms are in place.

PMS Ltd GDPR Statement v1.1 Document Draft

This GDPR statement is our way of helping you meet these GDPR regulatory requirements and to offer you assurance that we take GDPR and the security of your personal data as part of the everyday running of our services.

Our GDPR commitment

As a UK company, PMS Ltd is committed to ensuring our business, services and internal processes are GDPR compliant. As such, this GDPR Statement provides our assurances to GDPR compliance.

We will have put in place:

- Updated internal policies relating to data protection and responsibilities within our businesses for ongoing GDPR compliance
- Check all our systems, processes and services to ensure they meet the requirements of GDPR, particularly around security of data and our use of any external third party services
- Processes to ensure ongoing GDPR compliance
- Updated terms and conditions of services that meet the contractual requirements of GDPR in the Data Controller – Data Processor relationship

Our services are compliant because:

- We have fully assessed our own GDPR compliance both in terms of the services we offer to our customers and in terms of our own internal policies and procedures
- We have appropriate technical and personnel protocols in place to ensure the security of your data
- We carry out due diligence against any sub-processors or other third party processors we use to ensure their GDPR compliance (such as data centres)
- We only allow specific members of staff access to the admin level of our application service and what access that is available, is limited to specific circumstances
- As our services are hosted in the UK and backed up in the U.S.A. and as such, we are registered with the EU-US Privacy Shield framework
- Our staff are trained in GDPR compliance and understand their responsibilities for managing the systems that process your personal data

Our role as a Data Processor

You are the owner of the data you submit to our services (whether they are hosted on your premises or in our application and on our servers).

When your data is placed in our software application you are the Data Controller and PMS Ltd, the Data Processor. We do not access the data you store in our application service and any processing (as a Data Processor) is only in terms of the hosting services we provide to you. Should we wish to access your data, to help improve our service or your project delivery performance, we will do so, only with your permission. We do not use your data for any processing of our own.

We do not share or provide access to any of your data with third parties unless requested by you, or required to do so by law. Where law enforcement or other authorised parties request access to our servers, we follow strict internal policies for dealing with such requests in line with existing UK and U.S.A. law. Furthermore, the third parties are required to demonstrate they have a lawful reason to access the data and under what authority.

Data location

Your data is stored in our software application on servers provided by AWS. This hardware is co-located, in the UK, at the AWS London data centre with backups stored in the USA.

Security

Maintaining security

Our personnel keep up to date with all technical aspects of security and ensure the ongoing security of our software application service. This means we always have data protection and privacy in mind when introducing new developments to the software application which includes:

- Encryption of personal data
- Ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services
- Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing

Maintaining security

AWS has in place effective technical and organizational measures for data processors to secure personal data in accordance with the GDPR. Security remains a highest priority, and AWS continue to innovate and invest in a high bar for security and compliance across all global operations. AWS industry-leading functionality provides the foundation for a long list of internationally-recognized certifications and accreditations, demonstrating compliance with rigorous international standards, such as ISO 27001 for technical measures, ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1, and EU-specific certifications such as BSI's Common Cloud Computing Controls Catalogue (C5).

Access to servers

AWS do not permit third party access to its servers. Data centre staff have physical access to the servers, but have strict protocols in place to ensure they only do so, if requested by a member of AWS technical support team and such a request will only be in cases when they need to carry out a visual check of a server or carry out physical maintenance on the server itself.

PMS Ltd Personnel

PMS Ltd Personnel are trained and made aware of their responsibilities under GDPR. This includes their responsibilities with regards to access, security and processing of any personal data stored on our software application.

Third party services

Other than the data centres who host our software application, PMS Ltd does not use any third party suppliers or services that would have access to, or process, any data you process in our software application service.

Strict protocols (as set out above) are in place regarding data centre staff and access to servers. The data centres we use hold ISO 27001 certification and have high security access controls.

Changes to our approach

Should our approach to any aspect covered by this statement change we will make sure, where your data is impacted, that we notify you within a reasonable timeframe and in line with any contractual terms in place between us.

Data breaches

In the unlikely event of a breach occurring (as defined in the GDPR) we will notify you within 48 hours of the breach coming to our attention. This will be enough time for you to consider your requirements, under GDPR, for reporting the breach to the Information Commissioner's Office (ICO), and Data Subjects.

We help you to comply with GDPR

Our approach to our own compliance also helps you comply with your own GDPR compliance requirements. This statement should go some way to explain our approach to GDPR compliance. By using our services, you can be assured that your use is GDPR compliant.

Furthermore, if required we will assist you or the Information Commissioner's Office with any query relating to the GDPR compliance of our services.

Data protection contact

Any questions, queries or requests for further information regarding our GDPR compliance should be sent to David Douglas, Project Management Software Limited, 11/12 Hallmark Trading Centre, Fourth Way, Wembley HA9 0LB.

Our email: info@ezps.co.uk

Last Updated: 07.10.23