Qualsys GDPR compliance statement

Qualsys

Qualsys welcomes the GDPR. The success of our company builds on the trust that our customers, employees and other stakeholders have in our ability to deliver premier quality in all areas of our business.

Our software reduces compliance burden associated with regulations and standards:

ISO

GxP QUALITY SYSTEMS

FDA 21 CFR Part 11

MHRA Regulating Medicines and Medical Devices

1.

Introduction

The GDPR compliance journey

After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016. Enforcement date: 25 May 2018 - at which time those organisations in non-compliance may face heavy fines.

Many of the GDPR's main concepts and principles are much the same as those in the Data Protection Act. There are new elements, enhancements, a greater emphasis on accountability, and how organisations demonstrate their compliance.

Like the DPA, the GDPR applies to 'personal data'. However, the GDPR of personal data is more detailed. For example, online identifiers such as IP addresses, are considered personal data. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data. The GDPR refers to sensitive personal data as "special categories of personal data". These categories are broadly the same as those in the DPA, but there are some minor changes, e.g. the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

The GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the DPA – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf.

Qualsys is acutely aware of its role in providing the right tools and processes to support its users and customers to meet their GDPR mandates.

All Qualsys staff are currently required to sign DPA statements when they join the company and the importance of handling personal and sensitive data is embedded in Qualsys culture. Customer's systems are only accessed on a needs basis for Support and Maintenance purposes and this is all carried out in a strictly controlled manner that is line with both the GDPR and ISO 27001 principals. From a customer's data perspective (such as Account Information), all personal and sensitive data is held in systems with strict access controls by dedicated staff on a needs basis.

As our Quality Manager and IG Lead, Kate Armitage has been designated as the Data Protection Officer and as such takes responsibility for data protection compliance and the management of any security breaches.

Qualsys have are undergoing a programme of activities to ensure that we are ready for the GDPR changes. This include but are not limited to:

- Staff Awareness and Training Programmes
- Full Review and Gap Analysis of data held and how it is processed
- Full review of policies, processes and procedures to ensure they cover GDPR changes
- EQMS product review and enhancements

2.

Our Commitment

Our customer's data is of key importance.

Qualsys are registered with the ICO and have always honoured their customers' right to data privacy and protection in accordance with the requirements covered by the ICO. Qualsys have no necessity to collect and process their customers' personal information beyond what is required for the functioning of their services.

It should be noted that Qualsys utilise a 3rd Party Hosting Provider for all customer hosted solutions. Pipe Ten have demonstrated their commitment to data privacy and protection by operating to PCI DSS industry standards, achieving Cyber Essentials certification and are currently in the final process of achieving ISO 27001 certification.

Pipe Ten and Qualsys have always had strong privacy policies in place which are being adjusted to incorporate GDPR obligations and recognise that GDPR will help us move towards the highest standards of operations in protecting personal data.

For more information on Pipe Ten please refer to https://www.pipeten.com/

How have Qualsys prepared for GDPR?

At Qualsys we understand our obligation to our customers and their personal data. We have thoroughly analysed the GDPR requirements and are working through several initiatives to ensure that we are only holding the minimum information required to provide the contracted services to our customers, that we allow customers to manage the data that is held and easily be able to provide access to the data and removal wherever possible.

These include:

Pseudonymization and encryption:

Qualsys encryption and pseudonymization processes include:

- Transport encryption via HTTPS to the application itself
- Encryption of data media – Backups – AES256
- Secure remote access and maintenance for Support and Maintenance purposes. This is limited to authorised personnel for limited periods of time.

Confidentiality

Qualsys ensure confidentiality of data by the following means:

- Information Security Process that covers several data governance initiatives such as data control aspects, physical access control, access management and password policies.
- All staff are expected to sign confidentiality agreements on joining the company and these are regularly reviewed.
- There is limited access to customer systems by personnel who are trained, competent and reliable.
- There are clearly defined roles and responsibilities within Qualsys, maintained via QRR (Qualsys Roles and Responsibilities).
- Clear definition of IG and GDPR obligations in Job Descriptions and Contracts.
- Specified communication protocols which are defined in the Communications Strategy.
- All new developments and major business change are subject to Privacy by Design.
- Development and Production environments are separated.
- All hosted solutions are in a 27001 certified Data Centre
- Defined retention periods.
- Subject Access Request Process
- Data Disposal and Extraction Process
- Antivirus and Antimalware solutions in place

- Clearly defined Information Asset Register
- Clearly defined Data Processing Register

Integrity

In addition to the above Qualsys ensure Integrity data by the following means:

- Restriction of writing and modification permissions
- Use of password confirmations and electronic signatures where appropriate
- Documented assignment of rights and roles
- Defined GDPR processes including retention.

Availability and Resilience

Qualsys ensure availability of data by the following means:

It should be noted that all hosted solutions are in a 27001-certified data centre

- Preparation of data backups, process states, configurations, data structures, transaction histories etc., according to a tested concept
- Protection against external influences (malware, sabotage, force majeure)
- Environment monitoring including Power, temperature and humidity
- Defined roles and responsibilities and job descriptions
- Hardware monitoring
- Use of UPS for key systems
- Clearly defined backup processes.

Recoverability

Qualsys ensure recoverability of data by the following means:

- It should be noted that all hosted solutions are in a 27001-certified data centre.

- Qualsys have defined and documented Backup procedures.
- Use of UPS for key systems.
- Separate storage for systems and backups.
- Virus protection/firewall
- Emergency management
- Business Continuity Management systems
- Emergency plans (e.g. information and recovery plans).

Transparency

Qualsys ensure Transparency of data by the following means:

- It should be noted that all hosted solutions are in a 27001-certified data centre
- Clearly document IG and GDPR processes including but not limited to business processes, data flows and the IT systems used, operating procedures, interaction with other procedures
- Documented tested and approval of changes to software and business change
- Contracts with internal employees
- Contracts with external service providers and third parties
- Documentation of consents and objections
- Clear Version control for EQMS product cycle
- Clear and explicit consent is sort for use of personal data.

Unlinkability

Qualsys ensure unlinkability of data by the following means:

- It should be noted that all hosted solutions are in a 27001-certified data centre
- Standard coding practices within the Development arena
- Development is undertaken with principles defined in Privacy by Design
- Separation of production and testing environments

- Roles and Responsibilities
- Access management
- Regulated procedures for changes of purpose

Procedures for the regular monitoring and assessment of the effectiveness of technical and organizational measures adopted.

Qualsys measures for monitoring and assessment include:

- Clearly defined IG and GDPR policies, procedures and processes, including interaction and Roles and Responsibilities which are all subject to the Qualsys Audit schedule.
- Assigned DPO
- ICO registered
- Privacy Statement
- Consent Statement
- Supplier Management Breach Processes
- Data Retention Policy
- Business Continuity and Disaster Recovery process
- Subject Access Request process
- Development and Business Change Processes both of which include the Privacy by Design concept
- Regular Security and GDPR training for all staff (at least once a year)
- Asset Register, Information Asset Register and Data Processing Registers
- Privacy Impact Assessments as required
- Data Destruction and Disposal process.

From an EQMS perspective, the customer is considered as both the Data Controller and the Data Processor as they will determine what data is held within EQMS and how it is configured and utilised.

As a leader in the Governance, Risk and Compliance software market, EQMS has been designed with data protection, integrity, confidentiality and accountability in mind. EQMS has a variety of rich functionality throughout the system that supports the principals of GDPR.

This includes strict access controls not only to the system itself but also the data contained within. This is managed through functionality including Permission Groups, Document Control Types, Issue Types and Audit Types, Password Control and Acknowledgments and, Notification and Feedback functionality that allows users to be notified of changes and allow them to provide feedback as necessary. EQMS also has a thorough Audit Log functionality that allows the tracking of changes that have been made to the system and its contents. In addition to the controls in place, reporting functionality throughout the system can provide information to support GDPR requirements. User Accounts to the systems are controlled by customer determined System Administrators who have the ability to add, remove and edit user information for example.

Experienced Qualsys staff members will guide customers through the configuration of EQMS to best meet their requirements and provide guidance on System Validation.

FAQ:

Who is Qualsys' DPO?

Kate Armitage

kate.armitage@qualsys.co.uk

Contact details

Aizlewood's Mill, Nursery
Street, Sheffield, S3 8GG
info@qualsys.co.uk
+44 (0) 114 282 3338

Talk to us

Questions about our validation services? Talk to a domain expert who will demonstrate our validation services.

Qualsys