# QAD Privacy Whitepaper

QAD provides manufacturing, supply chain and connected workforce solutions to its customers; QAD provides tools to our customers to enable our customers to operate more effectively and efficiently. QAD is not involved in either data entry or extraction and uses the data that customers store in QAD environments, personal data or other data, to provide the contracted services.

The QAD offerings focus on manufacturing, supply chain and connected workforce solutions. As such, the type of personal data we expect to exist in our environments is typically limited to information that is relevant in this context. Based on the functionalities of QAD's offerings, the personal data present in QAD environments is typically limited to contact information, for instance, contact information for parties in a customer's supply chain. Additionally, data regarding access to and usage of the system is also kept, for instance in the form of usernames and system generated logs.

## Personal Data Protection

QAD has built its approach towards personal data protection around the requirements of the General Data Protection Regulation (GDPR - Regulation (EU) 2016/679). While the GDPR was conceived in and focuses on the European Union, it is generally seen as the gold standard for personal data protection regulations. Countries outside the EU have typically used the GDPR as an example and have used the same concepts and principles found in the GDPR. QAD has taken the GDPR as the basis for its global approach towards personal data protection, but does monitor for jurisdiction-specific requirements for supplemental controls.

## Key Concepts

The key concepts in personal data protection are Personal Data, Processing, Controller and Processor.

- Personal Data means any information relating to an identified or identifiable natural person (the so-called "data subject"). The definition is extremely broad and covers any information that can be used to directly or indirectly identify a person.
- Processing is defined as any operation or set of operations which is performed on personal data. This ranges from technical operations, such as storage, transmission and destruction of personal data to actively working with personal data. The main processing activities performed by QAD in the context of the provision of cloud services are technical in nature and do not involve human intervention. However, in the context of the provision of support or professional services, QAD may come into contact with personal data.
- A Controller is the entity that determines the purposes and means of the processing of personal data. In the context of the provision of cloud services, our customers are the Controllers as they are the ones making the decision to engage a cloud services provider, such as QAD.
- A Processor is the entity that processes personal data on behalf of the Controller. QAD fulfills the role of Processor when providing cloud services to customers.

With regard to customer data and information, the customer acts as the Controller and QAD acts as a Processor.

## Requirements when Engaging a Processor

The main obligation of a Controller when engaging a Processor is to engage only Processors that have implemented appropriate technical and organizational measures, sometimes referred to as TOMs, to ensure that the processing of personal data meets with the legal requirements. The engagement must be governed by a legally binding document that addresses the requirements, such as a cloud services agreement.

Separate data processing agreements or DPAs are sometimes requested to address the legal requirements that are specific to personal data protection. QAD believes that this disjointed approach towards documenting an engagement, using two documents (the main agreement and a separate DPA), rather than one is not optimal. While there are topics that are specific to personal data protection, most topics are relevant to the cloud services as a whole. Key examples are confidentiality, security and end-of-life; it goes without saying that these topics are of the essence when it comes to dealing with **all** customer data, not only when dealing with **personal** data. By dealing with these topics in two locations, there is a risk of inconsistencies and/or gaps. Consequently, QAD has opted to cover the topic of personal data protection in the cloud services agreement. Topics relevant to the cloud services in general are dealt with in separate articles, such as "security" and "confidentiality", the topics with specific relevance to personal data protection are grouped in the article "personal data". The technical and organizational measures required to secure the processing of personal data are documented in the Cloud Program Document (see below). In drafting the documentation, QAD has followed article 28 of the GDPR that lists the requirements that must be met when engaging a Processor.

## Assistance with Compliance

A Processor must make all information available to a Controller that is necessary to demonstrate a Controller's compliance with its personal data protection obligations. The QAD documentation comprises a number of elements that will help a Controller to do this:

- The Cloud Services Agreement addresses the legal requirements.
- The Cloud Program Document, referenced in the Cloud Services Agreement, contains the service levels for the cloud services, and also outlines, at a high level, the various security measures taken to address the "security triad" of availability, confidentiality and integrity. It also contains the contractual commitment of QAD to maintain various externally audited certifications (see below). It is available from http://www.qad.com/legal.html.
- The Privacy Whitepaper (this document) provides context around QAD's approach towards personal data protection.
- The Security Whitepaper, available from the QAD Trust Center (https://www.qad.com/trust-center), goes into more detail on QAD's approach to security.
- The various externally audited certifications, such as such as ISO 27001, SSAE18 (SOC 1 and SOC 2), CSA Star and TISAX (German location), for which evidence of certification is provided on the Trust Center (https://www.qad.com/trust-center), provide confirmation that QAD is honoring its contractual commitments.
- The QAD Privacy Policy (https://www.qad.com/terms-privacy#privacy) documents QAD's general commitment to privacy. The policy covers QAD's commitment to treat all personal data, be it customer personal data or QAD's own internal personal data, in accordance with the principles of the GDPR. QAD maintains a certification under the EU-U.S. Data Privacy Framework Program (DPF) principles, including the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Principles.
- The Standard Contractual Clauses (pre-completed version), relevant in situations where a QAD customer with activities in the European Union utilizes a QAD data center located outside of

the European Union (e.g. a US headquartered customer with European subsidiaries). The pre-completed SCC are available from http://www.qad.com/legal.html.

## Conclusion

QAD takes personal data protection seriously and has set up its organization, its cloud services and its supporting documentation to allow customers to check QAD's compliance with its various obligations and to demonstrate their own compliance with applicable personal data protection legislation to third parties.