QAD AND THE GDPR

by Robert van Kralingen,
QAD EMEA Regional Counsel

A QAD Leadership White Paper for the
Global Manufacturing Industry

CONTENTS

Introduction 3

Key Concepts 3

Principles That Apply to the Processing of Personal Data 4

Obligations of a Controller 4

Obligations of a Processor 5

QAD Cloud Customers 5

QAD's Commitment 6

QAD Conclusion 6

QAD AND THE GDPR

INTRODUCTION

The General Data Protection Regulation (GDPR) has garnered a lot of attention since its adoption by the European Parliament in April 2016. The GDPR focusses on the protection of the privacy of individuals by regulating how data pertaining to those individuals may be processed.

While the GDPR is a European regulation, personal data protection regulations exist in many countries and, consequently, focusing solely on Europe, or, more precisely, the European Union, would not do justice to the topic. Moreover, the GDPR will most likely impact operations of businesses outside of Europe, especially if personal data is shared within an organization operating internationally or if an organization offers its goods or services to people living in the European Union.

In this whitepaper we elaborate on personal data protection, with a specific focus on the GDPR and how it impacts your QAD environment.

WHAT IS THE GDPR?

The General Data Protection Regulation is the successor of the European Data Protection Directive from 1995. It focusses on the protection of natural persons in relation to the processing of personal data. The GDPR has been adopted in April 2016 and has direct application as of the 25th of May 2018. It is important to note that the GDPR is a Regulation, rather than a Directive. Whereas a Directive is intended to be transposed into national laws, a Regulation has direct force in all EU countries, i.e. the GDPR will be directly enforceable in all countries. An advantage of this approach is that a higher level of consistency exists between EU countries. While the GDPR adds various requirements and enhances others, it is not a complete departure from the past; all key concepts and principles from the Directive have been retained.

KEY CONCEPTS OF THE GDPR

The key concepts around which the regulation revolves are personal data, processing, controller and processor. Whereas the terms “personal data” and “processing” cover the topic of the GDPR, the terms “controller” and “processor” demark the entities that the obligations of the GDPR focus on. 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. The definition not only covers contact information, but also other data, such as IP addresses, that alone or in combination with other data can lead to the identification of an individual. Processing is defined as any operation or set of operations which is performed on personal data. Basically, if you come into contact with personal data in any way, you are processing personal data. The Controller is the entity that determines the purposes and means of the processing of personal data (we will go into this below), and, finally, the Processor is the entity that processes personal data on behalf of the controller.

HOW DO THE KEY CONCEPTS APPLY TO QAD CUSTOMERS?

Businesses process personal data for a multitude of reasons. A company employs personnel, has a financial administration, maintains contacts with customers and suppliers, provides services, manages its IT systems, etc. These are all activities that involve the processing of personal data. The business is the controller of the personal data used in the aforementioned activities. If a business has engaged with a third party for the processing of personal data on its behalf, then the third party is a processor of such data. Examples range from payroll processors to cloud solution providers such as QAD.

WHAT ARE THE PRINCIPLES THAT APPLY TO THE PROCESSING OF PERSONAL DATA?

The GDPR lists a number of principles that apply to the processing of personal data. The principles are listed below:

a) *'lawfulness, fairness and transparency'*: personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;

b) *'purpose limitation'*: personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) *'data minimisation'*: personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) *'accuracy'*: personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) *'storage limitation'*: personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

f) *'integrity and confidentiality'*: personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

When personal data are processed, the principles must be observed. Without elaborating on each of the principles, we want to make a few observations. Three of the principles, namely "purpose limitation", "data minimization" and "storage limitation", focus on the bigger idea that personal data should only be processed when there actually is a discernible need to do so and then only to the extent that such processing is needed. Two of the principles, namely "accuracy" and "integrity and confidentiality", align with the literature on IT system security, where confidentiality, integrity and availability of an asset are considered of the essence. Finally, the first principle, personal data shall be processed lawfully, fairly and in a transparent manner, makes it clear that the interests of individuals should be taken into consideration, that you should be clear about what you are doing with personal data and that there has to be a lawful reason, such as the performance of a contract, to process personal data.

WHAT ARE THE OBLIGATIONS OF A CONTROLLER?

The controller is responsible for and should be able to demonstrate compliance with the principles outlined above. As such, a controller is obligated to implement technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. A controller should maintain a record of all processing activities under its responsibility.

Your QAD environment will contain personal data, but, as QAD solutions focus on the manufacturing space, it most likely will be limited to contact information for customers and suppliers and to information on how the environment is used. For instance, the contact information stored in your QAD environment is likely used to be able

to perform the contracts in place with customers and suppliers (ordering supplies, shipping goods, providing after sales support, etc.). The information on the use of the environment (e.g. the system logs when someone signs on to the system) is required to maintain integrity and confidentiality of data. It is processed on the ground that processing is necessary for the purposes of the legitimate interests pursued by the controller (note: this is another example of a lawful ground for processing).

If you are using the QAD cloud, QAD takes care of a number of requirements. For instance, QAD implements security measures for its cloud environments, both on a technical and organizational level, and maintains various externally audited certifications which prove that the measures have been implemented to the required standard.

WHAT ARE THE OBLIGATIONS OF A PROCESSOR?

A processor may only process data when this is documented in an agreement. The agreement must describe the processing and should make clear that the processing is done on instruction of the controller. Additionally, a processor should keep personal data confidential, should implement adequate security measures, and should assist a controller in certain tasks, such as performing a data protection impact assessment and helping with requests from data subjects. A processor should also make data available that can help a controller demonstrate compliance with the GDPR and should allow for and contribute to audits to determine compliance with the GDPR. Finally, a processor should return all personal data at the end of an engagement.

HOW WILL QAD HELP ITS QAD (CLOUD) CUSTOMERS?

The QAD solutions are focused on the manufacturing space. As such there is not much focus on personal data within the context of such solutions. However, as the QAD environments do contain personal data, they should be included in an overview of personal data processing activities. Given the type of personal data present in your QAD environment, it is likely that standard security arrangements, such as access secured through a user name and password, will comply with the requirements of the GDPR.

If QAD provides cloud services, QAD is a processor with regard to such services under the GDPR. QAD takes its responsibilities as a processor seriously and will only process personal data obtained from its customers to provide services to its customers. QAD has implemented its cloud environments using industry best practices (data centers for European customers are based in Paris and Amsterdam) and maintains numerous certifications for its cloud environments, such as ISO27001, SSAE18 and CSA Star. We will share evidence of these certifications with our customers to aid in proving compliance with the GDPR when using the QAD cloud. If additional services are required, such as assistance with a data protection impact assessment or an audit of the QAD cloud environment, QAD can be contracted to provide such services. Finally, QAD services contracts have contained a clause on the processing of personal data reflecting these principles for well over a decade.

QAD AND THE GDPR

WHAT HAS QAD DONE ITSELF?

As a company QAD is committed to global compliance with applicable laws on personal data protection. As QAD is a global company, the issue of international data traffic is relevant to QAD, as it is to many of our customers. QAD has taken steps to ensure that the GDPR principles apply globally within QAD and, for customers, when dealing with a QAD entity anywhere in the world. QAD is certified under the Privacy Shield Framework which forms the legal basis for direct compliance with the GDPR principles by QAD in the USA. Additionally, QAD has adopted the rules of the framework globally by explicitly referring to the framework in its privacy policy (available from qad.com) without any geographical restrictions. To ensure compliance when it comes to the processing of personal data for which QAD is a controller, QAD has implemented a solution using the standard contractual clauses created by the European Commission.

CONCLUSION

The GDPR will affect operations in your organization. The definitions determining applicability are extremely broad. The GDPR does not only apply if your organization is based in an EU country, but also if you sell goods and services in the EU.

When processing personal data it is important that personal data should only be processed when there actually is a discernible need to do so and then only to the extent that such processing is needed. The processing of personal data should always be based on a lawful ground, such as the performance of an agreement, for instance and agreement for the delivery of goods. A controller should keep an overview of all processing activities and should make sure that adequate technical and organizational measures ensuring compliance with the GDPR are in place.

When QAD provides cloud services, it acts as a processor providing services for the benefit of the controller. In this position QAD can assist customers with certain aspects of GDPR compliance, such as the implementation of technical and organizational measures.

As QAD deems compliance with personal data processing regulations extremely important, QAD has committed to adhere to the standards imposed by the GDPR globally.

QAD Inc.
100 Innovation Place
Santa Barbara, CA
93108 USA
Tel: + 1 805 566 6100
www.qad.com