# Data Protection Management Systems and the GDPR

TÜV USA
TÜV NORD GROUP

# DEADLINE: May 25, 2018

The clocks are ticking down to May 25 2018, the day when GDPR becomes effective. The GDPR (or the General Data Protection Regulation) will require that all European Union and EEA member states adopt GDPR into their local legislation by this date.

What does this mean for companies selling products and services in the EU and the EEA? It simply means you need to comply with GDPR which apply to the product and/or service being sold – not all regulations included in the GDPR will be applicable to all companies. In this article, we discuss some tips on complying and staying up to date the GDPR regulations.

It is important to understand that you need to comply with GDPR, even if you don't have a legal entity in the EU. As long as you collect, process, exchange, or store personal identifiable information (PII) of EU and EEA citizens (referred to as Principals), you will need to ensure you comply with these regulations. Non-compliance and data privacy breaches may result in fines – up to 20 million Euro or 4 % of your global annual revenue – whatever is higher. You should really avoid that.

Many of GDPR requirements are focused on the legal basis for collecting and processing Principals' PII. At its basis is the idea that collecting and processing Principals PII is forbidden by law – unless there is a legal basis (by law, contract etc.), or you have a clear - and evidence based - consent. This creates a clear "Data Privacy by Default" and "Data Privacy by Design" working standard for companies looking to do business with the EU and EEA states, giving Principals the opportunity to control the use of their PII, including if you intend to change the use of PII already collected.

The message is clear to companies: you are obligated to get the Principal's consent BEFORE you collect data and for a new or changed consent BEFORE you change the purpose of the use of PII already collected.

The first data protection law was published in 1970 in the German federal state of Hessen. In 1974 the US Privacy Act was introduced. In 1980, the Organization for Economic Co-operation and Development (OECD) launched the first version of international data privacy principles, designed to ease the international exchange of information based on a common understanding.

**In 2011, ISO and IEC published the international standard, ISO/IEC 29100:2011. This standard was created with OECD in mind. There is a strong correlation between the requirements in ISO/IEC 29100:2011 and DGPR, as DGPR was also created around OECD. Companies who are compliant with DGPR will be following well established principles which can aid in meeting the regulatory requirements in other jurisdictions, such as Canada, Australia, or Singapore.**

**Companies should have robust processes in place, supported by technical measures. We would like to point out an important element of GDPR: certification (based on Article 42 of GDPR). You may use certification services provided by certification bodies to demonstrate your readiness for GDPR. This could be an important corner stone to build trust with your clients and partners around the globe and in the EU.**

**As a certification body, we believe in management systems. Certification helps companies ensure that they have the proper procedures in place that are compliant with the protections regarding PII, while also ensuring that there is a strong basis for the continuous improvement cycle regarding those protections. This is a valuable service provided by industry professionals who know what works and what doesn't.**

**A strong quality management system gives companies the relevant tools to identify, evaluate, and implement the measures, allowing for a significantly higher chance at successfully maintaining GDPR compliance. There are three valuable certifications that help support a company's compliance with GDPR. The first is the general quality management system certification, ISO 9001. Next is the more specialized standard, ISO/IEC 27001 which certifies quality in a company's Information Security Management System. ISO/IEC 27001 is a risk based standard which includes an annex of 114 controls concerns technical and organizational aspects of information security. Due to impartiality rules and regulations, certification bodies cannot help a company create a strong quality management system or DPMS – that is the arena of quality management consultants. Hand in hand with ISO/IEC 27001 is ISO/IEC 27018 which is a guideline that builds in the protection of PII in the cloud environment.**

When discussing GDPR we often hear: "We have ISO/IEC 27001 in place and we wish to integrate ISO/IEC 27018:2014 now. Will this be sufficient?" Unfortunately, this is not a clear "yes" or "no" answer. In essence, ISO/IEC 27018 adds additional controls that help aid in the integration ISO data protection principles. The bad news is: it is generally focused on public cloud service provisioning.

Legal requirements, like GDPR, tend to leave the legal entity liable for processing and collecting PII, but are not usually limited to a specific delivery model of services, like public cloud services. ISO/IEC 27001 and ISO/IEC 27018 can be a good solution for you - if you are a public cloud service provider and if you address the GDPR requirements in your Information Security Management System.

It may behoove your company to consult with your legal department, corporate lawyers, or other legal aid in understand the legal ramifications of the GDPR regulation rather than try to read through it on your own, particularly when handling international business considerations.

There are a couple of options facing companies who are interested in using a quality management system certification to help them meet the requirements of GDPR. The remainder of this article discusses these options.

## Option 1: Meeting GDPR requirements in your Information Security Management System based on ISO/IEC 27001:2013

ISO/IEC 27001 Annex A A.18.1.4 is a control covering Data Privacy and Data Protection. The requirement is very generic and give no additional guidance how to ensure PII is protected. The approach is not particularly handy for the implementation of new certification purposes.

So why not work with the power inherent to ISO standards? ISO/IEC 29100 is not a single standard, it is the groundwork for a series of standards concerning a range of Data Protection related issues. An example of this would be the new ISO/IEC 29151 standard containing controls with respect to data protection. And voila: it is in line with Annex A of ISO/IEC 27001!

So, we have a full set of implementation guidance based on the ISO data protection principles to implement data protection controls. These can be selected and improved based on the information security management system already in place. You may use the statement of applicability of your ISMS to justify inclusions and exclusions from this data privacy control framework. Two things to mention here:

1. It’s important to make sure that the scope of the ISMS covers all aspects of processing and collection of PII set by GDPR.
2. Make sure you address the relevant legal requirements of GDPR, e.g. the 72-hour timeframe for communicating data privacy breaches to the relevant authority located in the EU. So, you need to be aware what the specifics of GDPR, for example:
    - ♦ The legal basis for collecting and processing PII;
    - ♦ The processing PII of minors;
    - ♦ The "Right to be forgotten"; and
    - ♦ The restrictions regarding retention periods.

If you plan to, or already have, processed PII for the purpose of profiling be aware you need to conduct a data privacy impact assessment (DPIA). This comprehensive assessment is essential to ensure you understand the legal restrictions, the risks to Principals’ rights, and all the relevant technical and organizational measures. To guide you through this, it may be helpful to refer to ISO/IEC 29134 which provides a detailed guideline on how to perform a DPIA and how to keep evidence of it.

When using ISO/IEC 27001 for managing the collection and processing of PII means, the scope of the management system consists of all processes, activities, locations and applications relevant at least for collecting and processing PII under GDPR. To do so effectively, it is vital to ensure your company is familiar with all the GDPR requirements, especially those that impact your company’s activities. If you have considered this already, you may use ISO/IEC 27001 and go ahead with certification.

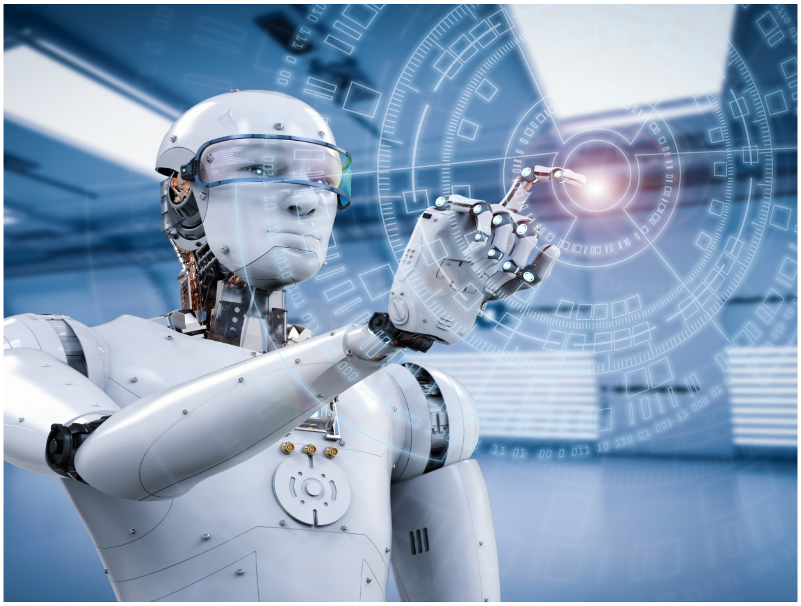
### Option 2: A Stand-Alone Data Protection Management System

The British Standard (BS) 10012 follows the high-level structure of all relevant ISO management system standards. For companies who are already compliant to an ISO standard, this is great news. Same structure, same core text.

Chapter 6.1 and 8.2 give guidance regarding the GDPR. The guidance covers data inventory, some legalities for collecting and processing PII, as well as Data Privacy by Design and Default. These sections are critical to GDPR.

Certification is possible, however the certification is not yet accredited. But major companies in the IT sector have already achieved certification successfully. And despite the lack of accreditation, consumers and authorities have been accepting and aware of this certification.

If needed, it can be possible to use ISO/IEC 29151 control framework and ISO/IEC 29134 for DPIA as an additional guidance for your DPMS.



## Conclusion

Either you integrate data protection into your ISMS or you choose for a stand-alone DPMS, a management system is a good solution to meet GDPR requirements and much more to stay ahead of the game.

Certification bodies can help you through the process by providing audit and certification service. These reports and certificates prove the effectiveness of your data protection activities, and that necessary processes in place. Both BS 10012:2017 and the ISO/IEC 29100 series provide sufficient guidance and groundwork for you and your certification body.

This is no guarantee for legal compliance, but it is a valid and acknowledgeable approach to build confidence in your services.

## About the Authors

**Uwe Ruehl**, Owner and Managing Director of RUCON Group (Consulting, Training and Managed Services) based in Nuremberg Germany

Uwe has been in information security, business continuity and data protection since the mid-90s. With his team he trains, audits and consults clients from all industrial sectors with a strong focus on effective and pragmatic management systems. Since 2004 he has been auditing management systems (ISO 9001, ISO/IEC 27001, ISO 22301 and ISO/IEC 20000-1) in various industrial sectors globally.

His job and education background consists of IT and telecom's sector (at Siemens), emergency dispatch centers operation and management and master's degrees in Risk and Compliance Management and Safety and Security Management. Since 2011 he has been working with Data Protection Management Systems successfully and is an expert in protecting PII in cloud environments as well. Contact Mr. Ruehl through LinkedIn.

**Janice Harvey**, Project Manager of TUV USA

Janice has been with TUV USA since May of 2016. She is the Project Manager of Medical Products Division. She is a content editor & writer of the TUV USA Blog.  Janice is currently attending Kaplan University for a Bachelor's Degree in Business Administration. Contact Ms. Harvey though TUV USA or LinkedIn.

## About TUV USA, Inc.

With locations throughout the USA and access throughout the world, TUV USA, Inc. is one of the most experienced companies in the management of assessing and certifying management systems and regulatory inspection activities in the United States of America.

TUV USA, Inc. has the expertise to help companies from small to large who need regulatory assistance and accurate information. We also provide ISO 9001, 14001 certification services, AS9100, AS9120, ISO 13485, CMDCAS, MDD, ISO 18001, ISO 27001 and training services. A value added audit service for costs that are less than other Certification Bodies. All auditors are industry certified and have more than 15 years of industry knowledge and auditing experience. We provide a higher level of service for customers that cannot meet the ever changing demands of quality requirements from your customers and from industry.

Please feel free to contact us to understand more about our company. We are simply the best resource for any auditing and regulatory need in the world and with our many locations; we can provide a local service to you.