

News

Vanderbilt's answer to the new GDPR



By Peter P. Mueller

In 2015, the EU launched the new “General Data Privacy Regulation”. This enters into force from May 25, 2018 and every company operating in one or more of the 28 EU member countries must abide by this regulation. As such, this will have a big impact on how companies handle of personal data.

Vanderbilt operates in the majority of EU's 28 countries and processes all data in private and public cloud suppliers in the EU and USA. Therefore, the GDPR compliance is an important issue for us.

Since the beginning of 2017, Vanderbilt has initiated several activities to comply with this

new adjustment. As the EU regulation highly depends on the old German Data Protection regulation, we enlarged our already existing protection processes in Germany, and began to roll these out to our offices in other European countries.



We assigned a Data Protection Officer on July 1, 2017. Until May 2018, their main task is to develop and implement a data protection concept. This includes obtaining general agreements with all our external suppliers to obligate them to store the relevant data and to operate according to the GDPR. Part of our agreement with suppliers is to get a list of third countries that might store our data. Mostly, we are using our GDPR compliant agreement for the commissioned data processing. If a supplier proposes their own agreement, we carefully check the content to ensure that all GDPR requirements are reflected.

A special area of focus is Software-as-a-Service products such as Vanderbilt's **ACT365** and **SPC Connect**. These solutions must also comply with the new regulation. As we operate and store personal data from our customers, we emphasize, for instance, on the security and encryption of the processed data, the storage time of data, and the design of the privacy and data protection.



The actual GDPR will not be the final version as there are further needs yet to be addressed. For instance, the new obligation to inform the authorities about data privacy or security violations is on the right track, but it is not clear when an incident must be reported. Companies still have different interpretations of what is a serious or harmless incident.

To summarize, we are certainly on the right track but still have more to do. Happily, however, in the last broad **cyberattack, Wannacry**, Vanderbilt and our selected providers could not report any violation of our data usage.



vanderbiltindustries.com