**PRESS RELEASE**

# macmon – Controlling network access within the framework of the General Data Protection Regulation (GDPR)

Berlin, January 29 2018 - From 2018 onwards, the European General Data Protection Regulation – or GDPR for short – will be the new basis for data protection. The GDPR replaces the more than 20-year-old legal framework for data protection. Until now, that framework consisted of the European Data Protection Directive from 1995 and the national data protection laws based on it, such as the Federal Data Protection Act (BDSG) in Germany. The GDPR regulates the type of data that must be protected and how this data is handled. It also prescribes specific control mechanisms and sanctions.

The regulation will apply to all companies with headquarters and/or a subsidiary in the EU without exceptions. It will furthermore affect companies worldwide that collect data from persons within the EU. In the short and medium term, companies will have to examine their use of personal data in detail and extend the protection of this data where necessary.

**macmon supports the implementation of the GDPR through monitoring, segmenting and isolating end devices**

macmon NAC, the leading German solution for network access control, provides an effective means of meeting various requirements of the GDPR.

The macmon solution has been certified by the German Federal Office for Information Security (BSI) and turns heterogeneous and complex networks into one intelligent unit, effortlessly enabling efficient monitoring and providing protection against unauthorised access.

This is how macmon guarantees a clear overview and documentation of the local network and access to it, for example. It also logs all attempts at access in full and even recognises when such an attempt occurs at an unusual time.

The network is segmented in connection with an easy-to-administrate end device group. This significantly reduces the scope of end devices to be considered for securely processing particularly sensitive data while simultaneously focussing it on critical devices. A clear web interface also offers an overview of which devices can be, and currently are, connected.

macmon isolates end devices not in line with the GDPR – because they do not, or they no longer, meet security requirements – from sensitive areas and moves them to quarantine. This significantly reduces the workload of IT administrators and makes it possible to comply with the processes specified by the GDPR.

In addition to issuing alerts and preventing unauthorised network access, segmenting networks dynamically is also the most effective and most secure way of preventing unauthorised access to data.

Combining the storage of sensitive data on separate servers (to make it accessible only within defined network segments) with macmon Network Access Control ensures maximum protection.

**Protection from data abuse**
Wireless networks (WLANs) are increasingly being used to link all types of different devices. In some cases, company devices even share a network with visitor devices. In hospitals, for example, such networks might even contain sensitive patient data as well.

Rob Billington, UK Country Manager macmon secure: "Even though the necessary technology is available, the required segmentation of WLANs into VLANs is not yet common practice. Its implementation is as simple as it is sensible. Without this segmentation, unmonitored devices, such as those of external service providers, are in the same network as highly sensitive patient data. The latter is therefore exposed to a significant risk of data abuse. It is important to close this gap with a secure NAC solution like macmon."

**About macmon:**
The company is manufacturer of an independent and modular NAC solution who protects the network against unauthorised and unsecured devices, as well as internal attacks. Customers benefit from macmon's security know-how, predictable costs and an increased level of security, gained from determining exactly which devices are allowed on which segments of a network. The software features ease of use, integration with other leading security products, and ongoing development to keep it in line with the latest standards. The customer base includes international companies of various branches and sizes.

The headquarters of macmon secure GmbH are located in Berlin, Germany.

macmon secure is a member of the Trusted Computing Group and actively participates in various research projects.

For more information, please visit https://www.macmon.eu/en/home
Facebook: https://www.facebook.com/networkaccesscontrol/
Twitter: https://twitter.com/macmonUK
Youtube: https://www.youtube.com/user/macmonsecure

**Contact at macmon**
Sabine Kuch
Manager Marketing & Communications
Alte Jakobstraße 79-80
10179 Berlin - Germany
Tel.: +49 30 2325777-0
nac@macmon.eu

**Press contact**
sugarandspice communications GmbH
Jens Dose
Tel.: +49 (0) 89 / 26 20 936 12
jdose@sugarandspice.online