# Comment

## GDPR: Regulation almost in force and all questions still open?

### An assessment on the occasion of the European Data Protection Day on 28 January – by Dominik Lehr, founder and CEO of Befine Solutions AG

Freiburg im Breisgau, 25th January 2018. In 119 days, on 25th May 2018, the General Data Protection Regulation will come into force once and for all. The transition period of two years, and with it the grace period for organizations and authorities, will come to an end. Although time is pressing, many still lack a plan for its implementation. They now have no choice but to set priorities. But where to start?

According to a survey carried out in September 2017 by Bitkom, Germany's digital association, only 13 per cent of companies had begun or completed first measures to implement the GDPR while 33 percent were still unprepared. According to a survey in October 2017 by the German-speaking SAP-user group (DSAG), the association for SAP users in Germany, Switzerland and Austria, every other organization still did not have a plan for implementing the Regulation. One should think that those in charge would have had enough time in the past 20 months, since the regulation had come into force in May 2016, to implement it.

Although they will certainly not be prosecuted immediately, those who cannot prove to the authorities that they are at least working on adapting their processes and tools in accordance with the requirements will be guilty of gross negligence and may rightly face penalties.

### Communicate only encrypted from now on?

How about starting with your emails? While, in many cases, GDPR speaks vaguely of "privacy by design", including in Article 32 ("security of processing"), it explicitly demands the "encryption of personal data". Of course, this does not mean that companies are only allowed to communicate via encrypted e-mails. However, it is true that factors such as the need for data protection must be taken into account. The Regulation applies only to personal data, but other confidential data should also be protected. Organizations must implement „Privacy-by-Design“ and „Privacy-by-Default“, the basic conditions are written down in Article 25. These principles require that data are collected anonymously or pseudonymously and processed in encrypted form wherever possible.

Email plays a central role in the whole issue. On the one hand, it has been established for many years as a primary means of communication in the corporate environment, since it is easy to use and universally available. On the other hand, this is precisely where security issues come into play: email systems are a preferred target of criminals, hackers and industrial spies - nine out of ten cyber attacks start with an email.

### How to pre-empt cyber criminals?

Dangers lurk in the way that company employees communicate. Therefore, it is important for IT managers to minimise the attack area. Particularly since it is not only economic damage that results if confidential information falls into the wrong hands - accidentally or intentionally - but also the potential damage to reputation should not be underestimated.

Special authentication and encrypted transmission of the contents make it impossible to read email correspondence. But only if the subject lines are encrypted can attackers not recognize who is talking to whom about what and draw conclusions from it - even this information ("Coordination required for takeover bid company X") can be sufficient to launch a social engineering attack.

An important compliance standard that GDPR demands is the classification of data. With appropriate solutions, companies can meet the legal requirements and implement their own guidelines: The e-mail protection classification enables users to classify data according to the level of protection they need in order to be able to send each outgoing message with an adequate level of security. Specifically, this means that for example strictly confidential patient data must be sent as an encrypted attachment with a one-time password and a traceable acknowledgement of receipt.

### How to avoid „shadow IT“?

In particular, large amounts of digital data that cannot be sent by email can tempt employees to use other means of data exchange - such as USB sticks, file sharing solutions or cloud services, which they know mainly from the private sector. The result: The often quoted "shadow IT", the frequently occurring use of unauthorized software in the company during data exchange.

This makes it all the more important that security, user-friendliness and cost-efficiency go hand in hand. In general, technical solutions are only one side of the coin which should not be considered in isolation. The other is to sensitize employees, ideally in the form of regular training. After all, users play a central role in all questions relating to IT security.

About the European Data Protection Day
The European Data Protection Day, established at the initiative of the Council of Europe, has been held annually since 2007, around 28 January. The day is called Privacy Day outside Europe.
Further information can be found here.

About Dominik Lehr
Dominik Lehr is founder and CEO of Befine Solutions AG located in Freiburg im Breisgau, Germany that develops and supplies software solutions for companies.

About Cryptshare and Befine Solutions
The owner-managed Befine Solutions AG develops and supplies software solutions that help companies support, optimise, and secure their processes. Founded in the year 2000, the company with now over fifty employees has its headquarter and development site located in Freiburg im Breisgau, Germany. There are sales locations in the UK and the Netherlands. In 2017, a subsidiary in America was established: Cryptshare Inc.
The focus is on Cryptshare, a communication solution for the exchange of sensitive business information. It makes it possible to send and receive e-mails and large files ad-hoc – securely, easily and at low cost. Cryptshare also offers auditability which helps companies follow compliance rules and regulations. Today more than 1400 companies use Cryptshare with about 3 million users in over 80 countries. This success is underlined by the award of the “Cybersecurity Excellence Award 2017” to Befine Solutions AG.
Please find further information on: www.cryptshare.com. Users may inform themselves on the blog.

Press contact:
phronesis PR GmbH
Marcus Ehrenwirth, Marcus Wenning
Kobelweg 12 ¼
86156 Augsburg
Germany
Telephone: +49 821 444800
Email: info@phronesis.de
Web: www.phronesis.de

Befine Solutions AG – The Cryptshare Company
Oliver Gäng – Head of Digital Marketing
Schwarzwaldstrasse 151
79102 Freiburg im Breisgau
Germany
Telephone: +49 761 389130
Email: oliver.gaeng@cryptshare.com
Web: http://www.cryptshare.com