A Brief Look at GDPR and IAM

There's been lots of talk around the world about "GDPR," or the European Union General Data Protection Regulation. The regulation is now in full force. Is your company in compliance?

This e-book takes a quick dive into the GDPR from the perspective of businesses, and, more specifically, examines the role of identity and access management (IAM) within the new regulations.

The basic facts … and "Mayday"

The GDPR is poised to transform data security privacy regulations throughout the European Union.

Simply put, GDPR is a data privacy and protection regulation designed to beef up data protection for individuals within the EU, while also considering and ensuring privacy for data that is exported beyond EU borders.

GDPR was created to replace the Data Protection Directive 95/46/EC, and the new regulation was approved and adopted by the EU Parliament in 2016.

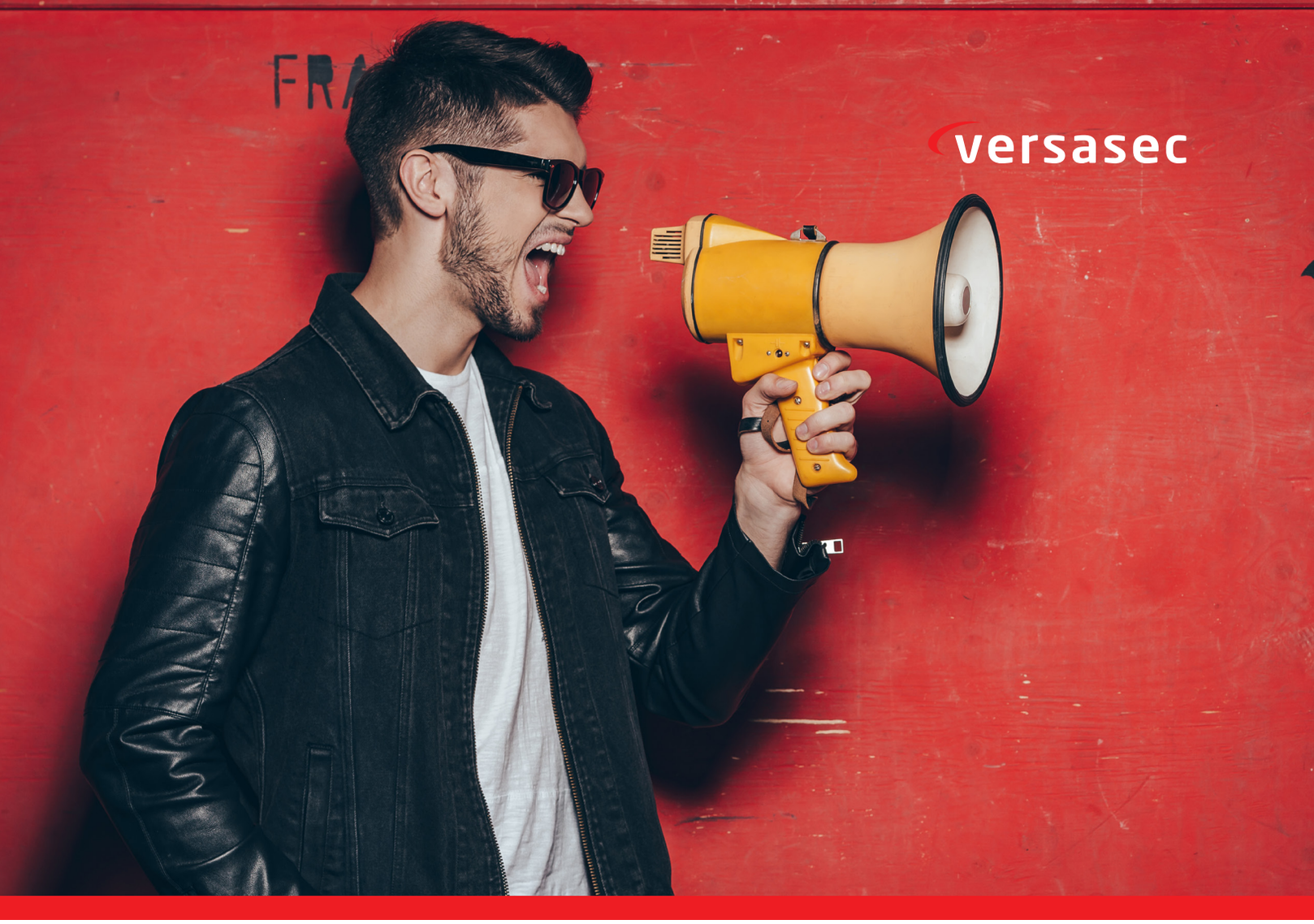
The GDPR went into effect on May 25, 2018. That date is important for a variety of reasons, not the least of which is that companies in non-compliance following that date may face heavy fines.

GDPR Regulations will:

- **Harmonize data privacy laws across the European Union**
- **Protect and empower the data privacy of EU citizens**
- **Reshape the way organizations across the EU approach data privacy**

In terms of how companies should reshape their data privacy, the GDPR specifies the following:

- **Only process data for authorized purposes**
- **Ensure data accuracy and integrity**
- **Minimize subjects' identity exposure**
- **Implement data security measures**



Notification requirements and penalties

It is important for organizations to fully understand how the GDPR works because non-compliance fines can be steep.

A major element of the GDPR involves how and when companies alert their customers when data may have been compromised.

With the new regulations, when a company learns of a data breach there are several possible activities they may be required to perform (much of this depends on the severity of the breach), including notifying the local data protection authority within 72 hours and, if needed, notifying the owners of the records that may have been compromised very quickly.

The GDPR rules do provide exceptions based on whether the appropriate security controls are deployed within the organizations. For example, if data is well encrypted such that a hacker cannot decrypt it, the company is not necessarily required to notify the affected record owners.

Fines will be assessed based on the following criteria: Nature of the infringement, negligent intent, damage mitigation, preventative measures in place, corporate breach history, organization's willingness to cooperate, type of data breach and notification protocols.

Companies that are found to be in non-compliance can be fined according to the most damaging infringement, rather than separately penalized for each provision. It is worthwhile to remain in full compliance as fines can be very steep for companies that do not comply with the regulations. In fact, maximum fines can range as high as €20 million (approximately $24million US), or 4% of the worldwide annual revenue of the prior fiscal year, whichever is higher. For a complete list of fine criteria, visit: https://ec.europa.eu/info/law/law-topic/data-protection_en

Who needs to worry about GDPR?

As the EU looks to protect the privacy of its citizens, companies with global reach also are impacted.

The GDPR, though a European-based regulation, has reach both within and far beyond the EU.

Companies based anywhere within the borders of the European Union must comply with GDPR. But it's also impacting other companies and organizations around the globe.

For non-EU-based companies that have European offices, have customers in the EU, that offer goods and services in the EU, or that have personal data on persons who live in the EU, knowing about the nuances of GDPR and abiding by the regulations can help them avoid non-compliance fines.

Meeting all GDPR requirements

There is no one-size fits all for GDPR compliance. The best solutions typically are provided by combining several solutions.

When it comes to GDPR, meeting all the requirements of the GDPR means working with multiple solution providers. Because GDPR seeks protections around governance, contractual obligations, security and more, there is no one solution that addresses all the moving parts of the regulation.

Companies must work with trusted partners and vendors to build solutions that help them address the critical areas relevant for their organizations.

In the past, many breaches have been attributable to third-party contractors working for companies and not following strict privacy regulations. Ensuring all third-party contractors are GDPR ready and can and will implement the stringent security measures your company requires to comply with GDPR is more important than ever.

Throughout the details of the regulation, there is one common thread: strong security. Security elements discussed within the GDPR framework include threat protection, user authentication, encryption, key management, antivirus, backup and recovery, and more.

Access Control and Restriction

Verifying and managing user identities is critical for meeting GDPR standards.

Understanding and legitimizing the identity of any user accessing data is another stringent GDPR requirement. Moreover, proving compliance with this requirement means companies must ensure their security controls can be audited with identity and access management (IAM) solutions: https://versasec.com/vsec-cms.php

Identity requirements are easily met with multifactor authentication – such as smart cards and virtual smart cards. Solutions like these help control which users have access to the network and the data within an organization (whether they are employees or contractors) and mitigates the risk of unauthorized users accessing the data.

Multifactor authentication is far more effective than password-only solutions and can be deployed easily and cost effectively.

These technologies help both known and unknown threats, and when used with an identity and access management solution, it becomes far easier for companies to stay in control of their data.

Strong Key Authentication Management

Encryption keys are the foundation of a strong, GDPR-compliant security solution.

Deploying strong key management is a pillar of the GDPR central data protection requirements.

Key management simply means the ways in which cryptographic keys are managed – including generation of the keys, storing keys, using and replacing, and destroying “cyber” keys -- in a cryptosystem.

Key management concerns keys at the user level, either between users or systems. This contrasts with key scheduling, which typically refers to the internal handling of keys within the operation of a cypher.

Successful key management is critical to the security of a cryptosystem. It is the more challenging side of cryptography in a sense that it involves aspects of social engineering such as system policy, user training, organizational and departmental interactions, and coordination between all these elements, in contrast to pure mathematical practices that can be automated.

This type of security helps protect encrypted data, but, very importantly, also makes it easier to comply with a user’s “right to be forgotten” when data is deleted.

End-point protection: VSCs and User Identities

There are billions of end points in corporate networks, and companies must ensure they are all protected to comply with GDPR.

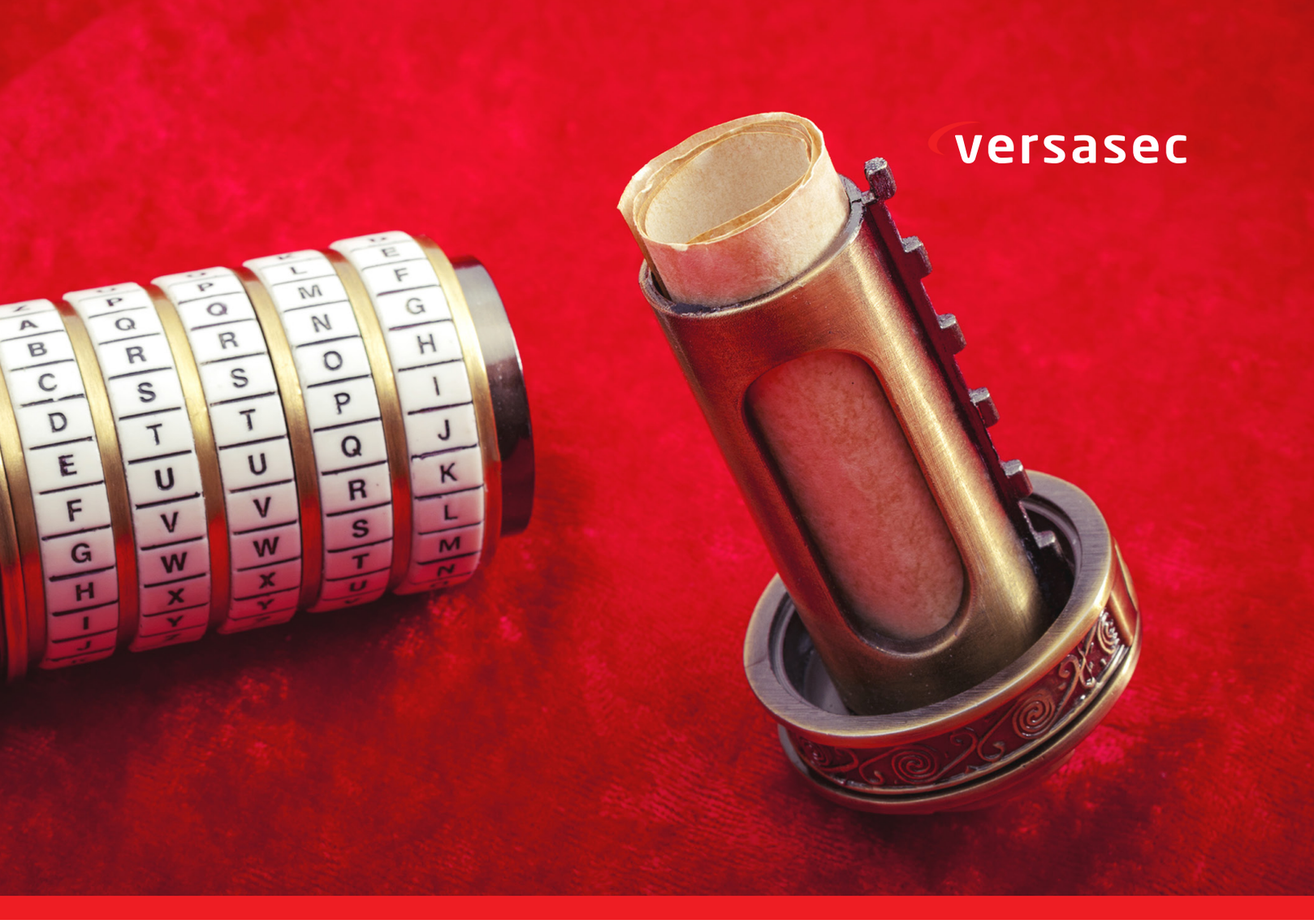
With an ever-growing mobile, global workforce, virtual smart cards (VSCs) are playing an increasingly important role in data security.

Virtual Smart Cards (VSCs) enable two-factor authentication (2FA) on a user's device without making use of extra hardware, such as smart card readers and USB tokens. VSCs are excellent for protecting companies' IT systems from external threats such as hacking and other unauthorized access from external devices.

This technology revolves around the use of the Trusted Platform Module (TPM): this is hardware that comes pre-installed in any modern computer. For users with Windows 7 onwards, VSCs can be created and the key is cryptographically-secured in the TPM.

Among the many benefits of VSCs are ease-of-use, strong two-factor authentication (2FA) and management for mobile workers, full security lifecycle management and overall cost-effectiveness.

By making use of VSCs, IT administrators see a significant hardware cost savings and faster deployments.



Other important technologies that complete the GDPR compliance story

No one security solutions can fully meet GDPR compliance. Other helpful technologies include encryption, threat protection and anti-virus options.

For most companies, addressing the GDPR requirements will involve adding some type of encryption methodology, both for data stored on-premise and in the cloud.

Threat protection solutions are required to help combat phishing, malware and DDoS attacks.

For example, data found on servers, in storage mediums, and networks must be secured, ideally by use of encryption. Types of data that must be encrypted include files, databases, applications, network data, virtual machine data, and more.

Other solutions that can help companies on their compliance journey include antivirus and anti-malware software, as well as back up & recovery software.

Companies deploying varied technology solutions will be the most effective in complying with GDPR.

How Versasec can help with GDPR Security Compliance

Choosing the best partner for each security area of GDPR is critical; Versasec is the best choice for secure identity and access management.

For a partner that can address the user identity challenges, Versasec is a logical choice because of its ability to fully manage the multi-factor authentication solutions that make it nearly impossible for unauthorized users to gain access to data. By implementing systems that manage strong authentication solutions, such as smart cards and virtual smart cards, companies are taking a crucial step in protecting their data.

Versasec's vSEC:CMS identity and access management (IAM) solution can play a critical role in the security requirements by ensuring companies can meet their audit requirements for user identification and credentials.

Versasec provides enabling IT security products centered on the usage of security devices such as smart cards and virtual smart cards. Our state-of-the-art solutions enable customers to securely authenticate, issue and manage user credentials more cost effectively than other solutions on the market.

Versasec products feature the following:

- **Fast installation and integration**
- **No (or limited) need of dedicated hardware**
- **Intuitive and efficient user interface**
- **Highest security levels**
- **No hidden costs**
- **vSEC:CMS software tools that securely manage smart cards**

Links to helpful resources

vSEC:CMS Product Information: https://versasec.com/products.php
Versasec Company Blog: https://versasec.com/blog/
Versasec YouTube Channel: https://www.youtube.com/versasec

Contact us to discuss GDPR or other security needs.

Visit us here and then select CHAT: https://versasec.com/
Download a trial version vSEC:CMS: https://versasec.com/registration.php
Email: info@versasec.com