DOING BUSINESS IN THE EU…
ARE YOU COMPLIANT?

A look at the EU's latest General Data Protection directive (GDPR) and the new PCI DSS and how BioSig-ID meets regulatory statutes to keep you in compliance.

By: Jeff Maynard, Founder, President and CEO, Biometric Signature ID

Case Study

GDPR Compliance Overview

This EU compliance regulation and the new PCI DSS will have a far reaching impact for organizations throughout the world.

The European Union (EU) General Data Protection Regulation (GDPR), adopted in April 2016, is a regulation that is intended to broadly and conclusively provide data privacy and security protection for residents of the EU. It becomes effective May 25, 2018. The GDPR is binding on all 28 EU member states and will immediately repeal previous data regulations, including the 1995 EU Data Protection Directive.1 The GDPR has a wider reach and broader scope than the EU Data Protection Directive. ***The GDPR can in many cases apply to U.S. higher education institutions and companies if those entities control or process data about residents of the EU.***

The GDPR imposes a variety of data privacy and data security requirements that organizations must follow, including:

- Data security practices
- Personal data usage and privacy restrictions
- Data breach reporting requirements
- Personal data consent collection requirements

If your organization suffers a data breach, under the new EU compliance standard, the following may apply depending on the severity of the breach:

- Your organization must notify the local data protection authority and potentially the owners of the breached records
- Your organization could be fined up to 4% of global turnover or €20 million

Exceptions to the Rule:
However, GDPR does provide exceptions based on whether the appropriate security controls are deployed within the organizations. For example a breached organization that has rendered the data unintelligible through encryption to any person who is not authorized to access the data, is not mandated to notify the affected record owners.

The chances of being fined are also reduced if the organization is able to demonstrate a " Secure Breach" has taken place.

Addressing GDPR Compliance:
To address the GDPR compliance requirements, organizations may need to employ one or more different encryption methods within both their on-premises and cloud infrastructure environments, including the following:

- Servers, including via file, application, database, and full disk virtual machine encryption
- Storage, including through network-attached storage and storage area network encryption
- Media, through disk encryption
- Networks, for example through high-speed network encryption

In addition, strong key management is required to not only protect the encrypted data, but to ensure the deletion of files and comply with a user's right to be forgotten.

Organizations will also need a way to verify the legitimacy of user identities and transactions, and to prove compliance. It is critical that the security controls in place be demonstrable and auditable.

GDPR expects organizations to stay in control of their data to ensure that it is accessed and processed by authorized users only when appropriate. The control requirements are covered in Articles 5, 25, and 32.

According to GDPR organizations must:

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

Moving Beyond Pins & Passwords:

The GDPR does not specifically mandate two-factor and multifactor authentication solutions per se, however a careful read of the regulation leaves no doubt that if you leave simple, static passwords in place and you are breached, auditors will come for you.

Multi-factor authentication is the first line of defense in any scenario. Strong authentication controls which users have access to the network and the resources found within. By assigning credentials to individuals, organizations can track access to resources to monitor internal risks. Multi-factor authentication also makes it more difficult for unauthorized users to access sensitive resources. For both known and unknown threats, multi-factor authentication raises the barriers to data access making it easier for an organization to stay in control of their data.

Unlike prior laws, the GDPR takes the position that residents of the EU should not be deprived of security and privacy protections solely because a business or organization that targets those residents is located elsewhere.

It's important to note, that no single solution will make an organization GDPR compliant. The regulation is too broad – covering everything from governance to contractual obligations. However deploying measures such as MFA will go a long way to maintaining best practices and mitigating future data breaches.

Thankfully for BSI clients (both present and future), our state-of-the-art authentication system meets the litmus test put forth by the GDPR. Not only is our MFA biometric solution the only one of its kind, but we provide all of the necessary forensics and reporting that you would need to accurately maintain sensitive personal information. With our ability to revoke and replace credentialing at any time, the answer is clear. For those doing business in the EU or working with EU citizens, BioSig-ID is the biometric solution of choice.

Multi-Factor Authentication Good Practices
Satisfies PCI DSS and meets the GDPR requirements

Both the PCI DSS and the GDPR aim to ensure organizations secure personal data. The PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers and service providers. It also applies to all other entities that store, process or transmit cardholder data or sensitive authentication data.

The GDPR focuses on European residents' personal data. The important difference is that the GDPR is less prescriptive than the PCI DSS. The GDPR provides guidance on what needs protecting but does not provide a detailed action plan. Conversely, the PCI DSS details clearly what needs to be achieved and provides a clear methodology for securing cardholder data.

The PCI DSS as a tool to achieve GDPR compliance:
The PCI DSS establishes a set of controls for keeping cardholder data secure, supported by a regulatory framework. If deployed to the rest of the business – without extending the cardholder data environment – these same controls and processes could provide organizations with a head start in meeting the sixth principle of the GDPR (integrity and confidentiality). This principle requires data controllers and processors to assess risk, implement appropriate security for the data concerned and, crucially, check on a regular basis that it is up to date and that controls to protect it are working effectively.

The first change to Requirement 8.3 in **PCI DSS** is the introduction of the term "multi-factor authentication" rather than the previous term "two-factor authentication", as two or more factors may be used. By changing this terminology, two factors of authentication becomes the minimum requirement. Two factors has also meant in the past 2 similar factors (sic 2 of the same or multi-layer). Example you know a password and you are then asked ask a security question – BUT these are not multi-factor as described below.

Multi-factor authentication requires the use of at least two of the three authentication factors as described in PCI DSS Requirement 8.2:

- Something you know, such as a password, PIN or the answer to secret questions
- Something you have, such as a token device or smartcard
- Something you are, such as a biometric

A PCI breach is a GDPR breach:

- Under the GDPR, personal data "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4, clause 1)

- As defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms, cardholder data is, at a minimum, the full primary account number (PAN), but may also appear in the form of the full PAN plus one of the following: cardholder name, expiration date and/or service code

Where cardholder data includes any information that could be used to identify the individual, then it is personal data as defined by the GDPR. If that data is compromised in a data breach, the breached organization is likely to be liable under both the PCI DSS and the GDPR.

It’s important to note that all reporting and fines because of a data breach fall within the legalese of the GDPR code.

For a description of the industry-accepted principles and best practices for a MFA implementation, select this link. Information Supplement – Multi-Factor Authentication version 1.0