{e}mazzanti technologies
TECHNOLOGY STRATEGIES FOR BUSINESS GROWTH.

Technology Partners Enable GDPR Compliance

The European Parliament adopted the General Data Protection Regulation (GDPR) in April 2016. GDPR provisions require businesses to protect the personal data and privacy of EU citizens. The regulation applies to every company that processes personal data of EU residents, regardless of where the company is located, hence many U.S. companies must achieve GDPR compliance.

Beginning in May 2018, the EU gave regulatory agencies greater powers to act against non-compliant organizations. Penalties include stiff fines of up to four percent of annual global revenue or 20 million euros, whichever is greater.

Implementing a plan for GDPR compliance can prove to be complex. Fortunately, a capable business technology provider can help organizations accelerate their response to the legislation and avoid the penalties.

Key GDPR Changes

The first step to GDPR compliance involves understanding the law. In general, the new regulations affect three main areas:

- **Personal Privacy** – Individuals have the right to access and correct errors in their personal data. They must have the ability to erase or export their personal information, as well as object to the processing of that data.

- **Security and Transparency** – Organizations must protect personal data with appropriate security measures and notify authorities of data breaches. They must provide explicit notice of data collection and obtain appropriate consents for processing data. They must clearly outline data policies and keep records of data processing.

- **IT and Training** – Organizations must train privacy personnel, employing a Data Protection Officer if required. They must audit and update data policies regularly and create and manage vendor contracts to ensure compliance.

Navigating GDPR Compliance

Compliance with GDPR regulations can prove challenging, requiring organizations to devote significant resources to the effort. So how can technology providers help organizations accelerate their response to the legislation and become GDPR compliant?

- **Data management and discovery** – The initial step is to discover personal data across your organization and protect it from unauthorized access. This includes regularly indexing and flagging sensitive data.

- **Access governance** – By managing user identity and access to sensitive data, organizations can more easily protect privileged activities and enforce data breach detection and notification.

- **Test data management and synthetic data generation** – Test data management (TDM) is the process of providing, distributing, and managing test data for development teams. By using synthetic data, organizations will avoid the privacy pitfalls associated with masking production data.

- **API management** – API management is the foundation for a future-proof GDPR-compliant architecture. It enables organizations to quickly and easily adopt rules for gathering consent and informing users about data policies.

Risks of Non-compliance

The GDPR regulations apply to all companies that process personal data of European residents. This includes companies with fewer than 250 employees where data processing impacts the rights of data subjects or includes certain types of sensitive personal data. In effect, the regulations apply to nearly all companies.

Violations of basic principles of the GDPR can result in fines that could prove devastating, particularly to a small business. There are two tiers of non-compliance:

- **Lower Tier –** These infractions generally involve failing to adequately integrate data protection by design into business operations. Fines can be imposed of up to 10 million euros or two percent of the organization's annual global revenue, whichever is greater.

- **Higher Tier** – These involve more serious infringements on an individual's privacy rights and freedoms. Fines in this category can reach as high as 20 million euros or four percent of annual global revenue.

In addition to fines, other penalties can prove incredibly harmful to your business. Violators may suffer a withdrawal of certification or a ban on processing personal data. Damage control can be costly to both the wallet and the reputation.

Benefits of GDPR Compliance

If the risks of non-compliance fail to provide motivation enough, consider the benefits of complying with GDPR regulations. The law provides an opportunity to reevaluate and improve your overall cyber-security strategy and data management.

For instance, with the findings of an audit, you will eliminate redundant, obsolete and trivial files. In addition, the transparency and responsibility you demonstrate will help you build more trusting relationships with your customers and the public.

GDPR compliance also allows you to increase marketing return on investment. Once you implement an opt-in policy and have a data subject's consent to process their personal data, you will be able to increase the effectiveness of your digital advertising. You can tailor your message to the specific needs and habits of a clearly defined audience that has more interest in your brand.

GDPR Compliance Partner

A business technology firm that is well-versed in GDPR regulations can prove to be an invaluable trusted partner in your compliance journey. The experts at competent technology providers will broaden your understanding of GDPR compliance, identify issues you may not have considered, help you realize the myriad benefits of GDPR compliance, and direct or assist in your compliance effort.