SKODA MINOTTI
CPAs, BUSINESS & FINANCIAL ADVISORS

GDPR Compliance: Are You Ready?

By Christopher Denton

The European Union (EU) enacted the General Data Protection Regulation (GDPR) on May 24, 2016, but allowed a two-year grace period until May 25, 2018 where it was not enforced. It replaces the 1995 Data Protection Directive and unlike its predecessor, it is binding and requires no extra regulation from EU member states.

The GDPR is designed to protect personal data of any individual in the EU including citizens (either at home or abroad) and visitors to the EU, regardless of where the organization processing or controlling the data resides in the EU.

What data does it protect?

- Identity information (e.g., name, address, ID numbers)
- Racial or ethnic information
- Geolocation data (e.g., locations, IP addresses, website cookies)
- Health and genetic data
- Sexual orientation
- Political preference

What are some of the big changes?

1. Scope – The GDPR crosses national boundaries and is consistently applicable and enforceable in every EU member state. In addition, it is enforceable on any organization regardless of whether that organization is located in the EU.
2. Supervisory authorities – Each member state is required to have a supervisory authority that will consistently apply GDPR and cooperate with each other.
3. Consent – Consent is now required to be explicit, presented in clear language, and separate from other matters.
4. Mandatory breach notification – Organizations are now required to notify supervisory authorities within 72 hours of a breach.

What rights do individuals have?

The GDPR also specifically provides for eight rights or freedoms for every data subject:

1. Right to be informed – Data subjects have the right to be informed on who is seeing or using their personal data.
2. Right of access – Data subjects have the right to know if their personal data is being processed and access that data upon request.
3. Right of rectification – If the data held by an organization is incorrect, the controller or processer is required to correct it.
4. Right to be forgotten – With some exceptions, if a data subject requests their data be deleted the controller must erase it without delay.
5. Right to restrict processing – With some exceptions, a data subject can restrict how their information is processed or used.
6. Right to portability – Data subjects have the right to receive their personal data in an easily read format and, if feasible, personal data should be transmitted directly from one controller to another.
7. Right to object – Data subjects have a right to object to how their data is processed.

8. Right to not be subject to decisions based on automated processing – Data subjects have a right not to be subject to profiling which produces legal effects or similarly affects them.

How can I prepare?
First, executive management should set a tone at the top regarding the urgency of GDPR and involve all business units in the readiness process. Personal data can reside anywhere and include HR, finance, marketing and operations. Involvement of each business unit is crucial to the data discovery process.

Data mapping or discovery should be conducted to carefully identify and document what data resides where. A data protection impact assessment (DPIA) should be conducted to identify, assess, and mitigate potential privacy risks. It is possible that if the data possessed by your organization is low risk, you may not need to be GDPR compliant.

Evaluate your cybersecurity program and how it addresses GDPR compliance. Are data privacy, protection and breach identification procedures in place?

Do you need to make sure your organization is compliant with a gap analysis or risk assessment? Are you interested in learning more about GDPR, SOC 2 examinations or other **risk advisory matters**? Please contact Chris Denton at 813-386-3879 or ***email Chris*.**