AICPA|Aon, here are some questions and actions CPA firms should consider.

Jul. 27, 2018

GDPR went into effect on May 25. According to Stan Sterna and Ken Mackunis of AICPA|Aon, here are some questions and actions CPA firms should consider.

What are the basics of the EU General Data Protection Regulation?

- Upon becoming aware of a breach impacting this data, the controller must provide notice to the supervisory authority within 72 hours, where feasible.
- Sanctions and fines can be imposed by each applicable supervisory authority, up to 20 million Euros or 4% of global revenues upon businesses in violation.
- The effective date is May 25, 2018.

How will EU-GDPR impact your firm?

- CPA firms and related entities typically have access to the personal data of:

o their employees, independent contractors, and individual clients.

- Firms also may have access to this data for:

o the employees, independent contractors, and customers of their business clients.

- This occurs in part through use of client portals and software supplied by third party providers. Such software is used in rendering employee benefit plan and human resource administration, payroll processing, and medical billing services.

What are some of the compliance requirements of EU-GDPR?

- Duties are imposed upon both controllers and processors of personal data, defined terms in the regulation.
- Under the regulation, a controller "… determines the purposes and means of the processing of personal data".

o Both third party cloud hosting providers and clients may qualify as controllers.

o Under some circumstances, CPA firms or related entities also may qualify as

agreement to submit to audits by the controller.

- Under the regulation, a processor "… processes personal data on behalf of the controller".

o Processors are required to notify the controller of a personal data breach "without undue delay".

Actions your firm needs to consider

- Understand where and how your firm uses and stores personal data of EU individuals.
- Review the regulation with technology professionals and legal counsel to understand your firms' obligations as a controller or processor of personal data.
- Implement a compliance and monitoring plan.
- Review your existing security controls.
- Assess your third parties' personal data security standards.
- Be prepared to report data breaches promptly, and within 72 hours.

Firm Management • Technology