European Union General Data Protection Regulation: How Can It Impact U.S. CPA Firms and their Clients?

By STAN STERNA and CATHY WHITLEY

On May 25, 2018, the General Data Protection Regulation (EU-GDPR), adopted by the European Union (EU) in 2016, went into effect and applies to all entities processing the personal data of individuals residing in the European Union, regardless of either the location of the entity or where the data is processed. It is designed to protect the privacy of EU citizens' personal information online. EU-GDPR imposes extensive privacy requirements on companies that have access to or process this information, in addition to reporting requirements in the event of a data breach.

CPA firms that have employees, independent contractors or individual clients who reside in EU member countries, or have access to the personal information of individuals who reside in these countries, are required to comply with the regulation. This includes the personal information of individuals who reside in the U.S., but maintain citizenship in any of the EU member states.

To understand how CPA firms and clients may be impacted, it is important to first review several definitions included in EU-GDPR.

Personal data "includes data that can be used to identify an individual, either directly or indirectly, … by reference to an identifier, such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."

A *controller* is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."

A *processor* is "a natural or legal person, public authority, agency or other body which processes personal

data on behalf of the controller." [1]

CPA firms typically have access to personal data for both their employees and independent contractors utilized by the firm, as well as for individual clients when rendering certain types of professional services. Examples of services that typically include access to this data include:

- Estate planning;
- Family office;
- Financial planning;
- Investment advice;
- Succession planning;
- Tax compliance and planning.

CPA firms should complete an investigation to determine whether any of its employees, independent contractors or individual clients either reside in one of the 28 EU member states or maintain citizenship in them.

Additionally, CPA firms may have access to the personal data of the employees, independent contractors and customers of their clients when rendering the following services to businesses, governmental and not-for-profit entities:

- Employee benefit plan administration;
- Payroll processing;
- Medical billing and coding.

CPA firms performing these services for clients, as well as any other services that allow the CPA firm access to the personal data of the client's employees, independent contractors or customers, should also complete an investigation with the client to determine whether any of the client's employees, independent contractors or individual customers reside in one of the 28 EU member states or maintain citizenship in them.

The compliance requirements of EU-GDPR are significant. Following are a few important facts.

Controller or Processor of Personal Data – CPA firms, their third party service providers and their clients may qualify as a controller or processor of personal data under the regulation. The duties imposed on controllers are broader than those imposed on processors. For example, in the event of a data breach that may impact personal data, a controller is required to notify the supervisory authority in the EU member state without undue delay and within 72 hours of discovering the breach. All 28 member states have their own supervisory authority.

Compliance by Third Party Service Providers – Depending on the level of control exercised, third party service providers that host client data on the internet for CPA firms may qualify as a controller under the regulation when they have access to the personal data of individuals residing in the EU. This includes firms hosting client portals and providers of online tax software. It is recommended that CPA firms investigate what these providers are doing to ensure compliance with EU-GDPR.

Written Contracts – Controllers are required to have written contracts with service providers qualifying as a processor of personal data. These contracts have specific requirements under EU-GDPR. For example, they must specify how the processor handles data and require the processor to both implement appropriate safeguards required under EU-GDPR and agree to submit to audits by the controller as required to ensure compliance with the regulation. CPA firms may receive updated contracts from clients that include these required provisions.

Supervisory Authority – Each of the 28 EU member states have their own supervisory authority under EU-GDPR and have the right to impose fines and sanctions upon businesses found to be in violation, including U.S.-based businesses.

Fines and Sanctions – Fines can range up to 20 million Euros or 4 percent of global revenues, whichever is higher. Sanctions can include suspending data flows to a company, reprimands and bans on processing of data.

EU-GDPR Impact

Both CPA firms and their clients should be analyzing how EU-GDPR applies to their business operations and evaluating their privacy and security protocols. This will require the collaboration of senior management and company stakeholders, experts in privacy and security, and legal counsel.

While CPA firms are required to maintain client confidentiality under applicable professional standards, and are likely already familiar with federal and state privacy laws, EU-GDPR adds a layer of compliance obligations that clients and CPA firm management may be unfamiliar with. CPA firms should consult with legal counsel possessing expertise in EU-GDPR throughout this process.

Business clients will have varying levels of awareness and knowledge of EU-GDPR and how it impacts them. While many businesses may not operate outside of the U.S., they may process the personal data of individuals in the EU in the context of offering goods or services to people in the EU or monitoring people's behavior as far as that behavior takes place within the EU.

It is important for CPA firm management to understand the general requirements of EU-GDPR and be prepared to discuss this with clients. Firms that provide client portals that clients can populate with their own data should be made aware that any client portal use agreement they executed remains applicable.

New Service Opportunities

There are extensive external resources available to CPAs and their clients regarding EU-GDPR. Additionally, this presents new service opportunities for CPA firms. Those with expertise in privacy and security consulting services, or the preparation of SOC 2 and 3 reports and SOC for cybersecurity examinations, may be able to assist clients in evaluating their controls over personal data covered by EU-GDPR.

ABOUT THE AUTHORS

STAN STERNA is vice president at Aon Affinity Insurance Services.

CATHY WHITLEY is risk advisor at Aon Affinity Insurance Services.

[1] See Article 4, EU-GDPR https://gdpr-info.eu/art-4-gdpr/