#ForensicPerspectives

GDPR Basics

When?

GDPR went into effect on May 25, 2018.

What is it?

The General Data Protection Regulation is essentially a set of new rules that govern the data of EU citizens and gives them more control over how organizations use it.

Who will it impact?

The new regulation applies to organizations located within the EU as well as to those outside of the EU that offer goods or services to EU citizens, or monitor their behavior.

Why does it matter?

Any entity that collects and stores personal information, such as financial or health details, from its clients, customers, or visitors to a website that it controls will need to update its practices and ensure protection of that data.

Where does is apply?

Both within and outside of the EU. The new regulation focuses on the individual and not the location of the data so it applies beyond the EU to any organization that processes the data of an EU citizen.

Eight elements of compliance

01

Appoint a data protection officer

Although not a requirement in the prior Data Protection Directive, organizations that process sensitive personal data must now appoint a data protection officer to monitor their activities to ensure proper retention, processing, and removal of information.

02

Maintain records of data processing activities

Data controllers and processors must maintain (and provide to the authorities, if requested) records that reflect basic contact information, as well as the purposes of and protocols associated with the processing activities.

03

Draft privacy impact assessments

Organizations that anticipate processing economic status, health, location, personal preferences, race/ethnicity, or sexual orientation data must conduct a Privacy Impact Assessment prior to doing so. This replaces an earlier notice requirement in the Data Protection Directive.

CRA Charles River Associates

04 Understand how to transfer data to third countries

Companies cannot transfer personal data to a country outside the EU that does not have adequate data protection regulations. Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Iceland, Israel, Isle of Man, Jersey, Liechtenstein, New Zealand, Norway, Switzerland, the United States, and Uruguay meet that standard.

05 Honor the right to be forgotten

The "right to be forgotten" requires organizations to identify and remove an EU citizen's personal data upon request or justify why it cannot do so, making information governance critical.

06 Implement the right to data portability

Individuals have the right to ask the controller of personal data they directly provided to that entity to transfer it to another controller.

07 Plan for a data breach

A data controller must report a breach within 72 hours, or explain why it could not do so, and alert the person to whom the information belongs. The processor must notify the controller. Both will need advanced technology that can adhere to the accelerated time frame.

08 Recognize data controllers and processors

Organizations that collect personal data, but designate others to store or transform it are "controllers," who need to ensure data protection, conduct a privacy impact assessment, develop a risk mitigation plan, and anonymize data. "Processors" work for "controllers" and must assure them they are following recognized standards for processing any personal data, maintaining proper records, applying adequate security, and notifying them in the event of a breach.

Avoid penalties for non-compliance

Under the GDPR, the European Commission can impose fines of up to 4% of total global revenues or 20 million euros (whichever is greater) for compliance failures. CRA's Forensic Services team routinely helps companies and their counsel independently respond to allegations of non-compliance. Contact an expert listed below to learn more.

Kristofer Swanson, CPA/CFF, CFE, CAMS
Vice President & Practice Leader, Forensic Services
+1-312-619-3313 | kswanson@crai.com

Josh Hass, CFE, CEDS
Vice President, Forensic Services
+1-212-520-7139 | jhass@crai.com

CRA's Forensic Services Practice and its state-of-the-art digital forensics, e-discovery and cyber incident response labs are ISO 27001:2013 certified. We also maintain private investigator licenses in multiple jurisdictions, as listed on our website (www.crai.com).

CRA Charles River Associates