Contact Us

GDPR Overview

Document change record

Date	Version	Author	Change Details
25 May 2018	1.1	Internal	Initial
20 March 2020	1.2	Graydon McKee / Ramesh Maturu	Update to reflect legal changes
18 March 2021	1.3	Gray Wolfe	Update to reflect legal changes
17 March 2022	1.4	Gray Wolfe / Iain Struan / Ramesh Maturu	Update to reflect legal changes
14 March 2023	1.5	Iain Struan / Ramesh Maturu	Update to reflect legal changes, re-write
22 July 2024	1.6	Joel Lawhon	Style and layout

What is GDPR?

The GDPR is a European Union ("EU") regulation that imposes obligations on companies that collect, store, or process the personal data of EU residents. Any organization that holds the personal data of EU residents is covered by the GDPR, regardless of the organization's physical location. At Pyramid Consulting, Inc. we are a firm supporter of the strong data privacy and security principles the GDPR highlights, and we comply with applicable GDPR regulations.

What is personal data?

The definition of "personal data" under the GDPR is broad and effectively covers any information that may identify an individual.

Pyramid Consulting, Inc.'s commitment: what are we doing to protect you?

We take our data privacy and protection responsibilities very seriously and are committed to ensuring the security and protection of the personal data that we process or control to provide a compliant and consistent approach to data protection. As such, to achieve compliance with the GDPR, we have amended our existing policies and procedures and implemented additional processes. These changes are in areas including, but are not limited to, data processing, information security, data transfer, third-party processors, data protection, and breach notification. We have amended our privacy notice and require all Pyramid Consulting,

Inc. employees who touch or manage personal data to complete additional data privacy and security training that is GDPR-focused. We also have implemented appropriate technical and security processes to ensure that we comply with our GDPR obligation.

What are your rights?

Your rights under the GDPR include the right to see a copy of any information we hold about you, and the right to request that such information be fully deleted from our systems (although we may be required to keep some records to ensure that you are not contacted in the future or to comply with our HR and legal obligations).

How can you contact us about GDPR-related questions?

We welcome your questions or comments about GDPR, this commitment statement, and our privacy or security practices Feel free to contact us at dpo@pyramidci.com.

Changes to this statement

Pyramid Consulting, Inc. will update this commitment statement as appropriate with additional information relating to further developments concerning our GDPR compliance program.

2021 GDPR updates

Broadened definition of joint controller

A joint controller refers to a situation where two or more people or entities oversee the collection and protection of customer data. These joint controllers -- data owners, really -- determine together why and how to process personal data. Joint controllers will often have a shared objective and shared purposes. They are fully and independently responsible for the correct handling of customer data. In the event of non-compliance with any GDPR provisions, both data controllers can be held responsible and face possible sanctions. The joint controller relationship arises more commonly than many people realize, however. For example, a simple activity such as managing an organization's social media presence or displaying a social media plugin on your website makes you a joint controller with that social media network.

Removal of the privacy shield

The GDPR's so-called privacy shield was intended to make it easier for data to be transferred from European organizations and institutions to their U.S. counterparts. This facilitated a smoother business relationship and enabled tech organizations such as Google, Yahoo, and Apple to easily share data on their customers with their U.S.-based parent corporations. However, the relative freedom the privacy shield gave to U.S. organizations to process data under U.S. legal provisions has been revoked. Instead, U.S. organizations that have previously used the privacy shield mechanism have now had to adopt standard EU GDPR contractual clauses to use the customer data of European citizens. Because the U.S. and EU have traditionally had

opposite views regarding the requirement of consent to work with personal data, this development is important because it effectively forces U.S. organizations to abide by much more stringent EU privacy laws.

All about cookies

In the past, there was ambiguity in the GDPR regarding cookies and the consent users must give for their use. In the new iteration of the GDPR, EU lawmakers have made it clear that explicit permission is required from site visitors to install cookies on their computer(s). A visitor who simply browses through a website does not imply consent; consent must be given in an undisputed and straightforward way for it to be valid.

The topic of "cookie walls" has also been addressed, and the EU lawmakers have made their view on the topic known. "Cookie walls" are designed to force users to provide their consent since without this consent (and cookies), some websites are inaccessible. Additional updates to the cookie policy and specifically cookie walls are expected to be amongst the next updates to the GDPR.

Shift away from third-party data processing

In something not so much a change to the GDPR but an effect of the changes, IoT companies are shifting away from third-party data processors in favor of keeping things in-house. This is hardly a surprise considering the risks associated with sharing data outside of your organization, especially when taking the joint controller clause and definition updates into consideration.

Implications of these changes to data strategy

This set of changes was one of the biggest since the introduction of the GDPR and it has sent shockwaves through the privacy community. It seems that the EU commissions strategy to get to adopt the GDPR and enforce it is the threat of large financial fines in the event of non-compliance. Bearing this in mind, organizations have scrambled to ensure compliance with the provisions of the GDPR.

An overall change in data strategy — Privacy comes first

The net result of the latest changes to the GDPR is that organizations worldwide are now taking the legislation and its provisions more seriously, and view data as a strategic tool and risk that must be managed. European customers are enjoying a higher level of privacy than ever before, and it is inspiring other countries to adopt the same level of protection for their citizens.