GDPR and Magento
New Steps to Protect Privacy in 2018

The EU General Data Protection Regulation (GDPR) goes into effect on May 25, 2018 and Magento has been working to make sure we are prepared and our systems are compliant.

The GDPR is the EU's new legislation that introduces substantial and specific changes to existing data protection laws to expand the scope of data protection. In particular, the new rules impact how companies that do business in the EU may collect and handle personal information.

Magento sees GDPR as an opportunity to further strengthen and clarify our already-firm commitment to customer data privacy. Protecting personal data has always been one of our priorities, and we're eager to embrace and comply with the EU's new rules.

Here's an overview of what GDPR is all about and what it will mean from Magento's perspective.

Understanding GDPR

GDPR is a single privacy framework that aims to ensure that individuals' personal data is handled with caution and care. It applies to organizations established in the EU that process personal data and to organizations based outside the EU that either offer goods or services directly to individuals in the EU or monitor behavior of individuals in the EU (for example, through customer profiling).

The GDPR regulations are designed to protect a wide range of information — including anything that could be used to identify a person in any way, even indirectly. That means, for example, that names, email addresses, photos, ID numbers, health data, biometric data, location data, and financial data are all included. Also included are IP addresses, social network posts, and web-based cookie data. If something is in any way relevant to the "*physical, physiological, genetic, mental, economic, cultural, or social identity*" of a person, it counts as personal data.

Companies can store or process this type of data only when the associated individual explicitly authorizes it — and even then, GDPR puts firm limits on the length of time the data can be kept.

Once GDPR comes into effect, any organization found to be in violation could be fined up to 4% of its group's global annual revenue or €20 million (about $23.7 million in current U.S. dollars), whichever is higher.

Magento's Role in GDPR Compliance

Magento has both customers that are located in the EU and customers that serve individuals in the EU, and GDPR compliance is a responsibility we take seriously.

Under the GDPR, Magento's EU customers are considered "data controllers" which entities them to determine how personal data is collected and used. Magento itself is a "data processor" because it processes personal data at the controllers' direction. That's all a fancy way of saying we'll be standing by and ready to support our customers' instructions and efforts to comply. Proper data handling is a shared responsibility, and all organizations that work with personal data need to have their own layers of protection in place.

To fulfill our obligations as a data processor, Magento has implemented changes in the following areas:

1. Policies/Contracts

We have been proactively reviewing and updating (where required) our customer and partner contracts and our policies and processes surrounding privacy and data protection.

2. Technology

Magento's products have strong architecture and security features built into their cores, so no major modifications are necessary to enable merchant compliance.

We are working closely with legal and engineering experts to assess our products to better assist customers to identify what personal data is being stored and where that data resides in an effort to help customers comply with GDPR-related transparency or data removal requests.

Our security team is also conducting detailed security audits across all Magento products.

Other Considerations for Magento Customers

All hosted Magento products have options for data to be stored in EU locations (Ireland for both Magento Business Intelligence and Magento Order Management and Ireland, London, or Frankfurt for Magento Commerce Cloud). Magento will not store personal data at a location outside of a customer's stated preference.

It's worth noting, however, that Magento Marketplace extensions may store personal data in different locations from the core eCommerce platform and may also send data to external services. It's up to customers to be aware of the data usage policies and behaviors of any extensions they choose to use.

In general, Magento customers should review all services and contracts connected to third-party companies to confirm GDPR compliance. Customers should also consult with their own legal advisers to decide what GDPR requirements apply to them and how they can best address those issues. Magento cannot provide legal advice.

For more information on GDPR, Customers may wish to refer to the European Commission's website:

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en