Magento GDPR Frequently Asked Questions

Whom does GDPR impact? Does this only impact European Union (EU) based companies?

The new regulation provides rules that govern how companies may collect and handle personal information, and impacts many companies doing business in the EU, even those that are not established in the EU. Companies that are not established in the EU will need to comply with the GDPR if they are:

- Offering goods and/or services to individuals in the EU (regardless of whether a payment for such goods or services is required); or
- Monitoring the behavior of individuals in the EU (such as through customer profiling).

Is Magento GDPR compliant today?

We are ready for the GDPR. And, we have implemented several initiatives across sales, marketing, operations and product.

Are changes required to the Magento products to be compliant with GDPR?

There are no anticipated material changes required for our products to be compliant with GDPR. GDPR provides individuals with rights with respect to the processing of their personal information, including access to, correction of, and/or deletion of personal information when requested by the individual. Enabling these rights doesn't require customization of the Magento products but does require a process to be in place by which Magento will assist merchants with such requests if/as required. Magento is ready to assist our merchants with these requests. Additionally, we enable our merchants to address such requests of its end users by providing certain documentation as referenced below.

Magento's product and technology leadership has taken inventory of the Magento products by mapping all personal information that is stored by the Magento applications.

We will be providing documentation to our partners and customers. We believe this will make it easier for our merchants to comply with such individual requests.

Separately, a relevant data processing agreement will be in place with any subprocessor that will be processing Magento's merchants' and merchant end user personal information on behalf of Magento, to address all aspects of GDPR compliance, including individual data subject rights requests discussed above.

Are there Magento product features to help with compliance?

Yes. We have carried out a data mapping exercise to identify all locations where personal information is stored in our system. You can find the data mapping documentation for the Magento software on Magento's official developer documentation site (Magento 1.x, Magento 2.x).

This documentation covers Magento Commerce (cloud), Magento Commerce (on premise), and Magento Open Source. Separately,internal documentation has been prepared for Magento Order Management and Magento Business Intelligence to assist our support team in responding to data rights requests. Admin tools, in the Magento Admin Console, automate the listing, exporting, and deletion of personal information may be considered in the future – depending on the demand from our merchant base.

Does GDPR require merchants (and their customers) to agree to the ways in which their personal information is used? How is this achieved in the Magento products?

It has been and continues to be important, regardless of GDPR, that individuals understand what personal information is collected, how and for what purposes the information is being utilized, and if that personal information will be disclosed to third parties and for what purpose(s). Individuals must also understand their choices and access rights with respect to such information. Our Privacy Policy addresses these points for information that is collected through Magento websites. With respect to the personal information that is collected by our merchants, it always has been and continues to be, regardless of GDPR, the responsibility of the merchant to maintain a compliant privacy policy and that it's disclosed appropriately to its customers.

Under GDPR, individuals (end users) can make a request to merchants to access, correct, and/or delete (among other rights), their personal information collected by the merchant. Does Magento provide a feature to assist merchants in its compliance with these types of requests?

Magento is providing documentation to all merchants to clearly lay out what personal information is stored by the Magento Commerce application and where that personal information is stored to assist merchants in addressing these individual rights requests.

Merchants using Magento Commerce (cloud or on premises) may work with their Magento developer(s) to use the documentation provided by Magento to extract, correct or delete personal information.

Merchants using Magento Commerce (cloud) and Magento Order Management will have the option to contact Magento's support team in connection with a data gathering, correction and/or deletion request, if needed. Additionally, Magento is building internal tools for our support team to assist in these processes and may make them available for merchants if there is ample demand for them in the future.

By default, Magento Business Intelligence syncs data from Magento Commerce. Therefore, changes to Magento Commerce will flow through to Magento Business Intelligence as well. In case of any customizations made within Magento Business Intelligence, merchants have the ability to conduct these compliance processes in a self-serve manner from the Magento Business Intelligence user interface.

Magento of course will also assist and/or advise the merchant in the event an individual rights request comes up, if/as needed.

How do merchants address GDPR compliance on their stores (e.g. disclosing their privacy policy)?

Just as Magento has reviewed and updated our privacy practices and policies, merchants should be engaging in their own privacy reviews.

What is Magento's stance on encryption being a requirement for GDPR?

Organizations should implement appropriate technical and organizational measures to ensure a level of security that is appropriate to the risk. Such measures may include encryption, but it is not a mandatory requirement under the GDPR. In GDPR parlance,

when determining appropriate technical and organizational measures, organizations should take into account the costs of implementation and the nature, scope, context and purposes of the processing.

Magento has conducted its own evaluation and assessment as an organization, and at this time, Magento believes implementation of database level encryption will significantly increase the support and maintenance costs and efforts of our merchants and partners. Of course, Magento Commerce (cloud) customers already benefit from disk-level encryption at rest and encryption in transit, today.

What are the GDPR requirements around data retention and are there any features in the current product(s) or planned for the future that help customers comply with those requirements?

Personal information should be retained for only so long as needed or permitted in light of the purpose(s) for which was retained. For example, Magento uses the following criteria to determine our retention periods: (i) the length of time we have an ongoing relationship with and provide services to the merchant or (ii) when we have an actual or potential legal obligation.

There are no product feature changes required to meet compliance. Generally speaking, merchants have a minimum of thirty (30) days from their Magento contract termination to retrieve customer content hosted on the Magento products. Of course, a merchant must comply with its own data retention practices around any content it or its end users place onto the platform.

How is opt-in handled in Magento Commerce? Does opt-in cover all the necessary services? How can a merchant add to or customize the default opt-in? Is this documented? Do the marketing features (like customer segments) need some opt-in or disclosure similar to the cookie notifications?

Magento Commerce allows for merchants to create and manage Customer Attributes. These can be required for customer account creation and stored with the customer record in Magento. Please refer to the Magento User Guide for more information. Magento Commerce also provides a feature that merchants can use to require explicit opt-in during account creation.

Magento Commerce's segmentation tools rely on authentication to access customer's account information. For unauthenticated shoppers, segmentation can only be done based on activity within the active session, such as number of items currently residing in

the cart. Magento Commerce stores a long-term cookie on the shopper's machine that connects to the following info stored within Magento Commerce:

1. Shopping Cart
2. Currently Compared Products
3. Comparison History
4. Recently Viewed Products
5. Customer Group Membership and Segmentation

Merchants have the ability to turn all five of these features off at the store level. The information stored in this cookie is anonymized.

How do extensions impact GDPR compliance?

When merchants purchase extensions from Magento Marketplace, or elsewhere, they contract directly with those extension sellers. Extensions may store personal data in different locations within the core eCommerce platform or send data to external services. Merchants must consider the data usage policies and behaviors of any extensions they use. In particular, services from and contracts with external companies should be reviewed by merchants for GDPR considerations. Starting May 25th, Magento will require all Extension sellers on the Magento Marketplace to provide their privacy policies.

Will white labeled offerings and bundled extensions be reviewed for any GDPR implications?

Yes. Merchants will be contracting with Magento for any white labeled offerings (e.g. Magento Shipping) to use these types of products and hence Magento is reviewing them for compliance. Merchants will be contracting with a 3rd party for any non-white labeled bundled extensions (e.g. dotMailer) but Magento is still reviewing their policies for compliance with GDPR.

What about Privacy Shield?

Magento is currently in the process of certifying to the Privacy Shield program (a privacy framework approved by the U.S. Department of Commerce, European Commission and the Swiss Administration to comply with data protection requirements), to cover personal data transfers from the European Economic Area and Switzerland to the US. In the meantime, Magento has put in place EU Model Clauses prepared by the European Commission to ensure that such transfers may be made.

Is there a certification for GDPR?

There are no certifications for GDPR compliance. Other certifications like PCI and SOC 2 are not specifically required, but help verify security practices and help Magento achieve the objectives of the GDPR.

Can Magento provide guidance to merchants on being GDPR compliant?

Merchants should engage their own legal counsel to help them understand what they must do to be compliant with the GDPR.

How is personal information transferred outside of the European Economic Area (aka cross-border data transfers) affected by the new GDPR regulations?

Just as in the pre-GDPR days, organizations have to have appropriate safeguards in place to transfer personal information outside of the European Economic Area. As mentioned above, Magento is currently in the process of certifying to the Privacy Shield program to seamlessly cover (without a lot of extra contractual language in each customer contract) personal data transfers from the European Economic Area and Switzerland to the US. In the meantime, Magento has put in place EU Model Clauses prepared by the European Commission to ensure that such transfers may be made. Separately, relevant data processing obligations will be in place with any sub processor that will be processing personal information of Magento's merchants and end users on behalf of Magento, to address all aspects of GDPR compliance, including cross-border data transfers.

Is a data processing agreement being used in contracts today?

When a merchant requests, we include a GDPR compliant data processing agreement in the merchant customer contract. For the rest, we will be updating new and existing customer contracts on a rolling basis to include a GDPR compliant data processing agreement, where necessary.

What are the options for EU customers to keep their data (including personal information) in the EU?

All hosted Magento products have options to host in EU locations:

- Magento Commerce (cloud) – Ireland, London, or Frankfurt
- Magento Business Intelligence – Ireland

- Magento Order Management – Ireland

Magento will not move personal data from the locations specified by the merchant. Magento might, however, have remote access to personal data stored in the EU from locations outside the EU. Magento has put in place appropriate safeguards for such remote access.