Marketing Personalization in the Age of GDPR

What is the significance of GDPR?

The GDPR will regulate the protection of personal data across the EU member states. The GDPR replaces the European Data Protection Directive of 1995. Because GDPR is a "regulation", it will become the law in the EU member states on May 25, 2018 without any additional actions by those states. This is in contrast to the previous "directive" which directed member states to create their own regulations within the scope of the European Data Protection Directive of 1995.

The previous regime led to differing data protection regulations across EU member states. Although member states can put in place laws and regulations in addition to the GDPR, it is expected that GDPR compliance will be the focus of member states for the foreseeable future, thus providing Acquia and other entities doing business in the European Union with the regulatory certainty needed to offer its products and services to customers in region. In addition, Acquia will monitor member state-specific laws and regulation going forward.

Acquia welcomes the GDPR as an important step forward in harmonizing the current disparate data protection requirements across the member states of the European Union. In addition, Acquia sees the GDPR as an opportunity to strengthen and deepen its commitment to data protection and to demonstrate how our offerings can help our customers on their own GDPR journey.

Learn how Acquia is prepared for GDPR.

What is GDPR?

The General Data Protection Regulation ("GDPR") is a data protection regulation that the European Union issued in order to replace the European Data Protection Directive of 1995. The GDPR will directly apply to all member states of the European Union from 25 May 2018 forward. The GDPR applies to organizations both inside and outside the European Union that are processing the personal data of data subjects who are in the European Union.

Questions?

If you have any questions relating to Acquia's GDPR Readiness process, approach or commitment, please contact your sales representative or Acquia's GDPR team at gdpr@acquia.com.

Additional Information and Resources

You can find more information about this reform of EU data protection rules on the website of the European Commission at the end of this guide or by visiting www.acquia.com/gdpr.

How GDPR impacts organizations and their marketers

While we cannot provide legal advice on the topic of GDPR, we can share guidance and best practices that we see in the market as it pertains to data collection and marketing personalization. In this guide, you'll also learn how our own personalization products provide tools and controls to help our customers configure their data collection responsibly.

How GDPR affects data collection

GDPR is focused on the protection of the personal data of individuals in the European Union. Under the GDPR, Personal Data is defined broadly in Article 4 (1) as follows:

"[A]ny information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The definition of personal data in the GDPR has been expanded to include any single identifying point for a natural person to the already general use of personally identifiable information (PII) and personal data found in regulations and laws such as HIPAA, PCI, etc. Examples would be: name, personalized email address, mail address, phone number, dynamic and static IP addresses. The effect on data collection is that the collection must be purposeful, with clear intent of use, transparent, as well as secure and legitimate, including receipt of an opt-in.

Six principles as it pertains to personal data

Protecting PII is important, and there are severe penalties for not doing so. Organizations can be fined up to the higher of 4% of annual global turnover (revenue) for breaching GDPR or €20 Million. This is the maximum fine that can be imposed for the most serious infringements. It is important to note that these rules apply to both data controllers and processors.

There are six principles mentioned to keep in mind with regards to personal data:

1. Should be processed lawfully, fairly and in a transparent way.
2. Should be collected for specified, explicit and legitimate purpose
3. Should be kept up to date.
4. Should be limited to what is necessary.
5. Should not allow identification of people for longer than necessary.
6. Should be processed in a way that ensures appropriate security.

The GDPR strengthens the rights of individuals under the currently existing data protection regulations, as well as giving new rights.

What users need to opt-in to

Any and all forms of data collection methods and purposes should be transparent and subjected to an explicit consent unless a contractual relationship justifies the collection of personal data in order

to fulfill the contract. The business purpose and intent of use must be clear and concise to the visitor. The visitor must have the ability to opt-out of one, some, and/or all forms of data collection and methods of use once their data was collected by an explicit consent documented by an opt-in - typically a check-box that is not pre-activated. At any time, the visitor has the ability to choose to opt-out (even if previously decided to opt-in) and has the right to request that one, some, and/or all types of personal data, methods of collection, or intention of use be deleted.

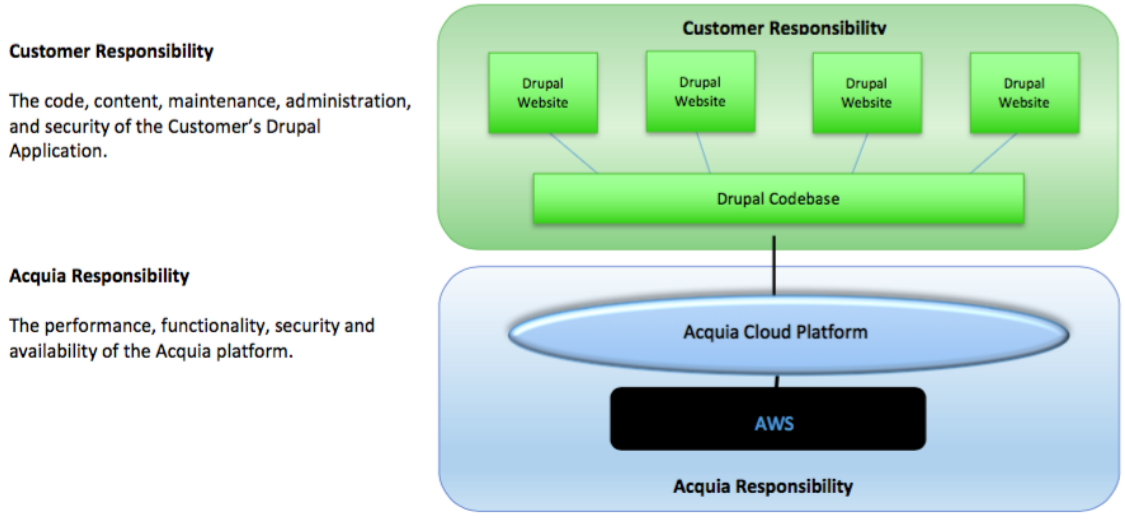
How GDPR applies to Acquia's products and services

The GDPR has different requirements depending upon whether an organization is a "controller" or a "processor" of the applicable personal data. As a global company, Acquia processes the personal data of persons in the European Union, so will be subject to the GDPR. Acquia will be a controller for the personal data which it collects in its own marketing, CRM, HR, finance and other internal systems. For its product and service offerings, however, Acquia will be a processor for personal data for which our customers are the controller. Customers will collect personal information of individuals, their clients, through their Drupal or other applications, which Acquia will then process through its digital experience products and services.

Data controller (Our Customer) vs data processor (Acquia) responsibility

For Acquia's products and service offerings, GDPR is a shared responsibility with our customers. The controller (i.e. Our Customer) is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor (Acquia) is an entity which processes personal data on behalf of the controller and subject to the controller's instructions. We also call this the Shared Responsibility Model.

Shared Responsibility Model



We are a processor for Customer-collected data in Product Offerings. This is separate from Customer who is Controller for data collected on the front end of its digital experience. We process such data on behalf of our Customers as their technical vendor supporting their businesses using the

data - always subject to their guidelines and instructions. In that context, the Customer will always be in control of what happens with such data. Because of the open source nature of Drupal, our Customers own their Drupal applications on our Acquia Cloud and Acquia Cloud Site Factory offerings, as well as any data collected and stored through Acquia Lift and Acquia Journey. Therefore, each Customer must determine from its own technical point of view what personal data are collected, stored and processed by our underlying platform offering to ensure GDPR compliance of the Drupal application.

Using Acquia Lift and Journey for personalization

To be clear, GDPR doesn't prevent personalization, it simply provides controls and regulations around the way marketers collect and use personal data.

Marketers who are informed about GDPR will understand that as long as the marketer has received the appropriate opt-in from a user and any gathering and use of personal data is justified for legitimate business purposes and secured (via least privileged access, access control management, encrypted, pseudonymized, etc.), they may continue to gather data from users for marketing efforts.

The biggest key here is that users must be aware that their data is being gathered, and know exactly what it's being used for and why, and they must have the option to opt-out of one, some, or all forms of data collection (e.g. you can collect my name and email but not my IP address). So long as this is made clear to users, and the users have accepted the terms of use, companies may continue to collect data as needed for use in marketing.

GDPR allows for personalization based on cookies. Our products provide tools for our customers to configure data collection (such as the ability to: set cookie duration; set visitor to do not track; anonymize profile; hash any identifier). As a reminder, the customer is responsible for compliance of its Acquia Lift or Journey implementation and configuration using the tools provided by our product offering. For instance, the customer will need to comply with applicable requirements such as transparency of cookies, user consent etc. We define "visitors" as the people our customers are using our products to collect data about and build personalized experiences towards. While Acquia Lift captures basic page level data, PII like an email address is up to the customer. Lift collects IP addresses for geo location, but this information isn't stored on a unified customer profile, meaning that it cannot be associated with a person.

Visitor data rights

There are eight visitor data rights for which marketers will be responsible: the right to be informed; right to restrict processing; right to access; right to rectification; right to erasure, right to data portability; right to object; rights in relation to automated decision making and profiling. Below you'll find a description of these rights, along with what is the customer responsibility as the data controller, versus Acquia's responsibility as the data processor.

Visitor Data Rights	Description	Customer Responsibility	Acquia Responsibility
Right to be informed	The right to be told what data will be collected, why, by whom, for what	Customer should inform visitors of what and how data is collected using Acquia Lift and Journey through website notification.	Acquia provides documentation on what data can be collected and gives Customer full control of what data they are pushing

	purpose and where data will go		into Profile Manager and how it is stored.
Right to restrict processing	The right to pause the processing of the data if there are grounds to do so	Customer can and should implement a button or some other type of option on the website to allow visitors to opt in or out of tracking.	Acquia provides a do not track method by which Customer can implement do not track into their applications by individual visitor profiles.
Right to access	The right to see the personal data that are being held about the data subject	Customer can implement a form using the visitor query API functionality where visitors can look-up data being collected on them. Alternatively, Customer could require visitors to request their data and Customer can then manually retrieve it via the API.	Acquia Lift provides the visitor query endpoint via the Decision API or Profiles API, which allows Customer to retrieve any desired information about an individual visitor. This API can return any combination of a visitor's identifiers, person, touch, or event data.
Right to rectification	The right to correct data if they are wrong or inaccurate	Customer can build a form which pulls data from the profile using Visitor Query, then allow the visitor to update it, after which it can be pushed back into the visitor profile via the Capture API.	Acquia provides the Capture API method which enables Customer to modify any data stored in visitor profiles.
Right to erasure	The right to have personal data removed when they are no longer necessary	Customer can and should implement a button or option to allow visitors to purge the identifying information.	Acquia provides a purge person function which enables Customer to completely remove any identifiers from a given visitor profile.
Right to data portability	The right to allow individuals to obtain and reuse their personal data for their own purposes	Customer can use the Visitor Query function within the Decision API or Profile API to get a formatted copy of all available profile data to provide to an individual.	Acquia Lift provides the visitor query endpoint via the Decision API or Profiles API, which allows Customer to retrieve any desired information about a visitor. This API can return any combination of a visitor's identifiers, person, touch, or event data.
Right to object	The right to object to processing personal data including profiling	Customer can and should implement a button or some other type of option to allow visitors to opt in or out of tracking. If a visitor opts out of tracking, they also won't be presented personalized content.	Acquia provides a do not track method by which Customer can implement into their applications to set individual visitor profiles to not track information.
Rights in relation to automated decision making and profiling	The right to reject being subject to decisions made based upon automated processing, without explicit consent	Customer can and should implement a button or some other type of option to allow visitors to opt in or out of tracking. If a visitor opts out of tracking, they also won't be presented personalized content.	Acquia provides a do not track method by which Customer can implement into their applications to set individual visitor profiles to not track information.

Additional information and useful resources

You can find more information about this reform of EU data protection rules on the website of the European Commission (see links below). If you have any questions relating to Acquia's GDPR Readiness process, approach or commitment, please visit www.acquia.com/gdpr or contact your sales representative or Acquia's GDPR team at gdpr@acquia.com.

Acquia's Privacy Policy:
https://www.acquia.com/about-us/legal/privacy-policy

Acquia's GDPR resources:
www.acquia.com/gdpr

Acquia's certification for the EU-U.S. Privacy Shield:
https://www.privacyshield.gov/participant?id=a2zt00000004FE2AAM&status=Active

European Commission – data transfers outside the EU:
http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm

European Commission – reform of EU data protection rules:
http://ec.europa.eu/justice/data-protection/reform/

Contact us today

To learn more about how Acquia is preparing for GDPR, please visit Acquia's Privacy Policy https://www.acquia.com/about-us/legal/privacy-policy or contact us at gdpr@acquia.com.