THE GDPR AND THE MARKETER

Marketo®

THE GDPR AND THE MARKETER

INTRODUCTION

There are key themes within the General Data Protection Regulation (GDPR) which will apply from May 25, 2018, however its purpose can be summarized very simply:

Its aim is to strengthen the rights of European Union (EU) citizens with regard to how their personal data is used and how it's protected. ('Personal data' means any information that relates to an identified or identifiable natural person).

To that end, the GDPR is structured around six key principles (detailed in Article 5 of the legislation):

1. Transparency on how data will be used and what it will be used for.
2. Ensuring that the data collected is used only for the purposes explicitly specified at the time of collection.
3. Limiting the data collection to what is necessary to serve the purpose for which it is collected.
4. Ensuring the data is accurate.
5. Storing the data for only as long as necessary within its intended purpose.
6. Prevention against unauthorized use or accidental loss of the data through the deployment of appropriate security measures.

In addition, there is a new accountability requirement to be able to demonstrate how compliance with the principles is being managed and tracked. This will mean maintaining records of how and why personal data was collected as well as the documentation of the processes put in place to protect it.

To whom does it apply?

The GDPR applies to any organization inside or outside the EU who is marketing goods or services to, and/or tracking the behaviors of, EU citizens. If you do business with Europeans that involves the processing of their personal data, this legislation applies to you.

Penalties for non-compliance are significant, with large fines for those in breach of the regulation: the maximum fine for a single breach is €20 million or 4% of annual worldwide turnover, whichever is greater.

IMPLICATIONS FOR MARKETING

As Marketers, if we create customer experiences that feel personal and human, that are founded on trust and delivered with care, we will win their hearts and minds.

Though the GDPR doesn't use these terms our goals are the same, namely to respect the rights of our customers and go on to earn their trust.

To build and maintain that trust we, as marketers, need to be attuned to the how, when, and why our customers want to be engaged and respect their preferences.

How we address these higher expectations around the collection, use, and security of the personal data that we routinely use in the course of our work is key and Marketo can help you meet those expectations.

There are two key aspects of the GDPR where Marketing needs to review past, current, and future practices. The first is consent by the individual to process their personal data and the second is accountability, namely being able to demonstrate how they comply with the principles of the GDPR.

"At Marketo we believe there is a real opportunity for Marketing to 'raise the bar' on customer engagement and respecting the privacy of customers is a foundation of that".

Sarah Kennedy, Chief Marketing Officer

CONSENT

The definition of consent under the GDPR is: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

This dual need for an 'affirmative action' that captures consent which also must be 'specific' in how the personal data will be used before any processing of the data represents a significant change for most marketers in how they record and respect customer preferences.

Of course, customer preferences change over time and rarely exist in perpetuity and GDPR has something to say about this too—namely that organizations, specifically marketing, must make it easy for data subjects to make any changes in preference or withdraw consent altogether.

All marketers need to audit, identify, and review the current points at which they are collecting personal data for processing.

"Affirmative consent puts individuals in control, builds customer trust and engagement, and upholds the principles of GDPR".

Matthew Fischer, Associate General Counsel, Chief Privacy Officer

As a rule, you should ensure the following necessary elements for consent compliance from Article 13 of the GDPR:

- Link to online Privacy Policy/Notice/Statement on every form. If personal data is obtained from sources other than the data subject, such as third party data providers, you must provide some additional information about the data and source. Refer to Article 14 of the GDPR if applicable.
- Consent field added to every form

- Lead fields for documenting consent:
  - Consent to processing
  - Consent last updated
  - Consent notes (purpose of processing and history of consent provided should be documented here)
- GDPR consent operational program
- Correspondence opt-out (subscription center)
- Link that enables web tracking / cookie opt-out

ACCOUNTABILITY

The most significant addition to current legislation under the GDPR is the accountability principle.

The GDPR requires you to show how you comply with the principles—for example, by documenting the decisions you make about a processing activity.

You need to make sure you can take a measured approach to who has access to personal data and resources, as well as a clear audit trail of changes and who made those changes. This ability to set fine grained access forms an important part of demonstrating compliance with the data protection principles.

Below is a summary of the key features available within Marketo that will assist with meeting the accountability principle requirements as part of your GDPR compliance plan.

User Roles and Permissions

Marketo provides several built-in roles, each with different permissions. Beyond these standard roles, it is possible to create custom roles to reflect your own policies and role types. In general, administrative access should be limited and there should be a clear policy and defined process around the granting of roles and permissions. Regular review of who has which access rights within Marketo for consistency with policy is an important piece of a well-functioning role-based access control.

Audit Trail

The audit trail gives you the ability to obtain a complete history (six months' worth) of changes made within your Marketo instance by your users. If your business requires the retention of a longer history of activity, then the audit trail can be exported for archival.

Data Encryption

By default, Marketo implements suitable measures to prevent personal data from being read, copied, altered or deleted by unauthorized parties during transmission, applying high grade TLS encryption to all data-in-transit through the use of HTTPS connections to all Marketo instances. In addition, customers have the option to add encryption to data at-rest by storing their data on AES-256 encrypted hardware. Encryption at-rest provides a further safeguard in the case of a data breach, as any data stolen would be illegible and unusable.

SUMMARY

As an enthusiastic advocate of the power and customer-centricity of the engagement economy, Marketo understands the importance of putting privacy and data protection in the hands of the data subject. As with other data protection laws, GDPR compliance requires commitment from both Marketo and our customers. This document is intended to help you make best use of Marketo's services to attain your own GDPR compliance.

We will continue to closely track applicable GDPR guidance issued by regulatory authorities and related legislation, updates will be posted to our Trust Centre on Marketo.com