ACTIVETRAIL
marketing automation

ActiveTrail:

The General Data Protection Regulation (GDPR)

Laws around security and privacy are continually changing to try and keep up with the fluid progress of the technology landscape, but it is rare that we see updates as sweeping as those regarding personal data protection and compliance embodied in the European Union's (EU) General Data Protection Regulation, or GDPR, which is scheduled to come into force on May 25, 2018.

As digital marketers, there is a good chance that the GDPR will impact your marketing efforts, in particular, and your business, in general, especially if you are located in the EU or do business with EU companies or citizens, just as it has bearings on ActiveTrail. In this guide, we have compiled our knowledge and insights regarding the GDPR and it's repercussions, and offer it to you to help you prepare for and manage the imminent changes the implementation of the GDPR will bring with it.

NOTE: The purpose of this guide is informational only, and it is not intended, in any way, to be relied upon or to replace legal advice or opinion. To understand how the GDPR might impact your business or organization, we urge you to consult with the appropriate legal, business or other types of professionals.

The GDPR – Introduction

Ever since 1995, data protection in Europe has been regulated by Directive 95/46/EC (the "Directive"), and, as you can imagine, has been due for a major overhaul for quite some time. Consequently, in 2016, the European Commission (EC - the EU's governing body), passed the General Data Protection Regulation, a comprehensive privacy law to be fully enforced throughout the European Union.

The GDPR is officially set to come into effect on May 25, 2018.

Owing to the extended time between enactment and execution, organizations will not be afforded a "grace period," and will need to be in compliance with the GDPR at the outset on May 25th.

Purpose of the GDPR

Over the years, the EC and the EU constituent nations enacted amendments to the '95 directive and local data protection legislation to keep up with times, causing privacy laws to be out of sync across the continent. In the words of the European Commission itself, the GDPR "…was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy…" (The GDPR portal, https://www.eugdpr.org/).

The GDPR reinforces the European view of the right to privacy as being on par with other basic rights, and controls how individuals and organizations may collect, use, store, and dispose of personal data. With such a broad scope and the GDPR's EU-wide enforceability, it has substantial consequences for businesses, governments and organizations across the globe.\

Who is Impacted

More precisely, the GDPR affects two central types of entities:

1. EU Organizations - All organizations formed or incorporated in the EU.
2. "Extraterritorial" Organizations - All organizations involved in processing personal data of EU citizens, i.e. the GDPR applies to any organization around the world that processes EU citizens' personal data, wherever such processing may take place.

The implication of #2 is that the GDPR has the potential to impact the vast majority of organizations on the planet. Therefore, all organizations across all industries and sectors, should, at the least, perform a thorough examination to see if they process EU citizen personal data.

Compliance and Penalization

Amongst the more far-reaching aspects of the GDPR are the sanctions and exceedingly heavy fines imposed on non-compliance. Companies or organizations found to be in violation of the GDPR could be fined as much as €20 Million or 4% of global annual turnover, the greater of the two.

We have already mentioned that if you are an EU company or organization, or one that processes EU citizen personal data (be it as "trivial" an item as holding EU citizen email addresses) then you are required to comply with the GDPR if you wish to continue pursuing activities related to such data. As the scope of this inclusion is so wide, most organizations are encouraged to seek legal and other professional advice regarding their need to comply with the GDPR, and if so, what they should do to ensure compliance after May 25, 2018.

It should also be noted that EU privacy legislation is often adopted, in some form or another, in other regions and countries around the world, such that it may be to your advantage to prepare your organization to comply with the GDPR, even if you believe the GDPR has no current bearing on your business.

Major Components of the GDPR

Terminology

To set the stage for understanding the important articles of the GDPR, here are few key terms defined in the regulation:

- **Personal Data:** The GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject')", i.e. information that by itself, or together with other information, could serve, to identify a specific person. This very broad definition brings data such as geographical data, financial information and IP addresses into the fold, along with "traditionally" personal data such as passport and social security numbers, names, biometric data, and email addresses.

Most of the subscriber information you collect and store in ActiveTrail could potentially fit this definition, even pseudonyms and aliases that can be linked to specific individuals. Moreover, the GDPR requires stronger protection for sensitive personal information such as health or racial data, and you should not keep such data in your ActiveTrail account.

- **Processing Data:** For purposes of the GDPR, you are processing EU citizen personal data if you, in any way, collect, manage, make use of or store EU citizen personal data. Quoting from the GDPR, processing is "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

In terms of using the ActiveTrail system, if one or more of your mailing lists includes an EU person's personal data, such as their name or email address. then you are considered to be processing EU personal data under the GDPR.

- **Data Controller:** A data controller is an organization that makes use of EU citizen personal data for its own purposes. Controllers determine which personal data to collect, for which purpose and how the data will be processed and used. The vast majority of ActiveTrail customers are considered data controllers in their interaction with the ActiveTrail system, i.e. ActiveTrail customers decide which personal data items they wish to collect and insert into ActiveTrail's system, which data to transfer to their own systems and how to make use of this data.
- **Processor:** A processor is an organization that processes the data on behalf of a controller. In the capacity of the services we provide to our clients, ActiveTrail serves as a processor.

Key GDPR concepts

Although the 1995 directive provides a starting point for the GDPR, many of the GDPR's central principles are aggressive, considerably altering those put forth in the 1995 directive. Of particular interest, in our opinion, are:

a. Wider definition of personal data, as described above.

b. Covers a much larger group of organizations, including not only EU organizations, but also organizations outside of the EU, or "extraterritorial" organizations that process EU citizen data.

c. Extended data privacy rights for EU citizens that organizations who process EU citizen data must protect, including:

- **Right to be forgotten:** An individual may request that their personal data stored by an organization, be promptly deleted.

- **Right to object:** An individual may declare that certain pieces of their personal data cannot be used.
- **Right of access**: Individuals may request of any organization to know what personal data about them the organization processes and how they go about it.
- **Right to rectification:** Individuals may request that an organization fill in incomplete data or correct erroneous data.
- **Right of portability:** Individuals may request that personal data held by one organization be transferred to a different organization, for instance, if they change service providers.

d. Harsher requirements regarding obtaining consent, most important of which is that organizations will need to obtain an individual's consent every time they make use of their personal data, save under certain conditions as described in below. As an ActiveTrail user, you will need to obtain such consent from your subscribers and members of your mailing lists, and the simplest way to do so will usually be directly. A few pointers regarding consent worth knowing are:

- Consent must be given in the context of a specific usage.
- Consent must be proactive, i.e. subjects must explicitly authorize, or opt-in to provide consent to store or use their personal data, thereby possibly disqualifying pre-marked checkboxes or similar as means of obtaining consent.
- Consent must be given separately for different types of processing, such that you must ensure that you explain how personal data will be used when requesting user consent.

e. Stricter processing requirements according to which subjects have the right to receive a "fair and transparent" description regarding how their personal data is being processed, including:

- **The purpose for which the data is being collected**: The purpose should be specific and the data should be used for the stated purpose only ("purpose limitation"). Also, you should, to the extent possible, collect and use only the data needed for the stated purpose and no more ("data minimization"). Organizations need to be very conscious of and be able to justify (to the authorities) which data they are collecting and why.
- **Retention period:** Organization should retain personal data for the shortest possible period of time ("storage limitation").
- **Contact details for the data controller** (further discussed herein),
- **Legal foundations:** Organizations must have a justifiable legal basis for processing personal data (they can't do so simply out of a desire to do so), such as needing such data to meet contractual obligations or consent has been given to use personal data for a specific reason.

The GDPR and transferring data across borders

We have mentioned a number of times that the GDPR has global implications, and much of this has to do with the way the GDPR treats cross-border transfers of EU citizen personal data from EU countries to countries outside the EU. However, in this regard, the GDPR does not stray far from the 1995 directive, as it deals with

conditions that must be met in order to transfer personal data outside the EU, implicitly suggesting that it is allowed to perform such a transfer. Essentially, these conditions form provisions under which organizations can legally transfer EU citizen personal data outside of the EU.

One such provision states that the European Commission can make explicit "adequacy" decisions, by which the European Commission "may decide **with effect for the entire Union** that a third country, a territory or specified sector within a third country, or an international organization, **offers an adequate level of data protection… In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorization**", i.e. the European Commission can, for instance, make a sweeping decision that a given country has sufficient personal data protection measures in place, such that organizations who transfer personal data to that country do not need to rely on any other authority to transfer the data.

Controllers and Processors

Organizations that interact with EU citizen personal data are either controllers or processors, per the definitions described earlier in this document. These definitions are nearly unchanged from the 1995 directive, however, the GDPR imposes greater (and different) responsibilities on each category of organizations. Naturally, controllers have primary responsibility for protecting personal data. Data processors, while not primarily in charge, do have direct responsibilities as well. It is therefore imperative that you are aware of your status as a controller or processor in the eyes of the GDPR, and, accordingly, to know your obligations.

Most ActiveTrail users belong to the controller category as they decide which information flows through and/is stored in ActiveTrail and ask ActiveTrail to process this personal data on their behalf (i.e. serving as a data processor), for instance by configuring ActiveTrail to send personalized emails to their subscribers.

Of course, these are only a few of the concepts and principles provided in the GDPR and it is recommended to review the GDPR in its entirety (and seek counsel, if necessary) before making decisions on how to properly prepare for the GDPR.

The GDPR, ActiveTrail and You

Privacy at ActiveTrail

At ActiveTrail we've been taking privacy seriously, well, always, and, in this sense, the GDPR provides us with further justification for what we've been doing all these years. On the other hand, on a macro level, we see the GDPR as setting a new baseline, ingraining protection of personal data into the fibers of business practices around the world.

In regard to the May 25th 2018 GDPR enactment date, from ActiveTrail's internal system's perspective, we have reviewed and documented processes and procedures, updated documentation,reviewed and tightened some of our security provisions,

added some specific positions and auditing committees etc. to be extra sure that everything is in order when 25.5 rolls around, and to make sure we can respond to requests from our customers arising from their rights as described by the GDPR, e.g. your “right to be forgotten”.

How ActiveTrail helps you comply with the GDPR

Perhaps most interesting to you as an ActiveTrail customer are the features of our system that make it easier for you to ensure your compliance with the GDPR, as follows:

Individual Rights:

While there is a good chance that you already have processes in place, perhaps even in ActiveTrail, our system can help you make sure that you can respond to subscriber requests stemming from the GDPR expanded individual rights.

- **Knowing what data you collect about your subscribers (right of access)**
- **End-user data correction (right to rectification)** – According to the GDPR’s right to rectification, subscribers may request that you correct their data at any time. You can do this at anytime through your ActiveTrail account and your subscribers may request this to be done directly from ActiveTrail at no cost to you or them.
- **Deletion requests (right to be forgotten)** - Per the GDPR’s right to be forgotten, your subscribers can request to be completely removed from your systems at any time. ActiveTrail will respond promptly if needed and will completely delete your user’s information from it’s systems. If this need arises, please contact our customer service and they will perform this procedure.
- **Objecting to use of data (right to object)**
- **Moving your data to another system (right of portability)** – ActiveTrail gives you tools to export any of your data from ActiveTrail to other systems, at any time you may choose. If you need help in doing so, we will gladly help you through the process. If you want your data completely deleted after exporting it, please contact our customer service and we will perform this procedure for you.

Consent and Processing

The GDPR lays out what you must do to lawfully collect and process personal data and email addresses from your subscribers and clients. Collecting subscriber data and requesting consent upon collection are one of the primary ways in which you can use the ActiveTrail system, and we provide you with the means to help you comply with the GDPR in this context:

- ActiveTrail offers you an easy to use landing page builder and signup forms which you can place on your landing pages, which help you collect information on leads and subscribers.
- When you design your landing pages and forms, make sure that, in a footer / disclaimer or in the body itself, you clearly indicate which information you

would like the user to provide and describe your intended use of this information.

- Get your subscribers' explicit consent that their data can be transferred to and processed by you.
- Always provide your subscribers with a simple way to "unsubscribe" and "change preferences, so that they can withdraw consent or change their data usage preferences. ActiveTrail makes your job easy here by automatically adding an unsubscribe footer to all emails.
- Make "double" sure your subscribers wish to opt-in to receive emails using the ActiveTrail double opt-in option, by which you place opt-in checkboxes on your sign-up forms and also send registrants emails asking them to confirm their opt-ins.
- Immediately update any information stored in ActiveTrail upon request from a subscriber.
- When a subscriber fills out and submits one of your ActiveTrail signup forms, ActiveTrail saves the email address, IP address, and timestamp associated with the submission, providing you readily available proof of consent. This helps you keep tabs on the consent given to you by your subscribers to send them marketing emails, store and use their personal data, or other types of processing for which you received their consent.

IMPORTANT: The GDPR doesn't differentiate between consent given prior to enactment or post-enactment, i.e. any subscriber consent must comply with the GDPR. Consequently, you should obtain legal counsel regarding compliance of any pre-May 25th 2018 consent with the GDPR, to check whether you may need to request additional / different consent.

Consent and 3rd Parties

ActiveTrail offers various types of integrations with 3rd party apps, greatly increasing the sphere of things you can do with and through ActiveTrail. Many of these integrations involve transfer of data to and / or from the 3rd party systems, and processing of such data in these systems. If you make use of any such integrations, you need to be careful that any consent that you obtain from your subscribers also permits transfer to and processing of information by the 3rd party systems.

Your Privacy Statement

Implicit from all of the above, is that you should make sure your own privacy statement reflects that certain parts of your subscribers' personal data will be transferred to and processed by ActiveTrail. For example, you may want to consider updating your privacy statement to specifically identify ActiveTrail as a personal data processor on your behalf, and mention how you use ActiveTrail to collect and process this data.

You can find the full language of the GDPR at the following link:

All languages: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1465452422595&uri=CELEX:32016R0679

English: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN