

General Data Protection Regulation (GDPR) Guidelines for Client Campaigns

As of May 25, 2018, an important change in privacy legislation in the European market took place. This legislation affects communications which may be intended or not, (e.g., accidentally emailing sole traders, handling EU web visitors) and therefore Direct Marketing Partners (DMP) must take steps to ensure the compliance of all the data we handle. This notice presents general information and best practices, rather than legal advice.

The new General Data Protection Regulation (GDPR) regulates the “processing,” which includes the collection, storage, transfer or use, of personal data about (European Union (EU) and Swiss individuals. Any organization that processes personal data of EU individuals, including tracking their online activities, is within the scope of the law, *regardless of whether the organization has a physical presence in the EU or not*. Importantly, under the GDPR, the concept of “personal data” is very broad and covers any information relating to an identified or identifiable individual (also called a “data subject”).

The GDPR provides more privacy rights to EU individuals and places significant obligations on organizations regarding data collection and storage. Some of the key principles are:

1. Transparency on how data will be used and for what it will be used.
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 deployment of appropriate security measures.
7. Clear and non-ambiguous language providing access to the communications preferences and “forget-me” options.

Because DMP uses “legitimate interest” as the basis for communication within the European Union, we must be sure the campaigns we undertaken on behalf of others are in compliance. For campaigns targeting Europe, we will want to know that a Legitimate Interest Assessment

(LIA) has been undertaken and filed with the appropriate authority and that lists have been audited for GDPR compliance (e.g., no sole traders or partnerships, no “forget-me” contacts and no private mobile phone numbers or emails unless they have specific consent and have recently been bumped up against a recent forget me (DNC) list). As another best practice, it is highly recommended our customers publish their privacy practice and allow prospects to view their policies, select the kind of correspondence they wish to receive and opt-out, if desired.

Since Direct Marketing Partners is holding and processing your data in order to provide you with our services, going forward we must request that our customers guarantee that their data that pertains to EU contacts sent to us for dissemination is GDPR compliant. We will be asking for assurance for each campaign. In the event that the customer is unable or unwilling to make such a certification, DMP must take the necessary steps to check the data. In certain cases, this may entail several additional steps vetting lists, further research and filing of relevant paperwork. DMP will charge for these services, with prior approval from client.

Please review DMP’s “Controller to Processor,” document, also attached, outlining the Processor’s (DMP’s) data security/privacy measures/tools and policy framework by which we will safeguard data provided by the Controller (Customer) going forward. This document describes each party’s obligations regarding compliance.

For further information on GDPR and access to forms, please check out ICO:<https://ico.org.uk/for-organisations/> or feel free to contact Tom Judge at 510.368.7527.