



Discover Media Groups LLC
Tonsley Pl, HighPoint NC 27265,USA
Phone: +307-414-9898
info@discovermediagroups.com

GDPR Commitment

Our commitment to your data privacy

We are wholly invested in our customers' success and the protection of customer data. One way that we deliver on this promise is by helping DMG customers and users understand, and where applicable, comply with the General Data Protection Regulation (GDPR) The GDPR is the most significant change to European data privacy legislation in the last 20 years and went into effect on May 25, 2018.

It is designed to give EU citizens more control over their data and seeks to unify a number of existing privacy and security laws under one comprehensive law. The GDPR not only applies to organizations located within the EU, but it also applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

GDPR Compliance

We appreciate that our customers have requirements under the GDPR that are directly impacted by their use of DMG products and services, which is why we have devoted significant resources toward helping our customers fulfill their requirements under the GDPR and local law.

At a glance

- o Understanding whether you are processing personal data is critical to understanding whether the GDPR applies to your activities.
- o Personal data is information that relates to an identified or identifiable individual.
- o What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.
- o If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.
- o If you cannot directly identify an individual from that information, then you need to

consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.

o Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.

o When considering whether information 'relates to' an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual.

o It is possible that the same information is personal data for one controller's purposes but is not personal data for the purposes of another controller.

o Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR.

o Information which is truly anonymous is not covered by the GDPR.

o If information that seems to relate to a particular individual is inaccurate (ie it is factually incorrect or is about a different individual), the information is still personal data, as it relates to that individual.

Checklists

The following checklists set out indicators that DMG Business Intelligence Group (DMG) are the controller or a joint controller. The below given boxes shows the decision that are made under the GDPR compliance -

- We decided to collect or process the personal data.
- We decided what the purpose or outcome of the processing was to be.
- We decided what personal data should be collected.
- We decided which individuals to collect personal data about.
- We obtain a commercial gain or other benefit from the processing, except for any payment for services from another controller.
- We are processing the personal data as a result of a contract between us and the data subject.
- The data subjects are our employees / Data Partners / Data Vendors / Data Networks / Business executives who have opted in or provided consent to communicate with third parties based on their interests and others consented contacts.
- We make decisions about the individuals concerned as part of or as a result of

the processing.

- We exercise professional judgment in the processing of the personal data.
- We have a direct relationship with the data subjects.
- We have complete autonomy as to how the personal data is processed.
- We have appointed the processors to process the personal data on our behalf.

Are a joint controller too..

- We have a common objective with others regarding the processing.
- We are processing the personal data for the same purpose as another controller.
- We are using the same set of personal data (eg one database) for this processing as another controller.
- We have designed this process with another controller.
- We have common information management rules with another controller

Lawful basis for processing

We have a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual / business executive. Most lawful bases require that processing is 'necessary' for a specific purpose. We determine the lawful basis before you begin processing, and we document it.

Our privacy notice includes lawful basis for processing as well as the purposes of the processing.

Checklist

- We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity.
- We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.
- We have documented our decision on which lawful basis applies to help us demonstrate compliance.
- We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.

Where we process special category data, we have also identified a condition for processing special category data, and have documented this.

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. We follow at least one of these whenever we process personal data:

- a. Consent: the individual has given clear consent for us to process their personal data for a specific purpose.
- b. Contract: the processing is necessary for a contract you have with the individual, or because they have asked us to take specific steps before entering into a contract.
- c. Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).
- d. Vital interests: the processing is necessary to protect someone's life.
- e. Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- f. Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if we are a public authority processing data to perform the official

Individual rights

Under the GDPR we provide the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.
- This part of the guide explains these rights.



Discover Media Groups LLC
Tonsley Pl, HighPoint NC 27265, USA
Phone: +307-414-9898
info@discovermediagroups.com

What DMG provides / Offers

With the heavy investment made towards having our data under the compliance of GDPR, We have shrunk our millions of records prior to May 2018 to few hundred thousand within the given EU scope. DMG confirms that each of recipients or individuals provided or transferred are under the consent of the recipient.

Along with individual information, we tailored firmographic data, chosen from seven detailed segments – covering corporate, financial, and digital information of global as well as local brand/entities. Authenticated from certified record agencies over the world, our 360-degree profiling services vie for accuracy and relevance.

Get your existing Database (European Prospect lists) to the new Standards by driving targeted Campaigns to gain Opt-in (double or single). We can assist with this process to initiate and start a new opt-in / consent campaign for companies

Get targeted Lists of all 28 countries to drive new Opt-in marketing campaigns following GDPR compliant by the consent sign up-process

We provide individuals with all the following privacy information:

- The name and contact details of our organization.
- The name and contact details of our representative (if applicable).
- The contact details of our data protection officer (if applicable).
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organizations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual

obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).

The details of the existence of automated decision-making, including profiling (if applicable).

When to provide it

We provide individuals with privacy information at the time we collect their personal data from them.

If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

within a reasonable of period of obtaining the personal data and no later than one month;

if we plan to communicate with the individual, at the latest, when the first communication takes place; or

if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it

We provide the information in a way that is:

concise;

transparent;

intelligible;

easily accessible; and

uses clear and plain language.

Changes to the information

We regularly review and, where necessary, update our privacy information.

If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

- We undertake an information audit to find out what personal data we hold and what we do with it.
- We carry out user testing to evaluate how effective our privacy information is

Best practice – delivering the information

- When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:
 - a layered approach;
 - dashboards;
 - just-in-time notices;
 - icons; and
 - mobile and smart device functionalities.

Accountability and governance

We take responsibility for complying with the GDPR, at the highest management level and throughout our organization. We keep evidence of the steps we take to comply with the GDPR. We put in place appropriate technical and organizational measures, such as:

- adopting and implementing data protection policies (where proportionate);
- taking a ‘data protection by design and default’ approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
- putting written contracts in place with organizations that process personal data on our behalf;
- maintaining documentation of our processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals’ interests;
- appointing a data protection officer (where necessary); and
- adhering to relevant codes of conduct and signing up to certification schemes



Discover Media Groups LLC
Tonsley Pl, HighPoint NC 27265, USA
Phone: +307-414-9898
info@discovermediagroups.com

(where possible).

- We review and update our accountability measures at appropriate intervals.

Security

We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place. When deciding what measures to implement, we take account of the state of the art and costs of implementation. We have an information security policy (or equivalent) and take steps to make sure the policy is implemented. Where necessary, we have additional policies and ensure that controls are in place to enforce them. We make sure that we regularly review our information security policies and measures and, where necessary, improve them. We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.

We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process. We use encryption and/or pseudonymisation where it is appropriate to do so. We understand the requirements of confidentiality, integrity and availability for the personal data we process. We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism. We ensure that any data processor we use also implements appropriate technical and organizational measures.

International Data Transfers

For many businesses, the international transfer of data is a critical part of day-to-day operations. The General Data Protection Regulation (GDPR) protects individuals' personal data in this regard, meaning organizations cannot transfer personal data outside the European Economic Area (EEA) unless certain safeguards are in place. We explain below the permitted transfer mechanisms that are followed by DMG in compliance with GDPR:



Discover Media Groups LLC
Tonsley Pl, HighPoint NC 27265,USA
Phone: +307-414-9898
info@discovermediagroups.com

SHARING AND DISCLOSURE OF INFORMATION TO THIRD PARTIES

We rent or sell personal information as data controllers. We share and disclose information that we collect with the third parties under the GDPR compliance: Is it an international data transfer?

First, we identify whether we are transferring personal data out of the European Economic Area (EEA). A “transfer” takes place where personal data is processed during or after the transfer to a third country.

The European Commission (EC) considers certain countries to provide an adequate level of data protection to EU data subjects. If we are transferring personal data to an “adequate” country then we can do this without putting further safeguards in place. The list currently includes Canada, Israel, New Zealand and Switzerland.

At present, personal data transfers are permitted to the USA under the EU-US Privacy Shield framework, which replaced the Safe Harbor transfer mechanism. It allows companies to self-certify their compliance with data protection standards that have been found to provide an equivalent level of protection to the EU. DMG examines the companies that the data is sold / transferred / shared too. Only on proper paper work the data will be licensed to third parties ensuring the legal aspects of a company that we are dealing with.

We do not transfer data to “non-adequate” countries under the EU privacy shield framework. The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America as providing adequate protection.

DMG Business Intelligence Group sees GDPR as an opportunity to excel. We fully comply with the GDPR terms and conditions. While the entire world is tripping over losing out the EU data-market in wake of its new legislative data protection reform, GDPR is not really the demon it was perceived to be. The General Data Protection Regulation (GDPR) is simply replacing an old directive that was in place from another millennium, to handle a datadriven ecosphere that has evolved from its times. The game has changed and so have the rules. It's not as if, nobody saw it coming.



Discover Media Groups LLC
Tonsley PI, HighPoint NC 27265, USA
Phone: +307-414-9898
info@discovermediagroups.com

New data technologies are being adopted by businesses every day. And data security and decay (inherent to any new technology installation) are two pressing concerns that GDPR addresses. Surely, adjusting to new regulations is a cumbersome process, but it's the necessary shuffle needed from time to time to open deadlocks and create fresh opportunities. GDPR is no different.

If you have questions or concerns regarding this Policy, you should first contact the Head Office at the contact address listed below or via email at info@discovermediagroups.com

Head Office
Tonsley PI, HighPoint NC 27265, USA
info@discovermediagroups.com

DMG