GDPR Compliance for B2B Marketers

A Quick Guide E-book

MEDIA DEV®

Table of Contents

Introduction

This paper was written as an informative guide to help raise awareness amongst businesses to the implications of the General Data Protection Regulation (GDPR) enacted into law by the European Commission on April 14, 2016 (for which compliance will be mandatory by May 25, 2018). The research presented here only covers the implications for companies conducting B2B marketing outreach to prospects or clients located in Europe. For the purpose of this paper, discussion of the processing of sensitive data or data pertaining to minors is not included. The management of (internal) employee data (which may include internal IT network security monitoring, human resources, payroll or other finance-related data) will also not be addressed.

Most B2B marketers have data usages that range from low to medium risk. High-risk data including large-scale processing of sensitive personal data, implications of CCTV video-surveillance monitoring or image capturing and automated profiling activities are subject to a greater level of scrutiny when it comes to ensuring compliance with GDPR. Such high-risk activities and data collection methods will also not be addressed in the scope of this paper.

Disclaimer: MediaDev's advice should not be taken as legal instruction. We suggest that your GDPR compliance process be verified by legal representation as depending on the nature of your business, you may need to implement additional steps.

Overview of GDPR

What is GDPR?

GDPR stands for the General Data Protection Regulation. This piece of legislation was designed to provide individuals with greater visibility, traceability and control over who collects and processes their personal data, and for what purpose. It aims to protect individual's fundamental rights and freedom in particular when it comes to the storage and protection of personal data in an effort to eliminate hacks or other security breaches that have affected large organizations in the past. It was developed to enable individuals to stop unwanted solicitation from businesses by mandating that explicit consent be provided to companies, authorizing their use of such personal data. Personal data is defined as any information relating to an identified or identifiable natural person. This includes: first name, last name, the name of the company you work for, your email and phone number, or an IP address.

The spirit of the law is a good one. There are currently 28 different sets of data protection laws across the European Union, and GDPR sets out to replace that with one, overarching pan-European regulatory framework. It was designed to give individuals more control over who can access their personal data and why, and it is in large part meant to curb unwanted solicitation. Of course, many marketers are worried about the implications that GDPR will have on their current outreach initiatives (since it requires explicit consent by the part of the data subject) and are rethinking what tactics they are going to be allowed to use moving forward.

Who is affected?

The EU GDPR applies to any business (regardless of location) that processes personal data related to a resident of the European Union; so, if you are doing business in Europe, or with European-based companies, this means you. It applies in all contexts and across all activity sectors. Much of the confusion around GDPR comes from the fact that this is a fundamental change to the law, which up until now did not require businesses located outside of the European Union to comply. Because of the nature of global business, requiring non-EU based companies to respect EU standards when it comes to handling, processing and storing data is a big win. This means that the offshore BPO outsourcer working with European companies, prospects or user-groups is also going to have to strictly abide by new processes and procedures. It also requires that both processors and handlers share in the responsibility; a company cannot use an outsourcer as a "cover" for poor data processing since they have a legal requirement to ensure that where processing is carried out on their behalf that the processer provides sufficient guarantees that they meet GDPR requirements to ensure the protection and rights of the data subject.

Why is it important?

GDPR is important for a number of reasons, one of which being that non-compliance comes with a high price-tag: Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). For some, that means running the risk of going out of business entirely if they do not comply. One of the fundamental rights of all EU-residents under GDPR is that any person who has suffered material or non-material damage as a result of an infringement of this regulation has the right to receive compensation from the data processor or handler. No-one yet knows how GDPR will be enforced, but in our opinion, enforcement will come from individual or group complaints lodged against companies that are non-compliant.

One can imagine that highly-visible lawsuits will result out of non-compliance in extreme cases; massive data hacks (like the Sony PlayStation data breach in 2011 where 77 million users had their data stolen, or the Ashley Madison scandal in 2015 that leaked more than 25 gigabytes of company-held data on its' users, including personally identifying information and user details) will not go unpunished. Since GDPR requires businesses to report data breaches within 72 hours of detection, many organizations will need radical changes to internal reporting structures in order to prove compliance.

When is compliance compulsory?

Compliance is technically mandatory now, since the law was already enacted in 2016. However, since enforcement will not take place until May 25, 2018, most businesses are working to prove compliance by that specific date. After May 25, 2018 all organizations must be compliant or they run the risk of hefty fines.

What do organizations need to do to prepare?

A necessary first step is to review all data processing activities. What personal data do you have, and what do you use it for? How is it manipulated? What permissions have been obtained for that data? What tools do you currently possess for data storage? How is your data backed-up and at what frequency? How vulnerable is your organization to outside attack? Do your employees have "rogue" processes (like using Skype to transfer data files, or storing data on free solutions like Dropbox?).

Doing a complete audit and mapping out processes in a workflow will enable organizations to work out how the GDPR affects their business operations, and identify the issues that need to be addressed. Again, if the activity involves the processing, handling or storage of personal data (that of individuals residing within EU member states), then GDPR applies. It is highly advised that legal counsel be sought; a designated Data Protection Officer may need to be appointed as part of the requirement (for any business or organization with more than 250 employees), and this person must be aware of all of the legal implications GDPR has on daily operations.

How will GDPR Affect Business-to-Business Marketing?

GDPR provides 6 lawful bases for processing data. No one way is better than another, but the one to select depends on your business purpose, and the relationship you have with the individual data subject.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data, but the method used may change depending on the type of data you have. In other words, you may treat employee data differently from the data that you have on prospects or current clients.

Here are the 6 legal ways in which to base data processing:

1. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

2. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

3. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

4. **Vital interests:** the processing is necessary to protect someone's life.

5. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

6. **Legitimate interests:** the processing is necessary for your 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 you are a public authority processing data to perform your official tasks.)

Many marketers are trying to use "legitimate interests" as a way of continuing to do what they've always done in the marketing space when it comes to outreach campaigns for prospects. The hope is that in doing so, it will enable them to get around having to obtain explicit consent. However, our professional recommendation is that obtaining consent is a more secure route to take because the legal implications of "legitimate interests" are not yet known. For the purpose of this paper, we will continue to develop data processing with "consent" as part of the process.

Thus, the first impact that GDPR will have on B2B marketing is that opt-in policies will have to be revised.

Due to the fact that all data subjects should provide explicit consent to allowing a company to access their personal data, outreach must be conducted in order to obtain that consent. The need for consent is the foundation that underlies GDPR. Individuals must opt-in whenever data is collected; privacy policies must be clear, concise and transparent. Consent must be able to be withdrawn at any time and a data processor has an obligation to delete data of a data subject upon request.

For all extensive purposes, companies are not going to delete all of the data that they already have and start over from scratch. That means they will need to work to get the consent from each individual data subject, and that consent needs to be explicit and voluntary. Blanket consent, consent by default and consent as a condition of sale, service, or general terms and conditions is no longer allowed. Data subjects must be provided with a clear explanation of the processing to which they are consenting (what are you using my data for?) and the consent mechanism must be a voluntary (active) opt-in. This means that pre-ticked boxes, silence or inactivity cannot be used as methods to collect consent.

Since consent needs to be freely given and explicit, companies will not be allowed to obtain opt-ins in exchange for gated content or other assets online if their intention is then to use their data for another purpose. Opt-in policies are going to have to be very clear—no more opting in to receive information from a company and its "partners." (Which up until this point was a nice way of saying, "We're going to give your data to a third-party to use as they please.") A user needs to know who has access to their personal data and providing a non-specific statement about partners without describing exactly who they are and what they are going to use your data for is a breach of GDPR.

Consent is linked to a specific purpose; therefore opt-in policies need to be carefully designed to clarify any and all uses of personal data. Because individuals must be allowed to withdraw consent at any time, subjects also need to be provided with an easy way to contact you (by phone or email) should they change their mind and request that you modify or delete their personal data. Internal processes need to ensure that personal data is then deleted from all platforms and is not used against the data subject's request.

Some leeway exists when using personal data to carry out marketing initiatives, but it's best to be as transparent as possible with opt-in policies. GDPR states that, "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." In other words, if it's for the good of your data subject that you are informing him or her about an offer or service, you may still be able to carry-out that marketing outreach. But can the marketing industry rely on "legitimate interest" or is it strictly required to obtain consent? The implications of GDPR are still unknown, but our standpoint on the subject is that it's better to be safe than sorry; consent should be given outright, and respected when it is taken away.

Online Data Collection

The profiling of data subjects is a controversial topic, and not just one that has inspired science-fiction films and best-selling novels. GDPR clearly states that data controllers must inform data subjects of the existence and consequences of any profiling activities that they carry out (including online tracking and behavioral advertising). Organizations that collect and use personal data will need to put in place robust privacy notices, providing more information in a more prescribed manner. This will involve a large-scale review of all privacy notices across online channels.

Marketers must also be very aware not to use profiling methodology to discriminate against certain user groups; preferential pricing based on age, sex or race for example will not be tolerated. While this usually is not an issue in the B2B space, it is important to recognize that GDPR is meant to protect data subjects against this type of discriminatory methodology and encourages the fair and equal treatment of individuals.

Gathering publicly available information online (such as a company phone number or address) is allowed under GDPR because it is not considered personal data. As soon as data is collected on individuals, however, this drastically changes the situation. The law now places the burden on data processors to keep their own records of data processing activities and make these available to supervisory authorities on request. Records need to contain information so that the who, what, where, when, why and how of data processing is clear. Small businesses (those employing fewer than 250 employees world-wide) are exempt from these record-keeping requirements unless their processing activities involve a "risk to the rights and freedoms of data subjects, are not occasional, or include special categories of personal data or data relating to criminal convictions or offences." Again, this is not likely to be the case for B2B marketers.

For all practical purposes, companies that outsource or conduct their own data mining activities are going to need to demonstrate how it is done, what information is obtained and what it is used for. Gathering data from social media or other publicly available online sources may be tolerated; however, using that data for a specific purpose will require the explicit consent of the data subject.

The End of Data Purchase through Brokers

Purchasing data on individuals from a third-party data broker without the explicit consent of each and every data subject will be strictly prohibited. Data brokers are trying to find creative ways to comply, but many will have a great deal of difficulty doing so unless they change their business models in the process. GDPR clearly indicates that, "when (data) processing has multiple purposes, consent should be given for all of them," and, "where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation." In other words, it is a requirement to obtain explicit permission from a contact in order to use their data The data subject must know who you are and what you plan on doing with their data, and you need to prove that the contact gave you permission to use their data for that specific purpose (or purposes).

Data brokers may claim that they have obtained opt-ins from their lists of contacts, but the fact of the matter is that they didn't get them specifically for you to purchase. Opting-in to receive information from one company and then being contacted by another (even if they are a "partner" as discussed earlier) is not allowed; so unless you reach out to a prospect and explicitly obtain consent for you to send them an email, you are not in compliance with GDPR.

Data brokers are considered data "processors" because they obtain, hold and process data. Thus, they are subject to following GDPR and they could also be accused of security breaches by transferring data to you since it is highly unlikely a data subject would give them explicit permission to sell their data to someone else. By purchasing personal data from a third-party data broker, you are exposing yourself to unnecessary risk. Our standpoint on the topic of purchasing data from a broker is clear: We do NOT advise the purchase of data from a third-party supplier that contains personal data on individuals residing in Europe.

The Resurgence of Telemarketing Tactics

Many questions have been raised about what techniques can be used in order to obtain consent for the hundreds (if not thousands) of existing data subjects a company may already have in its database of contacts, and how marketers can access net new contacts if they cannot purchase them from third-party suppliers. The law allows for telemarketing in the B2B space, so it is possible to call a company and navigate by phone to find the right decision-makers to target. Emailing subjects prior to calling is not allowed, but using outbound phoning to set the stage for obtaining consent is.

Oral consent is allowed by the law, and CRM time stamps or call logs can help serve as proof of contact. As mentioned previously, GDPR introduces new obligations on data processors even when these service providers may process personal data on behalf of organizations but do not themselves determine the purpose of the processing (such as call centers). Where a controller contracts a processor to process personal data, that processor must be able to provide "sufficient guarantees to implement appropriate technical and organizational measures" to ensure that processing will comply with the GDPR and that data subjects' rights are protected. This requirement flows down the supply chain, so a processor cannot subcontract work to a second processor without the controller's explicit authorization. Contractual arrangements will need to be updated, and stipulating responsibilities and liabilities between the controller and processor will be imperative in future agreements. Parties will need to document their data responsibilities even more clearly and the increased risk levels may impact service costs.

Using external agencies for telemarketing will still be allowed, but callers must clearly identify who they are and that they are calling on your behalf; the reason for their call should be clear and the call-to-action (sending an email and/or receiving a call-back from one of your specialists) explicitly agreed to. Some people find this part of the law contradictory (GDPR is likely to curb email spam but not cold callers who at times can be just as annoying to the end-customer), but it makes sense if you again take the spirit of the law into account. GDPR is about protecting personal data and giving more control back to the individual; a business calling another business is perfectly acceptable because it goes outside of the realm of personal data. And good thing! Otherwise you'd never be able to call a business with a general inquiry ever again. Along these same lines, soliciting businesses using generic email addresses such as contact@, sales@ or info@ is also fine since those types of email accounts are not considered personal (a professional, individual email address is considered personal data, however).

Necessary Steps to Achieve Compliance

It is highly likely that if you are reading this eBook, you have already taken some steps in order to get your organization GDPR compliant. The following list is by no means exhaustive, and should be followed with proper legal guidance as the exact requirements for each company may vary from one to the next.

Know the Fundamental Principals behind GDPR

Before doing anything, it is important to understand the guiding principles behind GDPR. These should serve as one's guiding force when working towards compliance:

1. Lawfulness, fairness and transparency – all actions revolving data must be legal and fair; inform data subjects clearly about what you plan on using their personal data for, and be utterly transparent about collection methods.

2. Purpose limitation – data should only be used for the purpose you set out to use it for and nothing else.

3. Data minimization – only collect the data that is needed and nothing more.

4. Accuracy – keep all data as up to date as possible, and deal with inaccuracies as soon as possible.

5. Storage limitation – data should only be stored for the period of time it is needed to be kept in order to achieve its purpose.

6. Integrity and confidentiality – data must be stored if a safe, secure location so that no unauthorized access can occur.

7. Accountability – organizations have an obligation to show that they respect and comply with all of the principals above.

Nominate a Data Protection Officer

It is highly important to establish who is going to do what, both within your initial project to comply with the GDPR, and for the long-term protection of the personal data that you hold. Since all marketers are accessing, processing and manipulating data just by the nature of their job functions, it is a wise idea to designate a Data Protection Officer to oversee (data) operations (even if your organization may not be legally required to do so). Organizations that fit into any of the following categories are required by law to designate a Data Protection Officer:

- Public bodies or authorities
- Those that monitor data subjects on a large scale
- Those that handle large volumes of special category data
- Organizations with more than 250 employees

Data protection officers may be part-time, shared resources across organizations or external resources/paid service providers. DPO contact details must be provided to the regulatory authority and published to the public. While they do not need to be a new hire, (an existing employee can take on the role), it is important that they know a reasonable amount about data protection law.

Update your Privacy Policy, Terms & Conditions, and Opt-in Consent Form

It is advisable that internal or external legal counsel review all privacy policies to make sure that the language is clear, easy to understand, and in plain language. The days of tiny font size are over—the text should be accessible, transparent and delivered in a friendly format (keep in mind that many people use mobile devises for accessing information they should not have to scroll for ages in order to read your conditions). Organizations will also need to make sure that privacy notices are given at the time that data is obtained from a contact and that it contains all the required information including: what you are going to use their data for, who is going to access it, how you will ensure the protection of any data that is transferred, how long will you store their data for, and how they can contact you should they wish to rectify or delete any data you have.

Create New Policies and Procedures

In order to ensure that GDPR is properly implemented across an organization, it is necessary to create new policies and procedures. These include:

• General Data Protection Policy – this should overview for all internal resources the why behind all changes, who will be impacted, what is expected, what obligations are required and who is the overarching authority internally to oversee such procedures.

• Data Subject Access Rights Procedure – this must outline with total transparency how data is processed and stored; it must provide a specific flow-chart for how a data subject can contact you and the necessary steps that will be taken to ensure personal data will be modified or deleted (and in what timeframe).

• Data Retention Policy – this will determine how long you will store data after the purpose it was collected for has passed. GDPR stipulates that data will only be retained for a reasonable period, but it's up to each organization to determine what that means. It should be noted that organizations do not have the right to keep data for an undefined period of time (i.e. forever), or use personal data for any other purpose other than what a data subject has given you permission for.

• Data Breach Escalation and Checklist – this outlines the exact procedure that must be followed in order to report any breach in data security up the chain of command and to the appropriate authorities within a 72-hour timeframe.

• Processing Customer Data Policy – your customers must also be informed about how you will handle and store their personal data. This can be something that is inserted into a contract, or may be subject to a separate privacy agreement should you conduct direct marketing activities to your current customer base. Policies and procedures will need to be implemented company-wide, and it may also be necessary to create specific policies that pertain to various data-sets within the marketing department (depending on the exact type of personal data you collect and store).

Provide Employee Training

Employees who manipulate data must receive training in order to ensure that they handle it in accordance with GDPR. The company should keep a record of training and provide updates and refresher trainings as needed. It's very important that resources understand the changes that are to occur, and that they implement them effectively.

Clean the Data you have to Obtain Explicit Opt-ins

Existing prospect data you have now will need to be called in order to be compliant because you are not allowed to email the contacts you have in order to be sure they agree to opt-in to receive any new information you want to send them. To be on the safe side, it's good to obtain double opt-ins (by phone and then again by email) prompting contacts to click on a link to access your updated Terms & Conditions and actively check a box to indicate their (active) consent.

Ensure Data Security

The days of sharing spreadsheets containing personal data on Skype or Dropbox are over. Even emailing data from one person to another opens the door to potential security breaches (because it could accidentally be emailed to the wrong person), so it is essential that all personal data be stored in one secure location and that it has limited and protected access. Security has to cover the risks to individuals

if data were lost, stolen or disclosed to unauthorized people. Security involves both people/processes and technical measures. The following factors should be considered:

- User log-ins
- Encryption
- Ensuring ongoing integrity, confidentiality, availability and resiliency
- The ability to restore in a timely manner
- Processes for testing security

User Bill of Rights

GDPR establishes a set of rights that the data subject can exercise and which the controller holding their personal data must react and respond to. These rights aim to ensure that personal data is processed fairly and transparently and that the data subject can take action if this is not the case.

1. The right to be informed: the right of the individual to be told what data will be collected, why, by whom, for what purpose, where the data will be stored and for how long.

2. The right of access: the enabling of a user to see the personal data that is being held about him or her. In this case, the Data Controller has to provide, upon request, an overview of the categories of data that are being processed about a data subject. Furthermore the Data Controller has to inform the data subject on details of the processing including: what the purposes are of the processing (Article 15(1)(a)), with whom the data is shared (Article 15(1)(c)) and how it acquired the data (Article 15(1)(g)).

3. The right to rectification: the allowing of a user to modify or correct any personal data held on the data subject should it be outdated, wrong or inaccurate.

4. The right to erasure/the right to be forgotten: whereas personal data is no longer necessary for the purposes for which it was collected because that purpose has been served, data subjects have the right to have all personal data deleted and entirely removed from all storage.

5. The right to restrict processing: pausing the processing of data if there are grounds to do so.

6. The right to data portability: obtaining the data in a transportable form and moving it to an alternative processor; Individuals will have the right to transfer personal data from one data controller to another where processing is based on consent or necessity for the performance of a contract, or where processing is carried out by automated means.

7. The right to object: stopping the data from being processed altogether, and the right to complain to the DPA.

8. The right to understand automated profiling: where the data was not collected directly from the data subject, the right to know the source of the data and an explanation of the logic involved in any automated processing that has a significant effect on data subjects.

Conclusion

Being GDPR-compliant will take time and thoughtful planning, but that doesn't mean you are going to have to completely halt all direct marketing initiatives. Working with the right people and using the right tactics will help ensure compliance. For more information on how to obtain consent for existing data sets, building net new contact lists, or designing new marketing outreach initiatives that are fully GDPR complaint, don't hesitate to contact MediaDev for a free consultation.

contact@mediadev.com

Glossary of Key Terms

Consent: "The consent of the data subject" means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

Data Subject: an identified or identifiable natural person.

Data Processor: one who conducts any operation or set of operations performed upon personal data or 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.

Data Controller: the natural or legal person, public authority, agency or any other body which alone or jointly determines the purposes and means of processing personal data.

Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal Data: Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Sources:

https://gdpr-info.eu/

https://www.eugdpr.org/

https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

https://appinstitute.com/gdpr-guide/

https://www.atg-it.co.uk/gdpr/dpa-vs-gdpr/

https://www.theatlantic.com/technology/archive/2017/06/online-data-brokers/529281/

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

24 Avenue Marceau, 75008 Paris, France
+33 170 76 2828 | contact@mediadev.com | mediadev.com