zoominfo

A Primer on GDPR and Marketing Data Protection Best Practices

May 25th, 2018, was the date on the minds of many sales and marketing professionals: the day the General Data Protection Regulation (GDPR) went into effect. The regulation outlines a specific set of rules and requirements an organization must abide by if processing personal information of EU-based individuals . With that in mind, many of our customers ask how they should prepare their data, and how ZoomInfo has prepared, as well. This brief primer provides practical tips to help sales and marketing teams navigate this regulation while leveraging a sales and marketing intelligence solution like ZoomInfo.

Does the GDPR Apply to Me?

1. **Scope**

The first question you need to ask is whether—and to what extent—the GDPR applies to you. The GDPR applies to your processing of personal data if (1) your company is "established" within the EU, (2) you are processing data on persons in the EU to whom you are offering goods or services, or (3) you are "monitoring" the behavior of individuals in the EU. (General Data Protection Regulation, Regulation (EU)2016/679, April 27, 2016 ("GDPR"), Article 3.)

"Established" means something like doing business in the EU through a branch or subsidiary, but the GDPR is clear that it is a substantive definition, not a formalistic one. (See Id. Recital (22).) If you have employees or contractors who work for you in the EU, you will want to analyze this more carefully.

If you are definitely not established in the EU, you need to figure out if you are offering goods or services to data subjects (people whose data you possess) in the EU. We think the GDPR, based on its plain language, does not apply to B2B marketing under this test because the offer is to the employer, not the employee. (See Id. Art.3(2)(a) ("The Regulation applies . . . where the processing activities are related to . . . the offering of goods or services . . . to such data subjects in the Union[.]") (emphasis added).) In layman's terms, B2B companies are offering goods and services to companies, not the data subjects AT those companies—their products and services are for the benefit of the company, not the consumer (data subject)—think of this is the difference between selling a vacation cruise to a person over the phone or email vs. selling a sophisticated firewall or backup solution to a company. But it is a gray area that wants additional guidance.

Lastly, the GDPR applies to you if you are "monitoring" persons in the EU, which the GDPR explains means tracking them on the internet to make decisions or predict preferences,

behaviors, and attitudes. (See Id. Recital (24).) So, if you are simply processing business contact data and using it to reach out to prospects, that would not appear to constitute monitoring. But doing something more sophisticated to predict what a particular person does based on their internet activity, then you will need to look at this more closely.

2. Okay, the GDPR applies, now what? (Lawfulness of Processing)

Assuming GDPR applies to you, you must first obtain a lawful basis to process personal data. (GDPR Art. 5(1)(a).) There are six different lawful ways to process personal data under the GDPR: (a) consent of the data subject; (b) performance of a contract to which the data subject is party; (c) compliance with a legal obligation of the controller; (d) protection of the vital interests of the data subject or of another person; (e) performance of a task carried out in the public interest or official authority; (f) for purposes of the "legitimate interests" pursued by the controller or by a third party, except where overridden by the interests of fundamental rights and freedoms of the data subject. (Id. Art. 6(1)(a)-(f).)

For the remainder of this document, we are going to focus on legitimate interests and consent as we believe our clients will most often fall into one of these lawful bases.

A. Direct Marketing as a Legitimate Interest

The biggest myth about the GDPR is that consent is the ONLY way to lawfully process personal information on EU data subjects. While consent is one lawful basis for processing, it is not the only one. (GDPR Art. 6(1)(b)-(f).) According to Elizabeth Denham, UK Information Commissioner, "Consent is one way to comply with the GDPR, but it's not the only way." Most of our customers will process under the "legitimate interest" basis, which includes direct marketing purposes. (See Id. Art. 6(1)(f), Recital (47).) In that case, you do not need to obtain consent, but you do still need to provide the person with a transparency notice explaining your processing activities. (See Id. Art. 14.) That notice needs to include all of the information from Article 14 of the GDPR, with an emphasis on (1) the fact that you are relying on direct marketing purposes as your legitimate interest, (2) the source of the data, and (3) the existence of the individuals privacy rights, including the right to object to your organization's processing of their data (opt-out)

The good thing is that you are allowed to provide the notice the first time you communicate with the person (but no later than one month from when you obtained the data). So, if you obtain a list for email marketing, you can include the notice with your first message - however most organizations will send a standalone notice prior to engaging in any commercial activity.

B. Consent

Consent requires you to get the data directly from the data subject. Perhaps prospects provided their information when visiting your website. In order to use that data, you need to make sure the consent is clear, freely given, and unambiguous. You also need to provide certain information at the time you obtain the consent, including (1) who you are, (2) the purposes for which you will use the data, (3) who you will be transferring it to (if anyone), (4) if you are in the EU and intend to transfer it out of the EU, the

countries where you intend to transfer it and the existence or absence of an adequacy decision by the European Commission with regard to the safeguards such countries have in place for the protection of personal data, (5) how long you intend to keep it, (6) the person's right to correct the data or have iterased and to withdraw their consent, (7) the right to lodge a complaint with the supervising authority, and (8) whether you are using any automated decision-making or profiling. (Id. Art. 13(1)-(2).)

3. Rights of the Data Subjects

Whenever you are processing someone's data, they have certain rights under GDPR. (See GDPR Arts. 15-21.) They always have the right to ask you what data you have on them, and for the other information that's required in the above-mentioned notices. They also have the right to make you correct the data if it is wrong, or delete it or object to processing. If you have transferred it to anyone else and the person requests deletion, you also need to tell whomever you transferred it to that the data subject requested deletion.

4. Compliance Protocols

You are also required to implement "appropriate technical and organizational measures" to ensure you are complying with GDPR, including appropriate compliance policies. (GDPR Art. 24(1); Art. 32(1).) These measures may take into account what is appropriate given the nature of the data and the purpose for which it is processed. (Id. ("Taking into account the state of the art, the costs of implementation and thenature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons . . . .").) The regulation as a whole seems clear that processing business contact information for B2B marketing does not require procedures that are as stringent as those that would need to be in place for processing, for example, sensitive health information.

You also need to maintain records of compliance, which include maintaining much of the information already discussed with respect to particular data. (Id. Art. 30.) However, you are not required to maintain these records if your organization has fewer than 250 employees. (Id. Art. 30(5).)

5. Breach Notifications

If there is a data breach, GDPR imposes notification requirements, both to the data subjects and to relevant supervisory authorities. (GDPR Arts. 33-34.) However, notification is not required if the breach is "unlikely to result in a risk to the rights and freedoms of natural persons." (Id.) If we are talking strictly about business contact information, we think a breach notification may not be required.

6. (Another) Disclaimer

The GDPR is very extensive and very complicated. We have tried to summarize a few key areas, but we cannot explain the entire 88-page regulation here. This guidance is intended to apply to your use of business contact information for your own B2B marketing purposes. Other uses and other kinds of data may impose significant additional obligations. As always, you should consult with an attorney for a full analysis of your rights and obligations under applicable law.

zoominfo

I'm in Sales and/or Marketing. What Should I Be Thinking About When Crafting My GDPR Approach?

Data is at the heart of prospecting. Although there are new regulations on the horizon, data management should already be a part of your sales and marketing operations. GDPR should be seen as an opportunity to implement better data management practices, which will also help establish and maintain trust with your customers.

If you are just getting started, here are some key best practices to consider.

1. **Establish a Data Management Team**

A data management team should consist of the core stakeholders who are impacted by your company's use of data. The team should be established to focus on maintaining the integrity and protection of your prospect database.

2. **Evaluate Your Current Data Practices**
    a. **The Data Management Team's First Task is to Evaluate:**
        - What data do we collect and store, and what is its nature (what data points do we have)?
        - How/when do we collect various types of data (i.e. through websites, trade shows, third-party data providers)? Where data is stored, and how does it move through our organization?
        - Who has access?
        - What security measures do we have in place with regard to the data?

3. **Understand the Data Protection Practices of Your Sales & Marketing Systems**

If you use a Marketing Automation or CRM tool, you should understand what your chosen vendor is doing to protect your prospect and customer data, including access controls, regulatory compliance, and information and application security processes and tools. In addition, explore existing functionality that may be helpful in preserving our data. This may include roles and permissions of users, history of user activity and/or data updates, and the ability to enable/ disable automatic data capture. Documenting the flow of data throughout your systems may be necessary to visualize what and who has access. If there is a data breach, GDPR imposes notification requirements, both to the data subjects and to the supervisory authorities. (GDPR Arts. 33-34.) However, notification is not required if the breach is "unlikely to result in a risk to the rights and freedoms of natural persons." As mentioned previously, if we are talking strictly about business contact information, we think a breach notification may not be required.

4. **Understand the Nature of the Data**

It is important to be aware of the type of data that is being collected and stored within your database. Processing sensitive information, versus simply business contact information, carries with it additional obligations. Sensitive information includes:

- Government ID and financial account numbers

- Health, genetic, and biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation or preferences

Generally speaking, B2B sales and marketing does not require processing of sensitive personal information; however, if you do possess any of the foregoing types of data on your prospects, keep in mind that your legal obligations to obtain consent and to protect the security of that data are much, much higher under the GDPR and other laws.

5. **Maintain Data on Your Data**

Part of complying with data protection obligations is showing that you understand where your data comes from, how it is maintained, and the legal justification for processing it (discussed below). This means you need to consider tracking additional data points on your prospecting records. For example, Lead Source may already be a value tracked within your database. Depending on the number of data sources feeding an individual contact record, you may need to expand this out to account for additional sources of data. In addition, it should be noted when and how data was obtained (i.e. via form fill, badge scans at an event, 3rd party data appending). Most MAT and CRM tools have the ability to timestamp the population or update of individual fields.

6. **Implement an Ongoing Database Health Program**

Once you understand the data you have, how you collect it, and are tracking the appropriate metadata, you should develop clear policies that outline your data practices and your plan for compliance. Your data protection plan should address issues around data gathering, notification requirements (if any) and practices, the purposes for which data will be used, practices for updating data and purging old data, and security practices and procedures.

What Is ZoomInfo Doing To Address Data Protection Regulations?

ZoomInfo is dedicated to GDPR compliance, and we employ several GDPR and privacy experts on our executive team who are working hard to ensure continued compliance with the regulation in our data practices. These include our Chief Compliance Officer, General Counsel, Privacy Counsel, Data Protection Officer, and Privacy & Compliance Manager, among many others

Many years prior to the introduction of the GDPR, ZoomInfo implemented a plan to provide notice to all EU-based contacts in our database. Over the years, we have expanded our notification program to encompass all contacts globally - not just those in the EU - creating an unparalleled approach to proactive privacy management. The notices state that we are processing their business contact information to provide to our customers and subscribers for their sales and marketing purposes. We give each person the right to opt-out of our database upon request and have been honoring such requests since we implemented this notice program.

Within our password-protected customer platform, we publish a list of contacts who have recently opted out of our database. Customers are asked to check this list regularly and independently honor those opt-outs, unless they have obtained an independent lawful basis to retain the individual's information. When we remove someone from our database for privacy reasons, we also flag these contacts as "opt-out" through our Enrich product and other select integrations.

ZoomInfo continues to process only business contact information for EU contacts: company, job title, work email address, work phone number, etc. We do not provide sensitive personal information of any kind, e.g. health information, political or religious ideology, or internet search history. We simply provide the type of information that is typically found on a business card, an email signature block, or a public professional profile.

Notice:
This is for discussion purposes only. ZoomInfo is not qualified to provide legal advice of any kind and is not an authority on the interpretation of the GDPR or any other rule or regulation. To understand how the GDPR or any other law impacts you or your business, you should seek independent advice from qualified legal counsel.