Preparing for GDPR:
What Channels Need to Know to Be Ready

Channeltivity®
CHANNEL MANAGEMENT MADE EASY.

Every channel organization is a dynamic and complex machine that is driven by interactions with their prospects, partners, their partner's contacts, as well as technology to enable these communications.

The regulations for these interactions have become more complex with the European Union General Protection Regulation (GDPR) that comes into effect on May 25, 2018.

This document is not intended to provide legal advice. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

What is GDPR and Who Does It Affect?

Any organization that processes data about individuals in the context of selling goods or services to 'Data Subjects'—this is what we refer to as a Contact—in European Union countries, regardless of the organization's location, will need to comply with the GDPR, a new data protection law that strengthens individual rights around consent and requires increased attention to cyber security and technological capacity.

It is paramount for channel organizations to be prepared, because the penalties for non-compliance are clearly outlined in the law and significant enough that they are not be worth the risk of breach.

Read the Full Regulation Here.

We will go through the main components of the law, review the risks to channel programs, and provide insight into how channel marketers can use these changes as an opportunity to review and reevaluate their current email marketing approach to build a plan that will not only survive, but thrive within the new regulations.

There are 3 main components to understand around GDPR, to be reviewed in the following pages:

- Opt-in Only
- All Consent Must Be Explicit
- Right to be Forgotten

Opt-in Only

Prior to GDPR taking effect, all company addresses were considered to be "opt-out". This means you can send an email to a company address without permission, provided you include an option to unsubscribe.

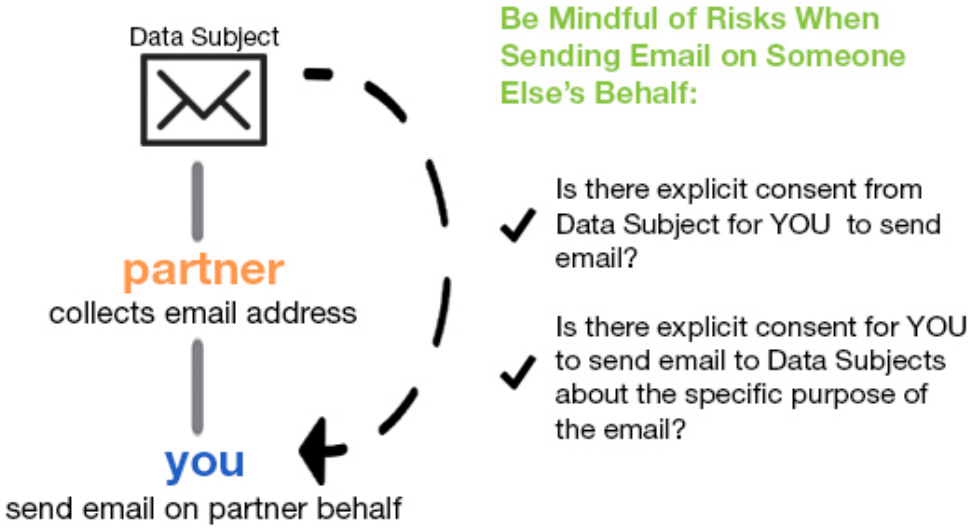
As of May 25, 2018, the new regulation fundamentally changes this. You will now need consent to send a marketing email. There is no distinction made between personal and business addresses. If the email address relates to an individual or identifies an individual, such as john@anyorganization.com then you will need consent to send the marketing email. A generic email address, such as info@anyorganization.com, will not require consent.

In addition, it will be up to the sender to prove that consent was given. Any data held must have an audit trail that is time stamped and reveals what the contact opted into, and how they opted in.

What This Means To The Channel

The further removed you are from the collection of data, the higher the risk of non-compliance becomes.

For example, running marketing campaigns on behalf of your partners has greater risks associated with it because you need to ensure your partner got permission specifically to have you contact them and for what purpose (and has a clear audit trail) for you to email that prospect, not just permission for the partner to send email to that prospect.



In addition, giving your partners marketing automation tools within your partner portal increases your risk because you are enabling the email marketing without holding the consent audit trail.

Because of the substantial risks, it is recommended that Channels focus on tried and true through-marketing strategies where each party is then responsible for their own consent documentation, lowering your risk of violating the GDPR:

1. Support your partner's campaigns with planning, content and funding (MDF), and enable easy deal registration through your partner portal. It is advised to inquire about a prospective partners marketing capabilities and strategies to understand their ability to successfully execute marketing campaigns. Those that can't may no longer be the right partner.
2. Create and manage your own marketing campaigns to generate opt-in leads and distribute these leads to your partners.

All Consent Must Be Explicit

Prior to GDPR, you could email market to an existing customer or partners if you gave them the opportunity to opt out at the time of purchase, or form completion. This is called implied consent or soft opt in.

Under the new GDPR law, all consent must now be explicit. You now must be able to prove that the customer agreed to receive the emails by a selection action, not just a disclaimer.

What This Means To The Channel

The main driver for the GDPR is protection of what they define as a **DATA SUBJECT**. In layman's terms, this is what we refer to as a Contact. The channel is a little more complicated as there are three types of Data Subjects:

- Potential customers
- Customers contacts/users of your portal
- Partner contacts/users of your portal

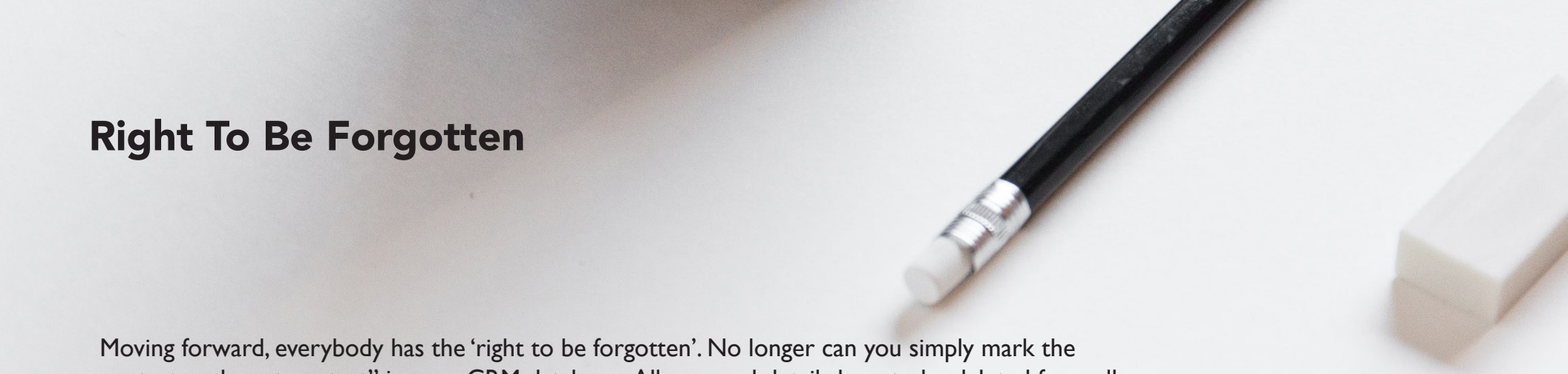
All of this information resides in your PRM and CRM.

In the case of potential customers and partners, it is important to establish consent directly if you intend to email market to these contacts. If the partner organization established the contact and the consent, it may be best to empower them to market to that list. Otherwise it is advisable to establish direct consent with the customer prior to any email marketing activities.

In the case of partner contacts/users as a Data Subject, it is critical to have ***clear acceptance of consent upon login to your partner portal***.

- Consent to receive emails should be a condition of using the partner portal.
- Your PRM must be able to store the timestamp of when your partner consented to receiving the emails, and in what way they specifically gave you that consent.
- In addition, make sure your partner terms and conditions have items specific to GDPR. Ensure any contracts within your portal also outline your GDPR guidelines. Talk with your legal counsel for more details and assistance.

Right To Be Forgotten



Moving forward, everybody has the 'right to be forgotten'. No longer can you simply mark the contact as do not contact" in your CRM database. All personal details have to be deleted from all databases that they reside.

What This Means To The Channel

The complexity around ensuring data being deleted across all platforms and databases where it might be stored cannot be minimized. It is critical that integrations across systems, such as between PRM and CRM systems, are in tight sync with rules defined in order to effectively comply with the law.

Critical path to GDPR compliance is to contact your PRM providers to understand what they are doing to comply as a data processor. See below for questions to ask your current or prospective solution provider.

According to a November 2017 survey of IT professionals by data modeling company Erwin, just 6% of IT professionals in North America are completely prepared.*

** Few Companies are Ready for the Upcoming GDPR, eMarketer, February 16, 2018 https://www.emarketer.com/content/few-companies-are-ready-for-the-upcoming-gdpr*

Questions to Ensure Your PRM Provider—and You—Are Compliant

Wrapping your arms around GDPR compliance is a big process, and knowing what to ask your solution providers is an important step in that process. Here are some of the questions to make sure you ask.

- How are they storing, or enabling you to store, time stamp and consent data?
- Do they have a GDPR addendum to their contracts? This addendum should protect you in the event the PRM provider (considered a Data Processor by the GDPR) violates the GDPR.
- Do they have GDPR Data Protection Agreements with their sub-processors? These could be any service they export data to for additional processing or storage. Examples include their hosting provider, address lookup service, marketing automation solutions, and any third party code required to make their system function. In essence any person or service who can touch the data.
- Is the PRM built on a fundamentally secure solution stack such as Oracle or Microsoft, or is it built on an open source platform such as WordPress? Open source platforms, by their nature, may be more vulnerable to data breaches.
- Is there custom work required to set up your portal? If so, who is performing any customizations? Are they on or offshore? What type of risk mitigation procedures do they have in place?
- Are they true single source multi-tenant in their delivery or does each client run on its own customized instance of code? This will make it difficult for them to manage security as each instance could be vulnerable for different reasons. A penetration test on your instance would be advisable.
- Do they use their own hosting facility or rent space where they bear the burden of ensuring security, or are they using a managed facility such as Microsoft Azure or AWS (Amazon Web Services)?
- What steps do you need to take to scrub data from all integrated systems to comply with 'Right to be Forgotten'? Is it automated? Are there steps you need to take in each system?

May 25, 2018 is coming quickly. Understanding your risk of system breach is critical to knowing what kind of trust you should place in your solution provider.

What Channeltivity is Doing

With over 20% of Channeltivity customers being in the EU and 100% of our customers doing business in the EU, Channeltivity has taken the steps needed to ensure we are GDPR compliant as a solutions provider, as well as providing the tools to channels to enable them to manage their go-to-market strategies in a compliant manner.

Contact us today if you have any questions about GDPR.

Channeltivity®
CHANNEL MANAGEMENT MADE EASY.

Growing your Channel Program?
Explore Channeltivity.

Channeltivity is a partner relationship management software platform that helps companies build strong relationships, optimize partner productivity and support new sales.

The Channeltivity platform is used and recommended by many channel programs to deliver effective and engaging partner training.

Channeltivity is easy to use, is fast to set up, and connects to Salesforce.com.

To find out why 20,000+ channel sales professionals around the globe depend on us, and to experience the solution through our hands-on demo, call 877-226-2564 or visit https://www.channeltivity.com