

Marketing Under the GDPR

Since its introduction, the General Data Protection Regulation (GDPR) has been poised to radically change the way that organisations handle their digital business operations. The GDPR expands the rights of individuals and their data, and places greater obligations on organisations that process personal data.

In order to comply, there are a number of revisions and adjustments that your organisation must make to your digital business practices, including your marketing and advertising efforts. If your organisation does not follow the revised regulations, you could receive significant fines and face prosecutions by the Information Commissioner's Office (ICO). One of the most effective methods to market under the GDPR is to highlight the content that your organisation can provide as a way to gain individuals' consent.

To ensure that your organisation effectively markets under the GDPR, it is essential that you understand consent along with how the new regulations impact your digital marketing and advertising efforts.

Overview of PECR, the GDPR's Marketing Guidelines

The GDPR's main focus is the protection of personal data and included under that umbrella is the Privacy and Electronic Communications Regulations (PECR), which specifically deals with electronic communications.

While PECR has existed since 2003, it is currently undergoing a major overhaul to adequately supplement the GDPR and update electronic marketing rules. [The proposed revisions to PECR](#) include simplifying cookies, banning unsolicited electronic

communications if users haven't given their consent and incorporating the GDPR's two-tiered fine structure.

PECR's biggest proposed change is making all forms of electronic marketing reliant on opt-in consent. Similar to the GDPR, this means that pre-ticked boxes will no longer be acceptable, even with business-to-business communications. [Under the GDPR, your organisation must identify and provide a lawful basis](#) to process personal data, which is any information that can be used to identify an individual. Put simply,

The GDPR impacts how your organisation is able to conduct its digital marketing and advertising practices. If you don't make the necessary adjustments, you could receive a €20 million fine.

joe.public@anybusiness.com would classify as personal data that requires Joe's consent before you can market to him through email, even though it's a business address.

However, even though EU lawmakers intend for these proposed changes to PECR to take effect on 25 May, the same day as the GDPR, there's significant doubt as to whether they will make that deadline. Regardless, as PECR sits alongside the GDPR, your organisation should follow the revised marketing guidelines to avoid potential fines.

Potential Consequences of Non-compliance

Under the GDPR, the ICO has the authority to mete out more substantial fines to organisations that don't

Provided by **Crendon Insurance Brokers Ltd**

The content of this Risk Insights is of general interest and is not intended to apply to specific circumstances. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly. © 2018 Zywave, Inc. All rights reserved.

Marketing Under the GDPR

comply with the new regulations. If you are found to be non-compliant, you could receive one of the GDPR's two-tiered fines:

- A fine of up to €10 million (roughly £8 million) or 2 per cent of your annual turnover—whichever is higher—can be given for the following causes:
 - Not properly filing and organising personal data records
 - Not notifying the supervising authority (such as the ICO) and affected individuals about a breach
 - Not conducting the necessary preliminary impact assessments
- A fine of up to €20 million (roughly £16 million) or 4 per cent of your annual turnover—whichever is higher—can be given for the following causes:
 - Violating the basic principles related to data security
 - Violating consumer consent

Even though your organisation could receive either fine, you would most likely receive the more substantial fine for any violations in your digital marketing and advertisement practices.

Real World Examples of Attempted GDPR Compliance

Even with the available guidance on GDPR compliance, some organisations may find implementing and following the necessary changes difficult. Despite their best intentions and efforts, organisations that strive to comply with the GDPR while disregarding other regulations, such as PECR, will be held liable by the ICO. The ICO has cautioned that, 'Businesses must understand they can't break one law to get ready for another'. To ensure that your organisation doesn't make the same mistakes, here are several examples of organisations that incorrectly followed the GDPR.

Flybe

Flybe, a British airline, was fined £70,000 after it sent more than 3.3 million marketing emails to individuals that had opted out of receiving them. The emails were

intended to amend out-of-date personal information as well as to update their marketing preferences in anticipation of the GDPR. To encourage individuals to provide the requested information, the airline offered them the chance to be entered into a prize drawing. However, since the airline deliberately sent emails to individuals who had specifically opted out of Flybe marketing emails, the ICO found the airline to be in violation of PECR.

Honda

Honda Motor Europe Ltd was fined £13,000 after it sent nearly 300,000 unsolicited emails to individuals. The emails were intended to clarify customers' choices for receiving marketing spam and help the company comply with the GDPR. However, as the company viewed the emails as a part of customer service rather than marketing, Honda did not attempt to obtain its customers' consent. During its investigation of the incident, the ICO determined that the emails were used as a marketing tool and, as such, violated PECR.

Morrisons

UK supermarket chain Morrisons was fined £10,500 after it sent out 230,000 emails to members from its database, asking them to update their account preferences. However, of those that received the email, 131,000 had previously opted out and unsubscribed. As Morrisons did not have the express consent of its customers, it was in violation of PECR.

Obtaining Consent is Key

One of the most significant changes introduced by the GDPR is strengthening the standards of obtaining consent to process personal data. Failure to obtain proper consent puts your organisation at risk for significant fines.

In order for your organisation to remain compliant with the GDPR in your electronic marketing and advertising efforts, your process for obtaining consent must meet the following standards:

- **Unbundled**—Consent requests must be separate from other terms and conditions, and should not be a precondition of signing up for a service.

Marketing Under the GDPR

- **Active opt-in**—Your organisation cannot use pre-ticked opt-in boxes.
- **Granular**—Provide options to individuals to consent to different types of processing.
- **Named**—Provide the name of your organisation and any third parties that will be relying on the individuals' consent.
- **Documented**—Keep records that demonstrate what the individuals have consented to, what they were told, and when and how they consented.
- **Easy to withdraw**—Inform the individuals that they have the right to withdraw their consent at any time and explain how they can do that.
- **No imbalance in the relationship**—Consent will not be considered freely given if there is an imbalance in the relationship between the individuals and your organisation.
- Ensure that your process for obtaining consent meets the necessary standards. In addition, you may want to implement a double opt-in practice, which asks individuals to take an additional step to confirm their email address and provide consent.
- Audit your mailing list to ensure that the collected customer data meets GDPR requirements. If you identify any individuals that don't have a record of their opt-in, you must delete them from your database.
- Educate your sales team about social media selling techniques, such as connecting with prospects on social media and sharing relevant content with them. The reason for this is that social media sites have privacy notices built into them.
- Create a content marketing strategy to provide individuals with relevant, useful content that incentivises them to give their consent. It could be a brief about important legislation, a hazard that impacts their sector, or health and safety guidance. Just remember not to make providing the content contingent on the individual giving their consent—this could mean consent was not freely given and thus make it invalid.

Advice for Marketing Under the GDPR

There are three main areas that your organisation may want to consider when marketing under the GDPR:

- **Data permission**—This refers to how your organisation manages your email opt-ins.
- **Data access**—This refers to the individual's right to access their personal data and remove consent for its use.
- **Data focus**—This refers to your organisation having to legally justify the lawful basis for the processing of all the personal data you collect.

Fortunately, marketing under the GDPR can be an easy endeavour by following these best practices:

- Review how your organisation collects, processes, stores and removes personal data.
- Identify which of the [six lawful bases](#) applies to your personal data processing, and document your rationale for collecting personal data.

Remember: Content Incentivises Consent

The GDPR has considerably adjusted the guidelines for how organisations can manage their digital marketing and advertising efforts. Obtaining consent is now central to establishing the necessary lines of communication with individuals, yet making that connection is not always easy. However, by highlighting the quality and benefits of the content your organisation can provide, individuals may be more likely to give consent.

For additional guidance on how your organisation can effectively operate under the GDPR, contact the professionals at Crendon Insurance Brokers Ltd today.