

# GDPR & B2B



## Alert BI is GDPR and PECR compliant

Alert BI provides company information. We do not provide personal data relating to individuals outside of an organisation. As per the guidelines of PECR (The Privacy and Electronic Communications Regulations related to direct marketing for businesses), any data we provide is at an organisational level and prior consent for contacting these organisations is not required – provided that the sender has given the recipient an opportunity to remove consent and withdraw from any future communications. We do not provide any personal email addresses or phone numbers, nor do we provide any contact data for sole traders who are deemed 'individuals' and not companies.

# Summary of GDPR and B2B guidelines

## Communicating with employees of corporates

When communicating with employees of limited companies, LLPs (limited liability partnerships), partnerships in Scotland and government departments (Health, Education, Councils, etc.) the GDPR rules for telephone, direct mail, email and texting are the same: they are required to OPT-OUT if they don't want to hear from you.

In other words, the default is 'they've opted in'. You do not need to seek prior permission and you are not obliged to reveal where you obtained their contact information.

However, when you make contact, you must provide the means for that individual to easily unsubscribe from future communications, and you must make it clear who you are, business-wise. You need to have a robust internal system in place to ensure ALL communications to OPT-OUTERS cease, unless the individual proactively contacts you later to change the opt-out position and/or to request service, support etc.

## Communicating with sole traders or partnerships

In contrast to the situation when dealing with corporates, when dealing with sole traders or partnerships, the general position for email and text is that you will need opt-in consent before you can communicate. That is, they must have agreed at some point beforehand to receive your communications – whether by ticking a consent form on your website or through a response card.

BUT, for telephone and direct mail, you don't need an opt-in first, though you do need to offer the ability to opt-out from future communications.

## For all B2B marketing communications, regardless of channel

To comply with the 'legitimate interest' requirement under GDPR, (see below) the content must be about products and/or services that are relevant to the recipient's job role; it must be easy for the recipient to unsubscribe; and, as stated above, you must identify yourself and your organisation.



## What is GDPR?

The GDPR (General Data Protection Regulation) is a legal framework introduced across EU member states on 25 May 2018, which brought significant changes to data protection in Europe. It came as a replacement for existing legislation surrounding data protection which was introduced in 1995. The purpose of the new legislation was to enhance protection of individuals' privacy and ensure they have full control over their personal data.

## How does GDPR affect organisations?

The introduction of this new legal framework means there is a significant increase in an organisation's responsibility and obligation to protect personal data, and ensure they are fully compliant with the GDPR guidelines on how they collect, process, and store this information. Companies must ensure that the information they hold on individuals is congruent to new legal standards. Under new legislation, companies are not permitted to contact individuals unless the companies can demonstrate lawful grounds upon which to do so.

## GDPR lawful basis for processing data

*"You must have a valid, lawful basis in order to process personal data" – The ICO.*

The GDPR is meticulous in its requirements for all data to be processed on a lawful basis. It allows six different options, encouraging companies to choose the basis that applies best to their needs in each business area.

The six different lawful bases of processing personal data are:

- 1. Consent** (where explicit consent is given by the data subject)
- 2. Contract** (where processing is necessary to fulfil a contractual obligation or as part of entering a contract)
- 3. Legal Obligation** (where processing is necessary for compliance with a common law or statutory obligation)
- 4. Vital interests** (where processing is necessary to protect someone's life)
- 5. Public interest** (where processing is necessary to perform a specific task in the public interest that is set out in law)
- 6. Legitimate interest** (where processing is necessary for the purpose of legitimate interest – which includes commercial interests)



These are aimed to be all-encapsulating, relating to every type of organisation as well as all departments within them. Some are not applicable to B2B marketing. The two main, lawful bases that apply to B2B marketing when processing personal data are 'Consent' and 'Legitimate interest'. Let's explore each of those further:

## Consent

Consent is currently the most commonly known and practiced lawful basis used by organisations when processing data, but the new GDPR has rigid rules surrounding consent. If it's your chosen path, then you will need to intricately check your ongoing systems for consent and refresh them accordingly.

The most notable change is to the definitive 'opt-in' process. This cannot be in any way ambiguous. For example, pre-ticked opt-in boxes are expressly unlawful under the new consent regulations. Opt-in must be a separate, individual and 'granular' process, singled out from any other terms and conditions. There must also be a clear right to withdraw.

Please see the ICO's page on Consent for further information.

## Legitimate interest

The ICO labels 'legitimate interest' as 'the most flexible' of all lawful bases of processing data, and it is likely that data processing for most B2B marketing departments will sit comfortably within this basis. In essence, it allows you to process personal data on the grounds that your organisation is working towards the legitimate interest of the individual; this can include commercial interests. As long as the data processing doesn't infringe on the rights and freedoms of an individual and you can prove the data subject (individual) in question is likely to have a legitimate interest in what you're marketing, you can collect and process their data.

For example, if you're an organisation offering recruitment services, and you collect and process data relating to HR Managers from a range of businesses, the individuals within those businesses are likely to have a legitimate interest in your services, based upon their job function and seniority. This is a good example of how legitimate interest would apply in a B2B marketing scenario. If, however, as an organisation you purchased a large list of Gmail, Yahoo! or Hotmail email addresses without consideration of who was being sent your email marketing communication, and without thought as to the relevance of your email message, then you would be in breach of those individuals' legitimate interest and therefore likely to be in breach of the GDPR regulation.



When leveraging legitimate interest as the lawful basis of processing personal data, you must also ensure that the rights and freedoms of the data subject are not compromised. Will your message put that person in danger? Will it land them in trouble? Are they likely to be personally negatively affected by your message? If so, then it is likely that your message will not be compliant with GDPR. Of course, for most B2B marketing it is highly unlikely that a data subject's rights or freedoms will be compromised. At most they won't be interested in your message, so it is essential to provide an 'unsubscribe' method, as the individual should always have the right to 'opt out'.

## Privacy and Electronic Communications Regulation

The Privacy and Electronic Communications Regulations (PECR), which sits alongside the Data Protection Act and GDPR, outlines the privacy rights of individuals specific to electronic communications, particularly those of direct marketing. The legislation stipulates that unsolicited marketing messages (i.e. any message that has not been specifically requested) are somewhat restricted for marketing to individuals. In the case of direct marketing to businesses, PECR states that:

*You may email or text any corporate body (a company, Scottish partnership, limited liability partnership or government body). However, it is good practice – and good business sense – to keep a 'do not email or text' list of any businesses that object or opt out, and to screen any new marketing lists against that. In addition, many employees have personal corporate email addresses (e.g. firstname.lastname@org.co.uk), and individual employees will have a right under section 11 of the DPA to stop any marketing being sent to that type of email address.*

This rule is also stipulated in GDPR guidelines:

*If you are processing an individual's personal data to send business to business texts and emails, the right to object at any time to the processing of their personal data for the purposes of direct marketing will apply. This right is absolute and you must stop processing to that individual for these purposes when an objection is received.*

Therefore, with regard to direct marketing specific to businesses, or individuals in a business capacity, it is permitted to send unsolicited messages – provided that the correct measures have been taken to ensure those individuals or businesses have an opportunity to object to such messages and opt-out from any further communications. Mass marketing, with poorly constructed messages of little value to the recipient, is likely to result in objection to such communications, and potentially reports of spam. All marketing messages should be relevant and specific to the needs of recipients. For more information on PECR, please read the following guidance:

<https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf>

