Fort Privacy
Quick Guides

GUIDE TO B2B MARKETING

Marie Murphy

Fort Privacy

Fort Privacy Quick Guides

Cork: (087) 419 2098;
Email: info@fortprivacy.ie
Website: www.fortprivacy.ie

GUIDE TO B2B MARKETING

HOW TO BUILD YOUR SALES AND MARKETING CONTACTS AND STAY COMPLIANT WITH GDPR.

Business information such as email contact information and job title are personal data. So, the GDPR does apply to business related personal information.

The GDPR applies wherever you are processing 'personal data'. This means if you can identify an individual either directly or indirectly, the GDPR will apply - even if they are acting in a professional capacity. So, for example, if you have the name and number of a business contact on file, or their email address identifies them (e.g. initials.lastname@company.com), the GDPR will apply.

The GDPR only applies to the personal data on business cards if you intend to file them or input the details into a computer system.

You need to identify your legal basis for processing your B2B marketing data – just as you need to ensure you have a lawful basis for all your other data processing activities.

The good news is that you are likely to be able to rely on 'legitimate interests' to justify most of your business-to-business marketing.

Using legitimate interests as your legal basis requires a three-part test known as a legitimate Interest Assessment (LIA).

The LIA assesses the necessity and proportionality of the processing activity and includes a balancing test. This tests the balance between your legitimate interest for carrying out the processing and the rights and freedoms of the individual whose personal data you are processing.

To rely on legitimate interests for marketing activities you need to identify your specific interest underlying the processing and ensure that the processing is necessary for that purpose. You also need to show the way you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object to what you are doing.

You then need to consider the balancing test. You may find it is straightforward as business contacts are more likely to reasonably expect the processing of their personal data in a business context, and the processing is less likely to have a significant impact on them personally.

Cork: (087) 419 2098;
Email: info@fortprivacy.ie
Website: www.fortprivacy.ie

EXAMPLE – LEGITIMATE INTERESTS

Individuals attend a business seminar and the organiser collects business cards from some of the delegates.

The organiser determines that they have a legitimate interest in networking and the growth of their business. They also decide that collecting delegate contact details from business cards is necessary for this purpose.

Having considered purpose and necessity the organiser then assesses that the balance favours their processing as it is reasonable for delegates handing over business cards to expect that their business contact details will be processed, and the impact on them will be low. The organiser also ensures that it will provide delegates with privacy information including details of their right to object. This is done in the form of a privacy statement. The organiser subsequently collates the contact details of the delegates and adds them to their business contacts database.

You also need to consider ePrivacy Regulations for B2B email marketing.

The existing ePrivacy Directive of 2002 and the Irish ePrivacy Regulations of 2011 (which implement the 2002 Directive in Ireland) apply to traditional means of communication for example, mobile or landline telephone calls, SMS text messages and e-mails. The Irish ePrivacy regulations of 2011 contain an exception in respect of direct marketing to business email addresses.

The ePrivacy Regulation always applies to B2C marketing. The ePrivacy Regulation only applies to B2B marketing where that marketing is to sole traders, partnerships, unincorporated trusts, partnerships and foundations and their staff members.

The ePrivacy Regulation does not apply where B2B marketing is undertaken to staff members of limited companies, public limited companies, incorporated partnerships, trusts and foundations, local authority and government institutions.

If the B2B email marketing is undertaken to a business that the e-Privacy Regulation applies to, businesses need consent if they wish to process personal data for e-marketing purposes, where the data subject is not a customer. In contrast, a business can market to its own B2B customers on an opt-out basis if it has a) collected its customers' contact details in the context of a sale and b) given them the right to object to the use of those details for e-marketing purposes at the time of collection.

The consent required is GDPR consent, it has to be opt-in consent.

Cork: (087) 419 2098;
Email: info@fortprivacy.ie
Website: www.fortprivacy.ie

BUSINESS EMAIL LISTS – BEST PRACTICES

Consider the source of the email information you are adding to the list

Was it collected in a business context – on a business card, from a business directory, at a conference? Make sure you are only adding contacts who are relevant

Consider the type of information you are adding to the list

Are you adding a business email address? Avoid using personal email addresses or Gmail addresses. Always ask for a business email.

Consider the type of business you are marketing to

Is it a sole trader/unincorporated entity? Separate organisations into lists identifying if the e-Privacy Regulations apply and separating existing customers from prospective customers

Consider transparency requirements

How will you ensure someone knows they are on your list? It is required that you inform people and it is good practice to include a link to your privacy statement on every email.

Consider how you will manage your b2b lists

Does every communication include an opt-out option? How will you deal with requests to be removed from your database? Do you need to maintain a blacklist and check all future communications against that blacklist?

You must tell people what you are doing with their personal data and this applies to B2B marketing also.

You must tell people what you are doing with their information. This includes your purposes for processing their personal data, your lawful basis for processing, how long you plan to retain the data, and who it will be shared with. Organisations generally create a privacy statement to provide this information.

If you are relying on legitimate interests for direct marketing, the individual's right to object is absolute and you must stop processing when someone objects. Some organisations recommend keeping blacklists of people who have objected to ensure you do not add them to a sales/marketing list again in the future, but these need to be considered carefully to ensure they are appropriate for the situation.

Since the GDPR does apply to business related personal information you need to consider all your obligations in relation to the processing of the personal data. This includes the individual's right to access a copy of their personal data, requirements to inform contacts about the occurrence of a data breach and obligations to keep the information you process secure.

Cork: (087) 419 2098;
Email: info@fortprivacy.ie
Website: www.fortprivacy.ie

The following table contains a checklist for the most common GDPR compliance considerations when carrying out B2B marketing activities.

Considerations for processing personal data when carrying out B2B marketing activities	
Knowing what personal data you process?	Do you know what B2B marketing activities you carry out? Do you know what personal data you process across all your B2B marketing activities? Is this documented?
Documenting your lawful basis	Have you identified your legal basis for all personal data being processed?
Processing personal data for B2B Marketing based on legitimate interests	Has an appropriate analysis been carried out to ensure that the use of this legal basis is appropriate? That analysis must demonstrate that • there is a valid legitimate interest, • the data processing is strictly necessary in pursuit of the legitimate interest, and • the processing is not prejudicial to or overridden by the rights of the individual
Processing Personal Data for B2B Marketing purposes based on Consent	Where consent is used as the legal basis, have you put procedures in place to demonstrate that an individual has consented to their data being processed?
	Where consent is used as the legal basis, have you put procedures in place to allow an individual to withdraw their consent to the processing of their personal data?
Sources of contact information	What sources of b2b contact information do you use and are they all collecting the data and processing legally? Do you have Data Processing Agreements in place with the suppliers of this information?
ePrivacy Regulations	Do marketing communications comply with ePrivacy regulations? Can individuals opt-out of receiving b2b marketing communications from you?
Training and Awareness	Have your sales and marketing staff received appropriate data protection training and do they understand what they can and cannot do with the personal data they process as part of their B2B marketing activities?

Cork: (087) 419 2098;
Email: info@fortprivacy.ie
Website: www.fortprivacy.ie

Considerations for processing personal data when carrying out B2B marketing activities	
Purpose Limitation	Are personal data only used for the purposes for which they were originally collected?
Data minimisation	Are the personal data collected limited to what is necessary for the purposes for which they are processed? For instance, if you are carrying out B2B sales or marketing activities do you ensure you do not collect personal information that is unrelated to the business relationship?
Accuracy	Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the necessary changes are made without delay?
Retention	Are retention policies and procedures in place to ensure data are held for no longer than is necessary for the purposes for which they were collected?
	Do you have procedures in place to ensure data are destroyed securely, in accordance with your retention policies? Do you regularly clear out old mailing lists?
Duplication of Records	Are procedures in place to ensure that there is no unnecessary or unregulated duplication of records?
Appropriate technical and organisational security measures (Article 32)	Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?
Documented security programme	Is there a documented process for resolving security related complaints and issues that specifies the technical, administrative and physical safeguards for that covers your B2B sales and marketing data?
Access to personal data (Article 15)	Does your documented policy/procedure for handling Subject Access Requests (SARs) include the retrieval of B2B Marketing related personal data?
Handling a Data Breach	Does your data breach handling process include procedures for managing a data breach relating to B2B marketing information?